

Trust in Blockchain Technology

Dissertation

Zur Erlangung des akademischen Grades

Doctor rerum politicarum

der Fakultät für Wirtschafts- und Sozialwissenschaften der
Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg

vorgelegt von

Alexandra Dominique Palt

Hamburg 2024

Abstract

This dissertation investigates the multifaceted role of trust in the creation of blockchain technologies, emphasizing two case studies: Ethereum and Hyperledger Fabric. By combining Guido Möllering's (2006a) integrative trust framework and Michel Callon's (1986b) notion of translation from Actor-Network Theory (ANT), the research examines trust in blockchain technology as a socio-technical process. This renders visible multiple ontologies of trust. Trust and the absence of trust can constitute a problem or act as intersement devices. Leaps of faith enable enrolments and enrolment implies reflexive trust building. Moreover, trusting relationships connect actors, can hold actor-networks together, and mobilize them.

The research adopts a qualitative, abductive approach, triangulating data collected from fieldwork online and in interviews which captures a period from the end of 2013 to the beginning of 2018. In a reflexive process, the study employs translation theory to describe the emerging socio-technical world of blockchain technology as a dynamic process between human and non-human actors, contrasting it with trust theory. Although trust ontologies of the two cases Ethereum and Hyperledger Fabric appear similar at first glance, findings highlight that the platforms and actors involved are different, as are the subjects of trust crises, the intersement devices, the existing trust relations, the trust building mechanisms and the mobilized actor-networks. Trust building in the Ethereum actor-network relies more on community-driven processes and technology, whereas Hyperledger Fabric builds more on established structures and corporate actors.

Contributions to organizational trust research include exploring trust's role in the translation of two blockchain platforms, describing trust in information technology as a social process, and providing a nuanced view of actors attributing agency to technologies as non-human actors. Additionally, the study advances translation theory by articulating the diverse ontologies of trust in translation, which connect trust theory and Actor-Network Theory.

Acknowledgement

First, I want to thank my doctorate supervisor Tobias Scheytt and his right-hand man, Christian Huber. During my Master studies at Helmut Schmidt University in 2012/13, they revived my passion for critical thinking and writing when I visited their lectures on Management Accounting and Control. A few years later, they welcomed me again and gave me and my crazy blockchain dissertation project a home at their institute. In our weekly research seminars and in countless individual discussions, they and my colleagues Benjamin Ditzel, Nadine Gerhardt, Nathalie Iloga Balep, Jaromir Junne, Michael Lust, Claudia Meister-Scheytt and Jacob Reilley challenged and inspired my thinking and writing. I could not have imagined a more supportive, collaborative, and creative environment for conducting my research.

Likewise, I found an open and supportive environment during my research visit at University College Dublin. I want to especially thank Paul Ennis, Donncha Kavanagh and Gianluca Miscione, who made my time at the UCD Business School possible, and so fruitful. Their perspective on research and knowledge of blockchain technology enhanced my curiosity and understanding of the phenomenon, as did a research seminar and the many one-on-one conversations on blockchain, trust, and translation. These would not have been so valuable without the researchers and students of University College Dublin and Dublin City University.

Moreover, I owe a thank you to the 13 interviewees, who took the time to patiently share their blockchain experiences and knowledge with me. Although in my original research proposal I had not planned to conduct interviews, these conversations turned out to be some of the most precious material in my empirical research.

I am also grateful to Bain & Company, the firm that I belong to and which gave me the opportunity to pursue my research dissertation project full time while on leave. Not to mention my colleagues who encouraged me to pursue the dissertation project, and who shared their experience and advice with me.

Most importantly I could not have done this without my friends and family. They believed in me, encouraged me, and when the project got serious, they respected that I was often unwilling to make conversation about my dissertation project. Torben, you were my home and stuck it out every single day. You are my stroke of luck.

Contents

- Contents..... 4
- Figures..... 14
- Tables 14
- Abbreviations 11

- 1 Introduction 9**

- 2 Blockchain technology 18**
 - 2.1 What is Bitcoin? 18
 - 2.2 What is blockchain technology? 22
 - 2.3 What does trust have to do with it? 24

- 3 Trust and technology 29**
 - 3.1 Trust..... 29
 - 3.1.1 Organizational trust research..... 29
 - 3.1.2 Möllering’s integrative trust framework 33
 - 3.1.3 How information technologies are implicated in trust 45
 - 3.2 The becoming of actor-networks 57
 - 3.2.1 Actor-Network Theory and translation 57
 - 3.2.2 How translation studies talk (or do not talk) about trust 64

- 4 Methodology, method, and case background 73**
 - 4.1 Research methodology and method..... 73
 - 4.2 Context of the Ethereum and Hyperledger Fabric cases 79

- 5 Ethereum..... 83**
 - 5.1 Problematization: Trust crises 83
 - 5.1.1 Translation..... 83
 - 5.1.2 Trust 93
 - 5.2 Interesement: Trusted trustless technology 95
 - 5.2.1 Translation..... 95
 - 5.2.2 Trust 107
 - 5.3 Enrolment: Building trust in Ethereum 111
 - 5.3.1 Translation..... 111
 - 5.3.2 Trust 128
 - 5.4 Mobilization: Daring to rely on Ethereum 132
 - 5.4.1 Translation..... 132
 - 5.4.2 Trust 139

6	Hyperledger Fabric	141
6.1	Problematization: Different trust problems	141
6.1.1	Translation.....	141
6.1.2	Trust	152
6.2	Interessement: Other trusted actors	154
6.2.1	Translation.....	154
6.2.2	Trust	162
6.3	Enrolment: Building trust in Hyperledger Fabric.....	165
6.3.1	Translation.....	165
6.3.2	Trust	173
6.4	Mobilization: Preliminary reliance on Hyperledger Fabric.....	176
6.4.1	Translation.....	176
6.4.2	Trust	179
7	Discussion, implications, and outlook	182
7.1	Summary and case study comparison.....	182
7.2	Contributions to trust research.....	192
7.3	Contributions to the study of translation	197
7.4	Implications and outlook	199
	References	202

Figures

Figure 1: Trustor, trustee and facilitator (own illustration)..... 31
Figure 2: The trust wheel – an integrative framework (Möllering, 2006a, p. 110)..... 34
Figure 3: Institution as facilitator for trust and as trustee (own illustration)..... 39
Figure 4: Roles of technology as trustee and as facilitator for trust (own illustration)..... 46

Tables

Table 1: Overview of retrievals of blog entries from the blogs of Ethereum, Hyperledger
Foundation and IBM’s international blockchain blogs 76
Table 2: Overview of press search 77

Abbreviations

ABC	Activity-Based Costing
ADEPT	IoT-blockchain research project by IBM
AML	Anti-Money Laundering
ANT	Actor-Network Theory
BaaS	Blockchain as a Service
BBVA	Banco Bilbao Vizcaya Argentaria
CEO	Chief Executive Officer
CIO	Chief Information Officer
CLS	Continuous Linked Settlement
CMO	Chief Marketing Officer
CSR	Corporate Social Responsibility
CTO	Chief Technology Officer
CUI	Centre Universitaire d'Informatique
DAH	Digital Asset Holding
DAO	Decentralized Autonomous Organization
DApp	Decentralized Application
DIY	Do It Yourself
DLT	Distributed Ledger Technology
DRG	Diagnosis-Related-Group
EBaaS	Ethereum Blockchain as a Service
EDI	Electronic Data Exchange
EEA	Enterprise Ethereum Alliance
e.g.	exempli gratia
EGOS	European Group for Organizational Studies
EOA	Externally Owned Account
ERP	Enterprise Resource Planning
ETH	Ether
EVM	Ethereum Virtual Machine
FINT	First International Network on Trust
FX	Foreign Exchange
GDPR	General Data Protection Regulation
HIPPA	Health Insurance Portability and Accountability Act

HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
IBV	IBM Institute for Business Value
ICO	Initial Coin Offering
i.e.	id est
ILDIS	International Legume Database and Information System
IoT	Internet of Things
IT	Information Technology
k	kilo
KYC	Know Your Customer
LF	Linux Foundation
LOC	Line of Code
MIT	Massachusetts Institute of Technology
MTN	Mobile Telephone Network
NSA	National Security Agency
OPP	Obligatory Passage Point
POC	Proof of Concept
SME	Small and Medium-sized Enterprise
SMTP	Simple Mail Transfer Protocol
STS	Science and Technology Studies
SWG	Standing Working Group
SXSW	South by Southwest
TCP/IP	Transmission Control Protocol/Internet Protocol
TSC	Technical Steering Committee
UBS	United Bank of Switzerland
U.S.	United States of America
USD	United States Dollar
UX	User Experience
VAT	Value-added Tax
WEF	World Economic Forum

1 Introduction

Today's emerging blockchain technology has not only assembled networks of IT geeks and cryptocurrency investors, but also managers of global information technology corporations, logistics and trade companies, manufacturing firms, banks, private and institutional investors, public institutions, governments, and regulators. Simply speaking, a blockchain platform maintains a transaction ledger, which is shared in a computational network and whose participants contribute to the validation of transactions; as basic IT infrastructures, blockchain platforms also allow for application programming.

Blockchain technology started to garner increased awareness from 2013 onwards, yet it has been around since 2008 as the digital infrastructure underlying the cryptocurrency Bitcoin – the alternative online payment system that was intended to be independent from governmental and corporate interference. Since blockchain's origins, a variety of blockchain platforms apart from Bitcoin have been developed, some of which are designed particularly for business use. In 2015, blockchain technology appeared on the agenda of the World Economic Forum (WEF) as an emerging technology in the field of financial services (McWaters, 2015). Ever since, the technology has been subjected to global hype¹ and enthusiasm insofar as “it has started to seem that the most intractable of the world's problems have merely been waiting for blockchain to arrive” (Mulligan, Zhu Scott, Warren, & Rangaswami, 2018, p. 3). Such a sarcastic statement from a WEF report shows that overblown expectations are being recognized. On the other hand, it makes it clear that business organizations' interest in the technology continues. In addition to commercial payments and cryptocurrencies, tried use cases include international money transfers, tracking of ownership and transactions of physical and non-physical items like cars, shipping containers, drugs, as well as luxury goods or financial assets. The technology also provides possibilities to share confidential information, for example customer data or health data, in a shared blockchain infrastructure.

¹ Public and economic attention and expectations are also reflected by blockchain technology's position at the “peak of inflated expectations” of Gartner's *Hype Cycle for Emerging Technologies* in 2017 and 2018 (Panetta, 2017, 2018). Moreover, McWaters (2016) figures exemplify market dynamics around blockchain technology: More than 1.4 billion USD of venture capital have been invested between 2013 and 2016, over 2500 patents have been applied during the same period and in 2016 over 90 central banks were involved in discussions on blockchain (p. 14). Venture capital investments in the technology multiplied during the following years to 3.9 billion USD cumulated in the first three quarters of 2018. In addition, through a new fundraising practice, digital tokens worth approximately 12 billion USD were invested in blockchain projects during the first three quarters of 2018 (“Burning Billions: Tokens cents on the dollar against raised capital,” 2018). Over the course of 2017 market prices of some of the largest cryptocurrencies Bitcoin and Ether, in terms of total value, raised up to exchange rates of over 17,000 USD in December 2017 and over 1,400 USD in January 2018 respectively before they collapsed again to nearly 3,750 USD and 135 USD respectively by the end of December 2018 (Coindesk, n.d.a, n.d.b).

Blockchain-based computer games are even available, and the technology has been tested for application in the Internet of Things (IoT).

Since its anonymous inventor(s) – who go by the name of Satoshi Nakamoto – proposed Bitcoin as a “system for electronic transactions without relying on trust” (Nakamoto, 2008, p. 8), the emergence of blockchain technology seems to be inextricably linked to matters of trust. Amidst the global financial crisis in 2007/8, Bitcoin was supposed to circumvent distrusted financial institutions by processing online payments. The Bitcoin system is comprised of algorithms, which allow it to operate on a distributed peer-to-peer computer network, without a central clearing house and with an algorithmically determined issuance rate of bitcoins. A prevailing narrative of the Bitcoin community is that Bitcoin is “trustless” or “trust-free”. This means users do not have to trust one another or an established institution in order to rely on the Bitcoin as money, or for the Bitcoin system to perform transactions. According to anthropology and media scholars Maurer, Nelms, and Swartz (2013) Bitcoin attributes trust to the algorithm instead:

Trust in the code substitutes for the (socially and politically constituted) credibility of persons, institutions, and governments. It is this – not the anonymity or the cryptography or the economics – that makes Bitcoin novel in the long conversation about the nature of money. (Maurer et al., 2013, p. 263)

The discursive turn from Bitcoin as a digital currency towards the technological infrastructure of blockchain also entails the promise of trust. In 2015, *The Economist* labelled blockchain technology “the trust machine” (“The promise of the blockchain,” 2015) and IT evangelists such as William Mougayar predicted that blockchain would change the nature of trust within and between organizations:

With the blockchain, the trust train is moving to a new destination. It is shifting from humans and central organizations to computers and decentralized organizations, via an underlying blockchain-based decentralized consensus protocol that governs its delivery. (Mougayar, 2016, pp. 39–40)

However, scholars researching Bitcoin and blockchain technology increasingly question claims about blockchain’s characterization as trustless, as they observe trusting relations within the socio-technical world of Bitcoin. Such controversial observations and statements in the empirical and scientific discourse on blockchain technology hint at a complex relationship between the emerging blockchain technology and the notion of trust. This is of particular concern for business organizations as they engage with blockchain technology. This in turn makes blockchain technology an interesting research phenomenon for those interested in the concept of trust in organizations studies. Curiously, however, work on trust in organization

studies has so far remained largely silent on the topic of blockchain and its implications for businesses. Thus, inspired by the debate about Bitcoin's trustless character and the presumable complexity of blockchain technology's relationship with trust, my work follows the question: What is the role of trust in the creation of blockchain technologies?

Over the course of half a century, organization and other management studies have yielded a vast and vivid academic discussion on trust within and between organizations and individuals. This has resulted in trust constructs that differentiate trust by levels, bases, or contexts. The organizational trust research community has also discussed trusts' dualities and relations to other concepts like distrust, power, and control. However, organizational trust research tends to emphasize the roles of human actors and organizations as trustees. Until now, less attention has been spent on trust in information technologies. A recent example of this is a dialogue in organizational trust research on institutional trust repair, which despite being fueled by the financial crisis of 2007/08, has mostly disregarded the blockchain technology and cryptocurrencies which have emerged during the same time. A glance at other academic disciplines, such as information systems research, also show that trust in general information technology infrastructures (how I understand blockchain technology) is undertheorized. The discourse in information systems research is rather user-centric, emphasizing the importance of user trust in specific IT artifacts, trust in the provider of online services and its websites, or trust between users. However, calls for more networked perspectives on trust in IT artifacts suggest that more consideration is needed of the dynamic relations among multiple actors. Moreover, in organization studies and in information systems research, those who focus on the topic of trust share an underlying assumption that information technologies lack agency.

In my work, I take a different stance to investigate the roles of trust in the creation of an information technology. I combine the integrative trust framework by Guido Möllering (2006a) and the notion of translation by Michel Callon (1986b) from Actor-Network Theory (ANT) as theoretical perspectives on blockchain technology. With this approach, I attribute agency to blockchain technology, consider the social dynamics between multiple actors during the creation of blockchain technology, and explore the various roles of trust in blockchain's emergence.

The work of Guido Möllering (2006a) reminds trust research of the full spectrum of bases for trust. In his monograph, *Trust: Reason, routine, reflexivity*, Möllering presents an integrative trust framework, which draws upon multiple streams of trust literature and bases of trust. With this, he contributes to an ontological shift in organizational trust research – one

which moves toward a process perspective on trust within and between organizations. This shift has not yet reached research on trust with regard to information technology – neither in organizational trust research nor in other disciplines, such as information systems research. I achieve an enriched perspective on trust’s role in the creation of blockchain technology by considering trust as a process, which has a broad spectrum of foundations. According to the integrative framework, the essence of trusting “in more or less specific others” (Möllering, 2006a, p. 111) is to take a leap of faith. This leap of faith implies that we have to deal with remaining uncertainties and our own vulnerabilities (Möllering, 2006a, p. 111). It does not mean that we need to eliminate them, but act despite them. Möllering (2006a) conceptualizes trust as a process, which can emerge over time. This process draws on “reason, routine and reflexivity” (Möllering, 2006a, p. 111). Reflexivity refers to active trust building in personal interactions, for example through familiarization and mutual openness. Routines are the rules, roles and habits, which facilitate trust between actors. And reason refers to rational choices one makes based on perceived trustworthiness. Drawing on the three bases and the leap of faith, I enhance extant literature by taking this process perspective on the role of trust into account when studying the creation of blockchain technology.

To conceptualize the processual character of an emerging information technology, and consider the agency of human as well as non-human actors, I combine trust research with the ANT notion of translation. ANT sheds light on the becoming of things. These things can be technological systems, for example an electric vehicle, but may also include scientific knowledge, management ideas, accounting systems, or cultural practice. With its origin in the investigation of the social production and legitimization of facts and technologies, ANT considers technology and knowledge as only temporarily stable. These things become mobilized as multiple human and non-human actors come together in a network of relations. The notion of translation describes the development of these relations, which assemble and thus become temporarily stable, as well as the transformation of actors in this process. Translation studies have become especially popular in organization studies and accounting research.

In my work, I refer to the much applied notion of translation by Michel Callon (1986b), which renders visible the intentionality of actors in constructing an actor-network. He distinguishes four moments of translation: Problematization, interessement, enrolment, mobilization. Problematization, as the term already implies, serves to create awareness of a problem and to propose a solution that is in the interest of particular actors. Interessement serves to inflict roles and relations to actors, ensuring the becoming of the network and

promoting the enrolment of actors. Callon (1986b) uses the expression of locking allies into place (p. 206), which refers to connecting actors around a common cause or interest. Interestment devices support the stabilization of identities and the building of relations between actors. Such devices can be different things, including physical objects, discourses, knowledge, or practices. During this phase, the new network is hypothetical. It becomes reality when actors negotiate, modify and accept their roles in relation to others and shape their behavior accordingly during enrolment. Finally, translation leads to a “mobilization of actors [...] by forming alliances and acting as a unit of force” (Callon, 1986b, p. 216). This is a network of actors, a temporarily stable actor-network with one identity. Although the ANT notion of translation and research on trust as a process share a focus on becoming, ANT has not yet been considered in organizational trust research. By combining the perspectives of Möllering (2006a) and Callon (1986b), I can afford attention to the assemblage of human and non-human actors, consider the processual character of trust, and shed light on different roles of trust in the creation of blockchain.

I developed the idea of combining these two theoretical perspectives while being confronted on multiple occasions with the uncertainty and messiness inherent to an emerging technology such as blockchain. The choice of these theoretical lenses became even more obvious with the explicit, but often contradictory claims surrounding blockchain’s relationship with trust. One exemplary incident occurred during the summer of 2016, as I searched for a dissertation topic at the Helmut-Schmidt-University’s department of management accounting and control. I had little knowledge about blockchain technology but found it interesting and started reading through scientific databases. Enthusiasts and IT evangelists claimed blockchain could disrupt ways of organizing and trusting in business. I admit that I was immediately fascinated. On the other hand, at that point in time, an automated blockchain-based fundraising organization had recently been exploited and the price of the cryptocurrency Ether had crashed. My own uncertainty and vulnerability about whether this technology would actually work, and whether the phenomenon would still be of relevance by the time I would have finished my dissertation project could not have been greater. I took my own leap of faith and continued following blockchain technology’s translation. In 2017 and at the beginning of 2018, I paid special attention to blockchain discourses and activities online; it was also during this time that I experienced a number of

practitioner conferences, blockchain meetups, and a blockchain hackathon². I saw young software developers, entrepreneurs, experienced developers, and managers trying to figure out – and debating the promises and limits of – blockchain platforms and applications. I recall one moment at a practitioner conference in the summer of 2017. A start up presented a blockchain-based application, and the presenter claimed their application would eliminate the need for trust. When a visitor countered “but we have to trust you”, the two started to debate. Though this debate remained unresolved, it opened my eyes to the centrality of trust in blockchain’s development.

Amid the novelty of blockchain technology and the scarcity of organizational research on the relationship between trust and general information technology systems, I investigate the blockchain phenomenon with a primarily qualitative empirical approach. This is in line with calls for qualitative studies, given that trust research is so far characterized by a strong bias towards quantitative work. My research draws upon two case studies of blockchain platforms, which have targeted and involved a broad range of organizations over the past several years: Ethereum and Hyperledger Fabric. According to ANT paradigm’s methodological suggestions to “follow the actors” (Latour, 2005, p. 12), I followed the development of these two blockchain platforms over a period of approximately four and a half years³.

The two case studies serve as examples of one phenomenon: Blockchain technology. Both platforms have been developed as open source projects. As such, the actors associated with each project often communicate in public while the information technology is being developed. In both cases, trust is an object of communication. Moreover, in contrast to Bitcoin, at the time of selecting the cases, both platforms were programmable and business organizations from their respective industries were involved in their creation. Each emerged, however, from different organizational backgrounds. As an incorporative blockchain project, Hyperledger Fabric (Swartz, 2017) was initiated by IBM as a blockchain platform for enterprises. Under the umbrella of Linux Foundation’s Hyperledger project, the Hyperledger Fabric platform was developed in cooperation with developers from other firms. By contrast, Ethereum started as a radical project (Swartz, 2017). It was initiated by programmers involved with the Bitcoin community. Its inventor was Vitalik Buterin, a then 19-year old college dropout who was involved in a Bitcoin-related project and wrote for the Bitcoin Magazine. As both platforms, Ethereum and Hyperledger Fabric have been developed as open source

² At hackathons, events which last one or more days, participants come together and develop software with a specific technology.

³ This time frame takes into consideration the publishing dates of my collected material.

software development projects, the code is transparent and developed in open source communities. Although both platforms are labeled as blockchain technology, they have some fundamental differences. The Ethereum mainnet is one shared platform and open for anyone to join. In this sense it is similar to Bitcoin. Its operations are conducted decentrally within a network of computational resources. All processes executed on the platform are stored in a decentralized and publicly accessible ledger. Conversely, Hyperledger Fabric is a software used by business organizations to create separate networks among a pre-defined group of network participants. Within these networks, transactions and data is also shared, but with specific access rights, e.g. it is not accessible for outsiders. Ethereum's mainnet has also been complemented with separate networks which have restricted permissions. I am interested in which ways these platforms, each with their own distinct characteristics, have been translated as well as how this process is related to trust.

My methodology is influenced by the descriptive attitude of science and technology studies (STS), in particular ANT, and by abductive reasoning. I aimed to experience the phenomenon and follow the traces of activity and communication in the creation of Ethereum and Hyperledger Fabric. My insights were derived from current and historical data in various online and offline contexts. As indicated above, I visited four practitioner conferences, four blockchain meetups, and a hackathon. The research method of my empirical analyses, however, draws mainly upon triangulation of data collected from fieldwork online and in face-to-face or video interviews. This analysis of documents, e.g. web texts and blogs in combination with other forms of data such as video recordings and interviews, is a common practice in case study research on virtual worlds. I gathered data mainly through web and press research and supplemented it with interviews. I reviewed the webpages of Ethereum, Hyperledger and IBM and retrieved 515 blog entries from their respective blogs. From these sources and their authors, I was directed towards other sources, e.g. books, white papers, reports, videos on YouTube, websites of blockchain projects and firms, blogs, forums, and social media networks. Moreover, I conducted a structured press search, which yielded 773 publications. I supplemented this search with 12 semi-structured interviews with actors participating in and observing the respective networks I studied. I gained access to interviewees mainly through my visits to practitioner meetings in Germany and Ireland, and with support of the blockchain researchers at University College Dublin. The data captures a time period from end of 2013 to beginning of 2018. I analyzed the data in a reflexive process of data gathering, analysis and theoretical interpretation. Exchanges and discussions with other researchers have also shaped my exploration and theorizing of trust in blockchain

technology. My research stay at the Management Information Systems Group at University College Dublin, an encounter with blockchain and trust researchers at Dublin City University, feedback from a Pre-Colloquium PhD Workshop in 2018, and regular discussions with my research group at the Helmut-Schmidt-University's department of management accounting and control between 2017 and 2019, were especially central in providing me with intellectual stimulation.

My main contribution to organizational trust research and to studying translation is that “trust in blockchain technology” – the title of this book – is manifold. In my empirical analyses, I explore trust's role in the translations of two blockchain platforms. I thereby shed light on multiple ontologies of trust associated with the creation of two blockchain platforms. With this approach, my work discusses the notion of trust as discussed by Möllering (2006a) and others, and contributes to organizational trust research in several ways. It describes trust building in an information technology as a social process, which involves problems with regard to trust, ideologies of trust, and reflexive trust building among multiple actors. For this I take into consideration a range of relevant actors by analytically separating the technical actor from actors who support the technology but are not necessarily singular provider organizations. My work also exemplifies what it means to attribute agency to blockchain as an information technology and by doing so, contradicts the established assumption in organizational trust research that information technologies as trustees have no agency. Overall, in speaking to research on trust in information technologies, my work proposes an ontological shift towards trust as a process. Lastly, my work leads to some speculations about how blockchain-enabled relations might influence theory on digital trust cues as well as the distinction between institutional and process-based trust.

On the other hand, my work also contributes to the study of translations in organization and accounting studies. My reflections on several relations and devices through the lens of Möllering's (2006a) integrative framework allows me to discover multiple ontologies of trust in translation, which connect trust theory with the notion of translation. Trust and the absence of trust can constitute problems, which destabilize actor-networks and substantiate the translation of blockchain technology. Furthermore, trust and trustlessness are used as ideologies or interestment devices to connect and attract actors. Moreover, trust building activities are part of an enrolment process, which is further nurtured by leaps of faith by particular actors. Such activities can result in the temporary establishment trust, which connects actors in mobilized actor-networks. This rich ontology of trust can sharpen our view

of trust as well as the language we use to describe trust when studying translation in organization and accounting studies.

I set forth these arguments in the following structure of my work. Although programmable blockchain platforms used by business organizations have distinguished themselves from Bitcoin, they inherited a complex linkage of blockchain technology from Bitcoin. In chapter 2, I take a glance over this heritage by introducing Bitcoin and its multiple identities – as a cryptocurrency, a technical system, and a community; I follow its complex linkage to trust and the discursive turn towards blockchain technology. In the subsequent chapter 3, I introduce two bodies of literature, trust theory and ANT's translation, which serve as theoretical lenses and to which I later also contribute. I outline Möllering's (2006a) ontological shift and argue how trust research spends little attention to trust in information technologies, and treats information technologies different from human actors. This inspires me to combine trust with translation, two theoretical concepts which I suggest are implicitly connected. This is followed by an outline of my qualitative research approach to investigating the role of trust in the translation of blockchain technology in two case studies 2. My empirical case analyses and discussions with trust theory in chapters 5 and 6 render visible multiple ontologies of trust – based on reason routine and reflexivity – including problems, interessement devices, trust as inputs and outputs to enrolment, trust building practices, trust as a relational element and failed trust in processes of trust building. Although the ontologies between the two cases appear similar at first glance, the platforms and actors involved are different, as are the subjects of trust crises, the interessement devices, the existing trust relations, the trust building mechanisms and the mobilized actor-networks. As I discuss in chapter 7, these findings contribute to organizational trust research and the study of translations in organizational and accounting research. Not only do they provide a multifaceted view of trust, but they also propose an ontological shift toward a process perspective for researching trust in information technologies. Furthermore, this study can inspire additional research on blockchain-enabled relations, which have only just begun to emerge.

2 Blockchain technology

In this chapter, I introduce the phenomenon of blockchain technology. I proceed by first referring to Bitcoin, before drawing attention to the complex linkage between Bitcoin and trust, which affects blockchain technology more generally. Bitcoin was the first blockchain system in operation, and it continues to be the most valuable cryptocurrency. Moreover, it has also served as a straw man from which my case studies – Ethereum and Hyperledger Fabric – have differentiated themselves. Thus, I start by introducing Bitcoin (2.1) before continuing with blockchain technology (2.2) and a dedicated a sub-chapter on the relationships between Bitcoin, blockchain technology, and trust (2.3).

2.1 What is Bitcoin?

Bitcoin is the oldest and so far most researched blockchain platform (Beck, Müller-Bloch, & King, 2018; Risius & Spohrer, 2017). When Bitcoin was launched in 2009, the term blockchain had not yet been established. At that point, the decentralized⁴ and pseudonymous⁵ (De Filippi, 2016) online payment transaction system of Bitcoin implemented a system outlined in a whitepaper by Nakamoto (2008). In that whitepaper, the anonymous author(s)⁶ describe a “system for electronic transactions without relying on trust“ (Nakamoto, 2008, p. 8).

The Bitcoin system features a built-in digital currency, the Bitcoin, which was intended as an online payment token (Nakamoto, 2008). Besides payment, it has been used for foreign transfer of bitcoins⁷ (Böhme, Christin, Edelman, & Moore, 2015, pp. 222–225), and has also been perceived as a financial asset (Dallyn, 2017; F. Glaser, Zimmermann, Haferkorn, Weber, & Siering, 2014). Currently, Bitcoin and other blockchain-based digital currencies are referred to as cryptocurrencies (Campbell-Verduyn, 2018b; DuPont, 2019). Scholars in economic and social sciences continue to discuss the extent to which Bitcoin is money (Dodd, 2018, p. 48; DuPont, 2019; Hütten & Thiemann, 2018; Kavanagh, Miscione, & Ennis, 2019; Maurer et al., 2013; Nelms, Maurer, Swartz, & Mainwaring, 2018; Weber, 2016). In addition,

⁴ Dallyn (2017) points out that although Bitcoin is based on “ideals of decentralization” (p. 470) the actual network is rather centralized with regard to bitcoin distribution, mining capacities and decision governance.

⁵ Transactions of bitcoins are operated through public addresses, which are random numbers. As long as such addresses are not associated with a users’ identity, her identity remains private. Pseudonymity disguises but doesn’t hide a user’s identity (De Filippi, 2016).

⁶ Until today, it is unclear who the author(s) is/are under the pseudonym Satoshi Nakamoto (DuPont, 2019, p. 44).

⁷ I follow literature on Bitcoin, where the system and cryptocurrency are referred to with a capital B, and the cryptocurrency unit bitcoin is referred to with a lower-case b.

much public attention has been spent on Bitcoin's volatile price (Dallyn, 2017) and the use of bitcoins for illegal activities (Dodd, 2018, p. 48; Kavanagh et al., 2019).

The open source algorithms which run the Bitcoin system and the issuance of bitcoins are not governed by an established governmental institution, such as a central bank (Dallyn, 2017). Instead, they are governed by a community which has assembled to support the platform (Hsieh, Vergne, & Wang, 2018; Musiani, Mallard, & Méadel, 2018). Especially during its first years of existence, this community comprised of mostly technology-savvy individuals (Swartz, 2018). Bitcoin's transaction processing also draws on a decentralized approach, where a peer-to-peer network of computational nodes executes Bitcoin transactions and maintains a historic record of all transactions. The nodes can be run by any user with sufficient computational capacity (Antonopoulos, 2014, p. 26). Thus, the system is intended not to rely on a single server operated by an authoritative institution, but instead a peer-to-peer computational network (Dallyn, 2017, p. 463). Each time a user makes a transaction, she digitally signs it (Antonopoulos, 2014, p. 18) and the transaction is sent across the network (Antonopoulos, 2014, p. 25). Periodically, nodes in the Bitcoin network bundle multiple transactions into a new block and process it according to Bitcoins' consensus algorithm (Antonopoulos, 2014, p. 27). This so-called proof-of-work consensus algorithm requires the nodes to solve for a cryptographic puzzle – a hash function – through, among other steps, trial and error in order to successfully process a transaction block (Antonopoulos, 2014, p. 26). This mechanism is meant to prevent fraud or manipulation by demanding costly computational work from the nodes. Network nodes are incentivized with the allocation of Bitcoin to participate in this process (Antonopoulos, 2014, p. 173). The node which executes the transaction first by solving the hash function is assigned a particular amount of bitcoin (Antonopoulos, 2014, p. 27). As bitcoins are created in the very moment of the incentive allocation, this activity is called mining. Mining thus also determines the issuance rate of Bitcoin (Antonopoulos, 2014, p. 173). The result of the transaction processing is an entry of the block in a ledger, which is stored and frequently verified on other network nodes. This ledger is called a blockchain, as within this ledger, all blocks are connected to one another in through a piece of information on the previous block in the chain (Antonopoulos, 2014, p. 28). Bitcoin's ledger is publicly accessible and comprises information about past transactions, including the timestamp, the amount of bitcoin, and pseudonymous sender and receiver account (Antonopoulos, 2014, p. 24; De Filippi, 2016). Such transparency of transactional data enables the Bitcoin nodes to coordinate among themselves without a central

authoritative platform. On the other hand, it can also compromise users' data privacy (De Filippi, 2016).

Literature on Bitcoin and blockchain technology agrees that the emergence of Bitcoin during and in the aftermath of the global financial crisis of 2007/8 was not accidental (Campbell-Verduyn, 2018b, p. 2; Dallyn, 2017, p. 468; Dodd, 2018, p. 39; DuPont, 2019, p. 33; Hütten & Thiemann, 2018; Musiani et al., 2018, p. 133; Werbach, 2018, pp. 34–35). A network of trusting relationships failed during the global financial crisis, as Gillespie and Hurley (2013) describe:

In sum, trust failed in the 2008 financial crisis because the foundation of the financial system was extremely fragile. The system was based on an intricate network of trust relationships: Home buyers trusted the knowledge and expertise of their mortgage brokers; banks trusted the mortgage brokers and the credit rating agencies on the viability of the loans and securities; investors, lenders and hedge funds trusted the banks and credit rating agencies on the predicted profitability and assessed risk levels of their products; bank shareholders trusted their leaders and their Board to monitor institutional risks prudently; ordinary citizens with a pension trusted the pension fund managers as well as government regulators. Everyone trusted the market. The system relied upon reputational effects and indicators of trustworthiness that, in the final analysis, proved to be largely unwarranted. (Gillespie & Hurley, 2013, p. 190)

In the U.S., the financial crisis caused a rise of unemployment and unexpected loan defaults (Uslaner, 2014, p. 21). The Occupy Wallstreet movement exemplified a mobilization of people who blamed Wallstreet for the global financial crisis and were dissatisfied with the actions of those in power, including governments and big business (Tremayne, 2013, 123). In Europe and the U.S., banks received financial support from public institutions (Campbell-Verduyn, 2018a, p. 2; Gillespie & Hurley, 2013). The crisis revealed that the global financial system was more interconnected than expected, resulting in systemic risks (Werbach, 2018, p. 35). On both continents, central banks behaved as “quasi sovereigns” (Hütten & Thiemann, 2018, p. 30). In Western societies, public trust in governments, business, and public institutions continued to decrease (Bachmann, Gillespie, & Priem, 2015, pp. 1123–1124; Gillespie & Hurley, 2013; Uslaner, 2014).

Nakamoto (2008) points out that Bitcoin circumvents financial institutions with regard to online payments (p. 1). This comprises two aspects. First, the issuance of money is algorithmically determined and second, the processing of transactions is conducted in the computational peer-to-peer network without a third party financial institution (Dodd, 2018, pp. 47–48) like PayPal or national clearing houses (Nelms et al., 2018, pp. 20–22). In this context, Bitcoin constituted an alternate currency system to fiat currencies backed by governments (Dallyn, 2017, p. 468; Hütten & Thiemann, 2018; Weber, 2016). In 2013, Nelms

et al. (2018) observed a “payment system channeling unmediated flows of money and reputation among a closed community of peers” (Nelms et al., 2018, p. 27), nurtured by an anti-state attitude and community exclusivity. Its users perceived the platform and its digital currency as an alternative or resistance to established institutions in the financial system, such as governments, central banks, and economic routines like inflation (Lustig & Nardi, 2015). They prevalingly ascribed themselves to political libertarianism (Lustig & Nardi, 2015), which manifested itself in the shared “conviction that an alternative money system based on cryptography, which is beyond the control of the state, is both sustainable and desirable” (Dallyn, 2017, p. 468). This concurrence of digital money and protest (Dodd, 2018, p. 40) has attracted “goldbugs, hippies, anarchists, cyberpunks, cryptographers, payment systems experts, currency activists, commodity traders, and the curious” (Maurer et al., 2013, p. 262). Moreover, despite its difficulties in disguising user information, Bitcoin was an anti-movement against big data practices that convert digital traces into assets (De Filippi, 2016; Dodd, 2018, pp. 40–41). In fact, Bitcoin has roots in the cypherpunk scene, which fought for privacy in information systems and society more generally (Swartz, 2018, pp. 3–4). Exemplary for Bitcoin’s opposition to stable institutions and regulation was when it became an accepted value for donations to WikiLeaks in 2011, after the payment service PayPal was forced to deny money transfers (Hütten & Thiemann, 2018, p. 32). Similarly, Bitcoin demonstrated ignorance towards institutions in its usage for buying and selling illegal products and services, for example drugs, guns, and computer-hacking services on the dark web online marketplace, the Silk Road (Musiani et al., 2018, p. 145) – what Hütten and Thiemann (2018) term Bitcoin’s “shadow economy” (p. 42). This introduction phase of Bitcoin lasted from around 2009 until 2014. Since then, Bitcoin has conceived a less shadowy existence. Until 2015, it was increasingly adopted within established stationary and online trade markets (Hütten & Thiemann, 2018). However, such attempts did not prove successful and today Bitcoin is rarely used for commercial transactions, partly due to its price volatility (DuPont, 2019, p. 51). After years of limited regulation in the Bitcoin sphere, regulatory agencies have begun contributing to a “normalization” (Hütten & Thiemann, 2018) of Bitcoin, although one can doubt whether it will ever reach mainstream adoption for its initial purpose, i.e. monetary payment (Dodd, 2018, p. 38). Instead, Bitcoin continues to be used for economic speculation (Dallyn, 2017; Hütten & Thiemann, 2018; Swartz, 2018).

I have started this chapter with an introduction to Bitcoin in order to illustrate the roots of blockchain, and at the same time, the straw man of subsequent blockchain platforms. In the

following, I describe the discursive and technical turn from Bitcoin to blockchain technology and explain what we understand as blockchain technology today.

2.2 What is blockchain technology?

Anthropology and media scholars Bill Maurer, Taylor C. Nelms and Lana Swartz have conducted research on money and investigated Bitcoin since its inception (Maurer et al., 2013). These authors have perceived the discursive shift from Bitcoin to blockchain at a payment industry conference:

At Money 20/20 in 2013, we saw a new discourse emerge as users and advocates began to formulate a narrative about Bitcoin not as a currency or commodity, but as a ‘protocol’. Many presenters emphasized not Bitcoin, but the blockchain, and some compared the blockchain to SMTP, the infrastructure underlying email. Like SMTP, they argued, the blockchain provides an ‘open platform’. (Nelms et al., 2018, pp. 21–22)

By the year 2015, the blockchain hype surpassed that of Bitcoin (Swartz, 2017, p. 85), directing our understanding to blockchain platforms as socio-technical infrastructures. With regard to Bitcoin, Swartz (2017, 2018) describes the emphasis on blockchain as socio-technical infrastructure as “the way some enthusiasts value the ability to mutually build and support a collaborative platform upon which to transact, free from the prying eyes and inference of corporate intermediaries” (Swartz, 2017, p. 85). She concludes that “for infrastructural mutualists, it [the primary feature] is the blockchain, a decentralized, autonomous infrastructure with shared utility produced and maintained by all participants” (Swartz, 2017, p. 85).

In today’s reality, many blockchains are not independent from corporate intermediaries as imagined by the cypherpunks (Campbell-Verduyn, 2018a; Swartz, 2017). The financial services industry’s (Campbell-Verduyn & Goguen, 2018, pp. 8–9) and startups’ involvement with the technology has led to a range of blockchain projects, which range from being radical to rather incorporative (Swartz, 2017). Despite ideological differences (Swartz, 2017), these projects have a common understanding of blockchain platforms as mutually shared infrastructures. Therefore, information systems research unifies them under one terminological umbrella:

Blockchain technology refers to a fully distributed system for cryptographically capturing and storing a consistent, immutable, linear event log of transactions between networked actors. This is functionally similar to a distributed ledger⁸ that is consensually kept, updated, and validated by the parties involved in all the transactions within a network. In such a network, blockchain

⁸ Blockchain technology is also often referred to as Distributed Ledger Technology (DLT) as similar platforms exist, which maintain the shared ledger without bundling transactions into blocks. This work, however, investigates platforms which use blockchain technology.

technology enforces transparency and guarantees eventual, system-wide consensus on the validity of an entire history of transactions. (Risius & Spohrer, 2017, p. 386)

At first glance, this definition appears to be an abstraction of Bitcoin's logic as described in sub-chapter 2.1. However, it does allow for a technological differentiation between permissionless⁹ and permissioned, public and private blockchain platforms (Beck et al., 2018; Peters & Panayi, 2016, pp. 244–246), which represents the ideological divide of radical versus incorporative blockchain projects (Swartz, 2017). The differentiation of permissions and privacy refer to the permission requirements for nodes to participate in transaction verification, and to the accessibility of blockchain transactions (Beck et al., 2018). Bitcoin and Ethereum are permissionless blockchain platforms, as all nodes are allowed to participate in its transaction processing (Peters & Panayi, 2016, 244-245). Moreover, they are public because anyone can conduct transactions on the system and there are no access limits for the transaction ledger. Incorporative blockchain platforms, like Hyperledger Fabric, are often permissioned, which means they restrict transaction validation to pre-selected nodes (Peters & Panayi, 2016, pp. 245–246). They also tend to be private in that they restrict data accessibility and the rights to propose transactions to specific parties in the network (Peters & Panayi, 2016, p. 244). Nevertheless, permissioned blockchain platforms can be public in principle (Beck et al., 2018). I will come back to these categories at later parts of this study (2, 5, 6).

Together with the discursive turn towards blockchain technology emerged programmable multi-purpose blockchain platforms applicable towards ends other than payment. Ethereum led the way in this regard (Swartz, 2017, p. 85). Such programmability relies in many cases on so called smart contracts and encoded agreements (Peters & Panayi, 2016, pp. 246–247), which were first described by computer scientist Nick Szabo (1994, 1997). A simple example would be a rule to pay out an amount of money under certain conditions (Peters & Panayi, 2016, p. 246), e.g. a flood insurance payment based on the measure of high water. Smart contracts are also experimented with to create and trade digital value tokens that are based on multi-purpose blockchains (F. Glaser, 2017, p. 1549), create digital marketplaces (Risius & Spohrer, 2017, p. 398), conduct transactions in the Internet of Things¹⁰ (Risius & Spohrer, 2017, p. 390), operate logistics process such asset tracking and financing, and experiment with algorithmic governance (DuPont, 2019). Although smart contracts can impact our

⁹ Permissionless blockchain platforms are also referred to as “unpermissioned” blockchain platforms. I use the terms interchangeably.

¹⁰ Internet of Things (IoT) refers to networks of physical objects exchanging and processing information over the internet.

practices of contracting and vice versa (DuPont, 2019; Werbach, 2018) and despite the misleading term contract (DuPont & Maurer, 2015) and blockchain enthusiasts' claim that "code is law" (Risius & Spohrer, 2017, p. 390), smart contracts cannot not really be understood as contracts. Smart contracts constitute fixed rules with the intention to automate business logic and exclude ambiguity instead of mediating conflict in cases of ambiguity (DuPont & Maurer, 2015, p. 9). They turn out to rather be the technical foundation for programming the application logic, which can be used by business and for other purposes on blockchain platforms (F. Glaser, 2017).

This sub-chapter has shown that, as Bitcoin and the broader technology on which it is based have emerged, they have begun to create and influence socio-technical worlds. However, one relational element that Bitcoin claimed to avoid was trust, as I have briefly touched upon in sub-chapter 2.1. Although not yet considered in organizational trust research, anthropologists, economists, information systems researchers, social scientists, and legal scholars have dealt with the linkages between blockchain technology and trust. In the following I outline their considerations.

2.3 What does trust have to do with it?

As indicated above, a linkage to trust is essential to the origins of Bitcoin. A glance at recent blockchain literature indicates that this linkage between Bitcoin and trust is complex. One finds the assumption that Bitcoin replaces trust while also holding the conviction that Bitcoin's algorithm is trusted and capable of creating trust. Such beliefs hold the Bitcoin community and the cryptocurrency together. On the other hand, Bitcoin's socio-technical world renders trust between its constituent actors visible. It stands to reason that this complexity persists in other blockchain platforms as well.

Bitcoin arose from a context of skepticism towards the financial industry and public institutions, which forfeited trust over the course of the financial crisis (0). Thus, a prevailing narrative of the Bitcoin community is that Bitcoin is "trustless" (Musiani et al., 2018, p. 133) or "trust-free" (Dodd, 2018, p. 35). This means users do not have to trust each other or an established institution in order to rely on Bitcoin as money or the Bitcoin system to perform transactions. This narrative lives on in management information systems research, where blockchain technology is often introduced as a trustless or trust-free system (Beck, Stenum Czepluch, Lollike, & Malone, 2016; F. Glaser, 2017; Hawlitschek, Notheisen, & Teubner, 2018; Notheisen, Cholewa, & Shanmugam, 2017). The term trustless is also used in business studies (van Rijmenam, Schweitzer, & Williams, 2017).

However, scholars increasingly question the notion of a trustless Bitcoin and blockchain technology, observing trusting relations within their socio-technical worlds (Campbell-Verduyn & Goguen, 2018; DuPont, 2014; F. Glaser, 2017; Hawlitschek et al., 2018; Mallard, Méadel, & Musiani, 2014; Risius & Spohrer, 2017; Weber, 2016). Bluntly said: “Whoever Satoshi was, one thing is clear: He, or she, or they, were dead wrong. Trust is central to Bitcoin, as well as to the wave of blockchain [...] solutions following its approach” (Werbach, 2018, p. 17). As Nelms et al. (2018) observe, Bitcoin produces trust between its users on the basis of algorithms:

For Bitcoin users, trust is established by code, through the blockchain and its cryptography. Since trust emerges out of the machine, so to speak, Bitcoin users don’t see it as a political or social arrangement, and relationships between individuals appear to be unmediated, wholly independent of any third party. (Nelms et al., 2018, p. 24)

In accordance with the skepticisms towards established financial and governmental institutions, Bitcoin users repeatedly claim that they trust mathematics and Bitcoins’ algorithms more than the above mentioned institutions (Lustig & Nardi, 2015, p. 748; Nelms et al., 2018, pp. 20–22).

What Werbach (2018) calls trustless trust intends to replace trust in individuals and in institutions with trust in algorithms – the assumption being that algorithmic output is trustworthy even if users are not (pp. 28–29). Bitcoin users believe in algorithms and numbers (Nelms et al., 2018, p. 21) although few understand how they work (Dodd, 2018, p. 52). Bitcoiners replace the U.S. banknote maxim “in God we trust” with “in proof we trust” (Werbach, 2018, p. 29) or “in digital we trust” (Baldwin, 2018). Maurer et al. (2013) argue that this trust is the revolutionary aspect of Bitcoin:

Trust in the code substitutes for the (socially and politically constituted) credibility of persons, institutions, and governments. It is this – not the anonymity or the cryptography or the economics – that makes Bitcoin novel in the long conversation about the nature of money. (Maurer et al., 2013, p. 263)

This trust relies on the intended characteristics of Bitcoin, such as its decentralized operations through independent computational nodes as well as the social relations, which constitute a socio-technical network. Bitcoin elicits trust from users in the system by making the algorithms which run the system open source and thus predictable (Lustig & Nardi, 2015, p. 750; Maurer et al., 2013, p. 263). On the other hand, only few users can read the code and know who can make changes and how this might be accomplished (Mallard et al., 2014, p. 5). Moreover, Bitcoin’s intended distributed operation on multiple computer nodes diffuses users’ trust from a single institution across a vast network (Weber, 2016, p. 29). What

enhances trust is its materiality, which arises from the computational work of mining (Maurer et al., 2013). The mining process with the proof-of-work consensus algorithm is understood as a “source of trust for the network in its entirety” (Mallard et al., 2014, p. 5). However, today’s actual centralization of Bitcoin mining activities in mining pools compromises this basis of trust (Dallyn, 2017, p. 470; Dodd, 2018, p. 46). Information systems research also questions whether proof-of-work applied to accountings systems is able to prevent fraud (Rückeshäuser, 2017). Code is vulnerable and thus cannot work without trust (Werbach, 2018, p. 31).

Researchers suggest that complementary mechanisms are at play when it comes to users’ trust in Bitcoin’s algorithms and the bitcoin cryptocurrency. Bitcoin’s exchange rate is commonly read as an indicator of users’ trust and mistrust in the cryptocurrency, and hence its volatility is often seen as a weakness (Campbell-Verduyn & Goguen, 2018, pp. 11–12; Mallard et al., 2014, p. 7). The value of bitcoins can be explained by the community’s shared belief in Bitcoin as an alternative currency system (Dallyn, 2017). Dodd (2018) escalates this thought by arguing that the community’s shared belief of Bitcoin replacing social relations, combined with trust with algorithms, assembles the community and the cryptocurrency. Though this belief, he argues, “is a fiction” (Dodd, 2018, p. 37).

On the other hand, Weber (2016) argues that Bitcoin users implicitly trust each other in their peer-to-peer trading practice, as Bitcoin has no chargeback feature (pp. 29–30). Although bitcoins are produced and processed by algorithms, its users show a community spirit, which engenders trust in the currency. This can be observed at frequent community meetings as well as intensive online communication in forums and calls (Dodd, 2018, p. 47). Moreover, in a case where a majority of Bitcoin miners ran different software updates than users of Bitcoin, Bitcoin miners colluded at the recommendation of Bitcoin developers to re-synchronize miners and users; this action against the algorithm was perceived as legitimate (Lustig & Nardi, 2015, p. 749; Musiani et al., 2018). The case exemplifies the required trust of users and miners in developers of the open source code (Mallard et al., 2014) of public blockchains. DuPont (2018) describes a similar case with the Ethereum platform where its inventor, Vitalik Buterin, other developers from the team, and the community resolved an unexpected exploit of cryptocurrency funds by jointly manipulating the platform. In this case, trust was needed (Werbach, 2018, p. 69) when “hell broke loose” (p. 67). Thus, Campbell-Verduyn and Goguen (2018) suggest that disputes on Bitcoin’s and Ethereum’s governance “[shift] rather than [eliminate] trust and distrust in elite-led governance” (p. 12).

Coming back to Bitcoin, research suggests that users trust the algorithms, the computational network, the cryptocurrency, and the developers. It also proposes that miners

rely on developers. Many also claim that there are other actors related to Bitcoin, which are implicitly trusted by users. These actors include financial services and vendors, which trade bitcoins for other cryptocurrencies and for national currencies (Campbell-Verduyn & Goguen, 2018); there are also digital wallets for transferring cryptocurrencies (Böhme et al., 2015, pp. 220–221); a number of privacy intermediaries, which obfuscate transaction flows, and also regulators which have entered the space (Mallard et al., 2014) since 2013 (0). With regard to Ethereum, DuPont and Maurer (2015) mention a browser interface, which can elicit trust through its standard structure and “symbols of trust” (p. 5). Trust to the newly arising actors makes users again “vulnerable to trust abuse which might strike back on the system’s legitimacy” (Weber, 2016, p. 37). Weber (2016) warns against the discouraging effects of Bitcoin’s pseudonymity on trust building within the Bitcoin community and towards other actors (p. 27). Meanwhile, other scholars observe several practices, bodies of knowledge, and interfaces as bases for trust in blockchain systems, in cryptocurrencies, and in other actors in the system. Users’ trust in the Bitcoin system as well as its related services and vendors were built through users’ regular reading of online information, communication among users, and the sharing of experiences (Lustig & Nardi, 2015). On the other hand, the high amount of formal and informal information and communication has led to misconceptions which can lead to uncertainty (Mallard et al., 2014, p. 5). Lustig and Nardi (2015) describe how users spent several hours a day reading online communication to keep up to date with debates and practices regarding the above mentioned actors. From these interactions they gained knowledge about how to assess the trustworthiness of service providers and how to store their cryptocurrencies safely (Lustig & Nardi, 2015, pp. 748–749). Sharing of information (Lustig & Nardi, 2015, p. 749) and responsibility (Mallard et al., 2014, p. 7) by service providers was perceived as trust-enhancing. Although people came up with new software and hardware devices to store bitcoins (Mallard et al., 2014, p. 4), users struggled with understanding how to prevent theft (Lustig & Nardi, 2015, p. 749) – something which endangered users’ trust in the Bitcoin system as a “repository of value” (Mallard et al., 2014, p. 4). However, multiple cryptocurrency exchanges have failed in protecting their users’ bitcoins and increased the vulnerabilities of the overall system. Such technical vulnerabilities and hacks bolster the public’s distrust in cryptocurrencies (Campbell-Verduyn & Goguen, 2018, p. 11). Similarly, the question concerning how to ensure privacy has had influence over users’ trust in the system. As Bitcoin’s privacy characteristics were deficient (De Filippi, 2016), new privacy intermediaries arose, which again required trust from its users. It was stated that the more knowledge on cryptographic techniques and peer-to-peer-networks users had, the more they

would be able to assess the abilities of the system (Mallard et al., 2014, p. 6). Finally, implicit public governance and explicit regulations are bases for users' trust in Bitcoin. Weber (2016) hints that when Bitcoin users' store bitcoins on their own hardware, they signal implicit trust in established institutions – such as governments – to protect their property (p. 30). Moreover, some community members and experts advocated explicit criminal prosecution of intermediaries as well as dedicated research and debates on regulatory authorities within the socio-technical world of Bitcoin; these were also carried out in order to distance Bitcoin from illegal activities and thus to enhance its legitimacy, (Böhme et al., 2015, pp. 230–232; Lustig & Nardi, 2015, p. 750), normalization (Hütten & Thiemann, 2018), and integration with the “real world” (Mallard et al., 2014, p. 8).

Overall, blockchain literature has begun to investigate the linkage of Bitcoin and trust. However, at the time of this writing, references to programmable blockchain platforms are scarce. This is true with regard to both radical and more incorporative blockchain projects. Nelms et al. (2018) suggest that “the blockchain was seen as a way to extend Bitcoin’s theory of (non)trust to any kind of contractual or financial interaction” (p. 22). The trustless trust narrative about the production of collective trust through algorithms has its supporters (Werbach, 2018). On the other hand, programmable blockchains with smart contracts might not be able to replace the social dynamics of trust in business (DuPont, 2019, p. 207).

After having introduced Bitcoin, programmable blockchain technology, and Bitcoin’s linkages to trust, it seems that the role of trust in blockchain technology is also multi-faceted. I will explore this phenomenon in more detail in my empirical work (5, 6). First, in the following chapter (3), I outline my theoretical perspectives and sketch out gaps in the organizational trust literature to which my research on blockchain technology makes a contribution.

3 Trust and technology

In the previous chapter I described that Bitcoin and trust are interrelated in multiple ways. It seems there is also a complex interrelation between trust and the blockchain technology used by business organizations. Consequentially, a discussion about blockchain technology and trust warrants a review of the scientific discourse on trust in organizational studies. I start this chapter with a brief introduction to organizational trust research (3.1.1), followed by an introduction to the integrative trust framework developed by Guido Möllering (2006a) (3.1.2). As the name suggests, the latter critically integrates multiple streams of trust research. Following this perspective allows me to approach the phenomenon blockchain technology from a trust perspective and to discuss its implications for organizational trust research in the remainder of my work. In a next step, I describe the role of information technology as a trustee and trust facilitator, which allows me to outline several research gaps (3.1.3). Research in organization studies on trust in information technology is rather scarce. Not to mention, it is curious that trust research in other academic disciplines, such as information systems research, does not attribute agency to information technologies and does little to consider the processual character of trust. To complement these perspectives, I incorporate Actor-Network Theory – especially the notion of translation – as a theoretical lens in my work. I introduce the concept in sub-chapter 3.2.1 and thereafter discuss the ways in which translation studies do and do not already touch upon trust. Following this, I deduce my empirical research questions for the analysis of blockchain technology (3.2.2).

3.1 Trust

3.1.1 Organizational trust research

Trust is a diverse concept which has been already discussed by philosophers and political scientists for centuries (Möllering, Bachmann, & Hee Lee, 2004). In organizational and management studies, a vast academic discourse on trust has emerged since the 1960s (Lyon, Möllering, & Saunders, 2015). The First International Network on Trust (FINT) and a standing working group (SWG) at European Group for Organizational Studies (EGOS) have played important roles in assembling an organizational trust research community over the past decades.

Trust research is of vital importance to organization studies, as trust has effects on organizing. Although some scholars attribute trust to negative economic effects (Jeffries & Reed, 2000; Langfred, 2004), experiences, and behaviors (Skinner, Dietz, & Weibel, 2013),

the trust discourse foregrounds the positive effects trust can have on organizing (Sydow, 2006, p. 377). For example, trust can enhance information sharing, increase performance in inter-organizational exchange relations, lower transaction costs (Dyer & Chu, 2003; Sako, 1998; Zaheer, McEvily, & Perrone, 1998), and serve as an organizing principle (McEvily, Perrone, & Zaheer, 2003). Trust is necessary for inter- and intra-organizational exchange relations which occur within an increasingly globalized and connected business context (Lane, 1998; Stevens, MacDuffie, & Helper, 2015).

For more than a decade, there has been a latent ontological shift from trust-as-attitude toward trust as a process of embracing a leap of faith (Li, 2017). This means that organizational trust research interprets trust not just as an attitude based on the perceived trustworthiness of an actor, but expands its view towards the choices and actions of trusting as well as the respective social processes leading to and resulting from trust. Despite this shift, the organizational research community has by no means agreed on a universal definition of trust. To the contrary, trust is rather differentiated, e.g. by bases (Möllering, 2006a), by levels (Bachmann & Zaheer, 2006a; Fulmer & Gelfand, 2012), or by contexts (Höhmann & Welter, 2005). Research also discusses trusts' dualities and relations to other concepts like distrust (Bijlsma-Frankema, Sitkin, & Weibel, 2015; Saunders, Dietz, & Thornhill, 2014; Walgenbach, 2001), power (Bachmann, 2001; Hart & Saunders, 1997), or control (Costa & Bijlsma-Frankema, 2007; Möllering, 2005). But there is some common ground for these trust concepts. For instance, vulnerability and uncertainty are essential attributes of trust. By trusting, one party remains vulnerable to the potential actions of the other (Mayer, Davis, & Schoorman, 1995; Rousseau, Sitkin, Burt, & Camerer, 1998). This does not imply accepting violations or disappointments (Möllering, 2006a, p. 8), but coping with uncertainty in social relationships (Gambetta, 1988; Luhmann, 1979). While vulnerability and uncertainty are defining characteristics of trust, trust is also capable of decreasing complexity (Luhmann, 1979) and to a certain extent bridging uncertainty (Simmel, 1950). This implies a perspective – which is not shared by all scholars – of trust as a social mechanism which can be actively shaped. These characteristics also explicate the so-called trust paradox: “Trust is abundant when it is not needed, but trust is hard to find when it is needed” (Li, 2017, p. 9). This paradox gets to the heart of the interdependence between trust, uncertainty, and vulnerability. If uncertainty and vulnerability are high, it is difficult to take a leap of faith and trust; at the same time, it is under such conditions when trust is most required. Where certainty is high, the disposition to trust is often high, yet not required.

Trust involves at least two parties: The trustor and the trustee (Möllering, 2006a, p. 3; Rousseau et al., 1998) or, in other words, a subject of trust and an object of trust (Nooteboom, 2002, p. 10). The trustor places trust in the trustee. By doing so, the trustor makes herself vulnerable to the potential actions of the trustee. This relationship can be unilateral or bilateral. While this relation can involve a direct linkage between trustor and trustee, social relations can also involve additional trust-facilitating entities. Figure 1 illustrates with arrows the trust relations between trustor, trustee, and facilitator in a unilateral trust relationship.

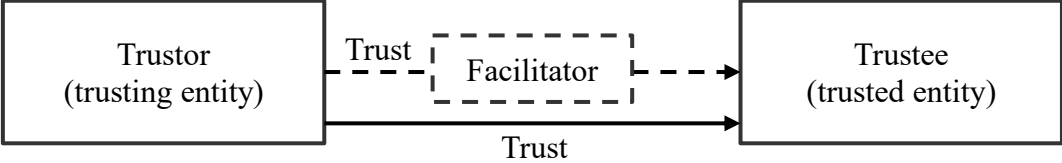


Figure 1: Trustor, trustee and facilitator (own illustration).

While envisioning entities helps establish analytical clarity, the relation between trustor and trustee is more relevant to trust research than the entities themselves (Nooteboom, 2002, p. 8). This is because trustor and trustee interact and mutually influence each other through their actions (Möllering, 2006a, p. 8). Trust is therefore a characteristic of the social relation between trustor and trustee (Nooteboom, 2002, p. 8). Uncertainty, as described above, stems from the agency of the entities involved. Their ability to act unexpectedly, or to even violate the trustor’s trust, entails uncertainty and vulnerability on behalf of the trustor (Lane, 1998; Luhmann, 1979; Möllering, 2006a; Rousseau et al., 1998).

These abstracted notions of entities, trustors, trustees, and their relations to one another should not obscure the different organizational levels of analysis addressed within trust research. Trust exists on interpersonal, intra-organizational, inter-organizational, and institutional and societal levels; it is also a multi-level phenomenon (Bachmann & Zaheer, 2006b, 2013; Currall & Inkpen, 2006; Möllering et al., 2004). This means that persons, groups, and organizations can trust and be trusted (Currall & Inkpen, 2006; Fulmer & Gelfand, 2012). Institutions or social systems shape how trust is formed in relation to various entities – either as a context (Bachmann & Inkpen, 2011; Zucker, 1986) or facilitator (Zucker, 1986) for trustors and trustees. On the other hand, institutions and social systems are themselves trustees (Möllering, 2006b). The latter circumstance is often conceptualized with Luhmann’s (1979) and Giddens’ (Giddens, 1990) “system trust”. The relations between these different constructs are also a matter of trust research. In inter-organizational relations, for

example, trust in a member of another organization is related to trust in the respective organization (Zaheer et al., 1998).

Over the past years, the influence of context on trust has become a more important aspect of trust research (Li, 2017). Several examples draw on culture (Saunders, Skinner, Dietz, Gillespie, & Lewicki, 2010) as a context: National institutions in cross-border relations constitute contexts for intra-organizational trust (Child & Möllering, 2003) and inter-organizational trust (Lyon & Porter, 2010), as do cross-cultural negotiations (Kramer, 2010), cultures of individualism (Huff & Kelley, 2003), and cultural distance (Li, 2013). Entrepreneurship (Höhmman & Welter, 2005; Welter, 2012), alliances, networks (Das & Teng, 2001; Sydow & Windeler, 1998), and politics (Hardin, 2013) are also considered to be contexts in which trust plays a crucial role (Li, 2017). The internet or cyberspace is another, yet undertheorized, context where trust is central (van der Werff, Real, & Lynn, 2018; Zand, 2016). The relation of trust to other theoretical concepts such as control, power, or distrust is of similar importance. Organizational trust research investigates the levels, contexts, and ways in which trust intertwines with control (Bijlsma-Frankema & Costa, 2005; Costa & Bijlsma-Frankema, 2007; Das & Teng, 2001; Möllering, 2005), power (Bachmann, 2001), and distrust (Bijlsma-Frankema et al., 2015; Cook & Kramer, 2004; Gambetta, 1988; Kramer, 1999; Lewicki, McAllister, & Bies, 1998; Saunders et al., 2014; Zand, 1972). While most trust studies implicitly assume that trust is advantageous for all actors involved, researchers have also recently investigated the “dark side of trust” (Skinner et al., 2013), i.e. the negative implications and consequences of trust.

There is also a sub-discourse on trust repair (Dirks, Lewicki, & Zaheer, 2009; Gillespie & Dietz, 2009; Gillespie & Siebert, 2018; Kramer & Lewicki, 2010), which has been fueled by the 2008 financial crisis (Bachmann et al., 2015; Gillespie & Hurley, 2013). Research in this regard is motivated by the decrease of public trust in institutions such as governments and business over the past decades, which has become more severe during and after 2008 financial crisis (Bachmann et al., 2015; Gillespie & Hurley, 2013; Harris, Moriarty, & Wicks, 2014; Uslaner, 2014). With its investigation of organizations’ active trust repair mechanisms, this research is embedded in a general turn within organizational trust research towards active trust building. Bachmann et al. (2015) synthesizes six mechanisms of organizational and institutional trust building in the wake of damaged trust: “Sense-making, relational, regulation and control, ethical culture, transparency and transference” (Bachmann et al., 2015, p. 1125). Such trust repair mechanisms draw upon underlying trust building mechanisms such as “collective learning”, “remorse and redemption”, “formal control”, “informal control”,

“information sharing and accountability”, and “reputation spill-over” (Bachmann et al., 2015, p. 1126). However, the emergence of blockchain technology in conjunction with cryptocurrencies since 2008 has received little attention in organizational trust research until now. This may be due to the fact that trust in general information technologies in organizational studies is undertheorized (van der Werff et al., 2018). I elaborate on this point later (3.1.3). Next, I introduce the integrative trust framework by Möllering (2006a), which will serve multiple functions in my empirical analyses and theoretical discussions (5, 6, 7).

3.1.2 Möllering’s integrative trust framework

Möllering’s (2006a) integrative trust framework will play a central role in my work. On the one hand, the trust categories it outlines provide a theoretical lens for the exploration of an emerging blockchain technology. Its comprehensiveness as well as its emphasis on the processual character of trust enhances established theoretical perspectives on trust in information technology. Further, Möllering’s integrative trust framework represents a significant part of the overall literature on trust in organization studies to which the findings of my analysis will contribute. Möllering’s (2006a) framework critically incorporates different streams of trust literature into a multi-perspective framework. As such, it provides a holistic understanding of trust, regardless of the organizational level or context that it might apply to. Moreover, it relates trust to different trust building mechanisms and bases for trust. I agree with Möllering’s (2006a) aspiration that “trust research needs to be broad, applying multiple perspectives in order to form a picture of the enormous elephant called trust, as in the classic Indian fable” (p. 105). The following definition of trust considers the underlying processes of trust building as well as the state of trust itself:

Trust is an ongoing process of building on reason, routine and reflexivity, suspending irreducible social vulnerability and uncertainty *as if* [italics in original] they were favourably resolved, and maintaining thereby a state of favourable expectation towards the actions and intentions of more or less specific others. (Möllering, 2006a, p. 111)

This definition positions remaining vulnerability and uncertainty as the circumstances that makes trust necessary in social relations. In other words, without uncertainty there would be no need to trust. A defining element of trusting is the suspension of uncertainty and vulnerability or leap of faith – it is an act of bridging uncertainty. For example, to work with somebody whose actions are not fully controllable or foreseeable implies the suspension of any remaining uncertainty, i.e. trust. The emphasis of trust as a continuous and reflexive process stresses another important aspect of this trust definition. As it projects an understanding of trust as something that develops over time, this definition highlights how

trust is actively shaped by those who participate in the trust building process. At the time of its publication, Möllering's (2006a) emphasis on these two aspects – the leap of faith and trust as a process – marked important contributions that supported an ontological shift in theoretical discourse on trust in organizational studies (Li, 2017; Nooteboom, 2006). This ontological shift moves organizational trust theory beyond an understanding of trust as a rational attitude, and moves it toward an understanding of trust building as a reflexive process and trust expressed through choices and actions.

Bases for trust are “reason, routine and reflexivity” (Möllering, 2006a). Such a focus incorporates various streams of trust research. Reason refers to rational choice in social and economic theory. It often goes hand in hand with calculativeness, e.g. as in game theory (Möllering, 2006, p. 4, 2006, pp. 25–26). Routine includes rules, roles, and habits that facilitate trust between actors, also referred to as institutional-based trust (Zucker, 1986); these mechanisms are often trusted themselves (Möllering, 2006a, pp. 51–54). Reflexivity refers to processes of active trust building in personal interactions between trustor and trustee, such as familiarization, mutual openness, and favorable anticipation of trustees' actions (Möllering, 2006a, pp. 98–100). Reason, routine and reflexivity can also be paraphrased as “cognition, taken-for-grantedness [and] communication loops” (Möllering, 2006a, p. 105). Figure 2 illustrates these bases for trust and their interplay with the leap of faith (suspension of uncertainty and vulnerability) which leads to trust.

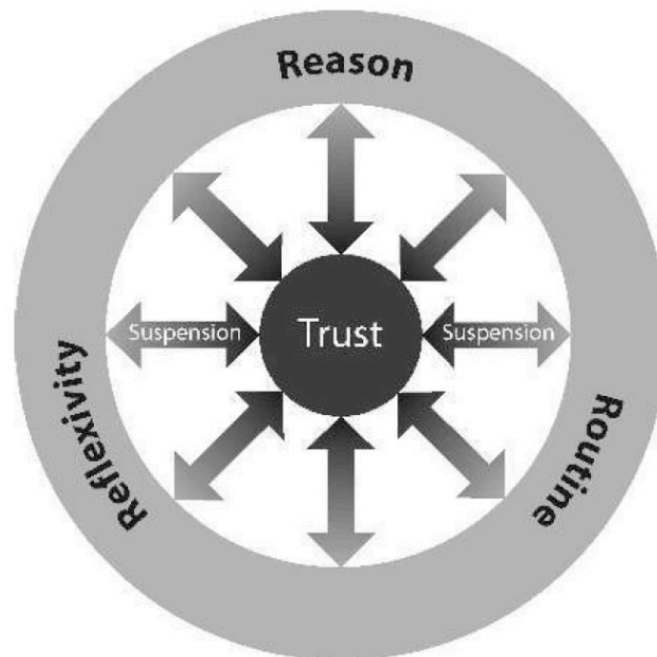


Figure 2: The trust wheel – an integrative framework (Möllering, 2006a, p. 110).

The framework illustrates that these three bases for trust should not be confused with trust itself, but are rather trust building mechanisms which are influenced by trust and by each other. The leap of faith, also referred to as suspension of uncertainty and vulnerability, is the element required when speaking about trust and to achieve trust upon these three bases (Möllering, 2006a, pp. 110–111). In the following, I explain each element of the integrative framework, along with its respective stream of theory in more in detail.

Leap of Faith

With the leap of faith Möllering (2006a) recalls a construct Simmel (2004) implicitly put forth at the beginning of the 20th century, which was later taken up by various other authors (Giddens, 1990; Lane, 1998; Luhmann, 1979; Möllering, 2001; Zaheer et al., 1998). Within the integrative framework, this leap of faith is the essential element for describing how trustees deal with uncertainty. Möllering (2006a) quotes Simmel (2004), according to whom trust is a combination of vague “inductive knowledge” and “socio-psychological quasi-religious faith” (p. 178). It is important to note that the leap of faith is a concurrence of both of these elements mentioned by Simmel. Inductive knowledge alone – e.g. a peasant’s confidence of a bountiful harvest (Simmel, 2004, p. 178) – is a kind of trust, but not necessarily a leap of faith (Möllering, 2006a, p. 109). A more indicative example was given by Tillmar and Lindkvist (2007). They discuss how starting a business cooperation in the remote context Tanzania, which had little support from formal institutions, a combination of faith and knowledge allowed for a gradual suspension of uncertainty. Interestingly enough, Simmel (2004) touches on trust with regard to money’s role in economic interactions. Economic exchange that relies on money requires a leap of faith by the involved parties, who have to assume that the value of the money persists within the community. Providing credit implies believing in the debtor to pay back the borrowed money.

Economic credit does contain an element of this supatheoretical belief, and so does the confidence that the community will assure the validity of the tokens for which we have exchanged the products of our labour in an exchange against material goods. (Simmel, 2004, p. 178)

There are several action patterns, which explain how trustors compensate for uncertainty by taking a leap of faith: (1) As-if behavior, (2) bracketing, and the (3) will to believe (Möllering, 2006a, p. 111). With as-if behavior, trustors compensate missing information with fiction (Möllering, 2006a, p. 115). This allows them to cope with the uncertainty inherent in all actions that take a possible future into consideration (Möllering, 2006a, p. 112). Trustors fill these information gaps. This behavior has several peculiarities, such as idealizing the

trustee, interacting as if the trustee is trustworthy, or taking the trustee and one's trust in it for granted (Ortmann, 2004). Trust in the form of as-if behavior can draw upon reason and reflexivity. The trustor and trustee can jointly create an image of the trustee as a trustworthy actor where "the trustee's performative acts and a high level of familiarity with the situation merely assist the trustor in making the leap of faith" (Möllering, 2006a, p. 114). This has been the case, for example, with R&D team leaders whose engagement in leadership practices evoked their team members to trust them (Gillespie & Mann, 2004).

With bracketing, actors do not compensate for missing information, but actively ignore information gaps and uncertainty, which allows them interact in spite of these things (Möllering, 2006a, p. 115). Möllering (2006a) summarizes that

actors interact with each other as if ignorance, doubts and dangers that exist alongside knowledge, convictions and assurances are unproblematic and can be set aside, at least for the time being [...] Specifically, they bracket out irreducible social vulnerability and uncertainty as if they were favourably resolved. (Möllering, 2006a, p. 115)

Möllering (2006a) attributes to bracketing the idea of "just [doing] it" (p. 118), which gives the notion a practical dimension. By acting, trustors often bracket out missing information unconsciously, take smaller or bigger leaps of faith, and feel anxiety or not (Möllering, 2006a, p. 118). Bracketing has been empirically observed, especially in the context of medical care. For example, some patients facing surgery bracketed potential risks (Bernstein, Potvin, & Martin, 2004), or expressed a just-do-it attitude (McKneally, Ignagni, Martin, & D'Cruz, 2004; Möllering, 2006a, p. 122).

In turn, the "will to believe" (James, 1948) is "a conscious leap of faith" (Möllering, 2006a, p. 121). This is best illustrated by someone who deliberately jumps over a crevice with the uncertainty of whether she will reach the other side. It is not a fatuous action, but rests on a faith which the trustor (the person jumping) feels is right (Möllering, 2006a, p. 121). According to James (1948), trustors have "the right to believe at [their] own risk any hypothesis that is live enough to tempt [their] will" (p. 107). The term hypothesis reflects that trust in somebody or something is uncertain and can turn out to be unsound. However, the belief appears plausible to the trustor (Möllering, 2006a, p. 121), and is not confounded by strict rationality. In his reflections on the will to believe, James (1948) discusses religion and men's faith in God in particular (p. 107). The existence of God is the hypothesis in which people believe. They trust God to exist and do not wait for ultimate proof, something which would hinder them from acting (James, 1948, p. 107). Möllering (2006a) stresses this

connection between faith and action by James (1948) and extrapolates it to a more general level of analysis:

Faith means belief in something concerning which doubt is still possible; and as the test of belief is willingness to act, one may say that faith is the readiness to act in a cause the prosperous issue of which is not certified to us in advance (Möllering, 2006a, p. 22).

The will to believe also softens the apprehension of the trustee. While studies in organizational research tend to specify trust in individuals, teams, organizations (Fulmer & Gelfand, 2012) or institutions and systems (Bachmann & Inkpen, 2011), the will to believe refers to trustees as “more or less specific others” (Möllering, 2006a, p. 111).

Overall, the leap of faith materializes in actions where trustors consciously or unconsciously suspend uncertainty. In the description of Möllering’s integrative trust framework, trustors are primarily people or groups of people, such as teams. While as-if behavior and bracketing primarily refer to trust in people or social systems, the will to believe reflects a broader trust to ideas or the good outcome of a particular action. This broad understanding of trust should be kept in mind during the review of trust literature, which draws on reason, routine and reflexivity – three aspects which Möllering (2006a) considers to be bases of trust rather than trust itself.

Reason

Trust is based on several aspects that are incorporated into the leap of faith: Reason, routine, and reflexivity. A study on buyer-supplier relationships is illustrative for the comprehensiveness and concurrency of these three bases for trust (Möllering, 2006a, pp. 155–189). According to Möllering (2006a), reason is paradoxical given how rationalist trust theory “explains trust away” (p. 43). Nevertheless, it is important to briefly reflect on the role of reason in this chapter; most importantly, because it provides insights to the trust perspective that underpin some of the statements about trust made by those who build and promote blockchain technology.

From a rationalist perspective, trust is a rational choice based on the perceived trustworthiness of a rational actor. It is reasonable to trust somebody or something if that actor is perceived as trustworthy. This assumption has been emphasized in several economic theories, such as principle-agent theory (Eisenhardt, 1989; James Jr., 2002; Sheppard & Sherman, 1998), game theory (Axelrod, 2006; Deutsch, 1973; Luce & Raiffa, 1967), transaction cost theory (Williamson, 1983, 1991), and signaling theory (Bacharach & Gambetta, 2001). Moreover, one of the most cited definitions of intra-organizational trust – the “willingness to be vulnerable to the actions of another party” – builds on the assumption

that indicators of trustworthiness are determinants for decisions to trust (Mayer et al., 1995). Research on trustworthiness indicators has found a variety of indicator sets related to ability, benevolence, and integrity (Mayer et al., 1995), or competence, benevolence, honesty, and predictability (McKnight, Cummings, & Chervany, 1998). In this context, ability is the trustee's situation specific competence, benevolence is the trustee's perceived goodwill towards the trustor, and integrity is the trustee's perceived adherence to principles that the trustor finds acceptable (Mayer et al., 1995, pp. 716–720). Regardless of the specific indicators, trustworthiness indicators propose that trust is reasonable when someone is perceived “able and willing and consistent in not exploiting the trustor's vulnerability” (Möllering, 2006a, p. 48).

In transaction cost theory, trust is considered through the lens of reduced transaction costs, e.g. transaction partners are deemed trustworthy in cases when they are not perceived as opportunistic. The perception of not being opportunistic prompts the other actor to reduce precautionary, control, and defensive measures which in turn reduces transaction costs (Möllering, 2006a, pp. 26–29). Principal-agent theory implies a trust relationship between principle and agent as well, although it claims to limit an interference of trust. A principle is a trustor who assigns a task to a trustee. She secures her interests by aligning the trustee's interests with her own, e.g. through incentives that should eliminate uncertainties and thus also the need for trust. However, Möllering (2006a) has argued that the principle-agent relationship is never perfect, and that uncertainties and a need for trust remain (pp. 29–32). In signaling theory, trust is a matter of showing and perceiving signals about one's trustworthiness. Optimally, the cost of signals are low for the trustworthy and high for the untrustworthy – such an incentive is thought to make the signal more confinable (Möllering, 2006a, pp. 41–43). Game theoretical studies on trust have a common ground in that they study strategies of cooperation between actors, assuming that this cooperation involves trust. A calculative understanding of trust is inherent to game theoretical approaches, as game theory emphasizes the paying out of strategies. An actor decides to trust in another if she expects a positive result for herself. This comes under the assumption that the other actor also rationally seeks for a positive individual outcome (Möllering, 2006a, pp. 40–41). Overall, rationalist economic theories struggle with conceptualizing trust since they aim to reduce uncertainties in economic relations. They do so by proposing incentives, calculative approaches, and rational arguments to evaluate the trustworthiness of actors. Moreover, they seek for mechanisms and actors that can guarantee or execute agreements that assure trust (Möllering, 2006a, p. 60). This explains how uncertainty is reduced, but does not explain how remaining uncertainty is

dealt with. Therefore, such an approach rather “[explains] trust away” (Möllering, 2006a, p. 43) and appears to have limited relevance for organizational trust research (Möllering, 2005). On the other hand, Möllering’s integrative trust framework acknowledges that calculative approaches and those based on reason are foundations from which trustors take leaps of faith. In light of my study of computational artefacts and organizations that produce algorithms, it seems important to bear in mind that trust concepts in computer sciences have a rationalist notion as well. Trust in computer science often implies low or no vulnerability (van der Werff et al., 2018, p. 400), instead of stressing the need to cope with remaining uncertainty.

Routine

The routine category in Möllering’s integrative framework comprises institutions and systems as both trustees and as facilitators of trust between actors. With trust through institutions and trust in institutions, “trustors draw on things that are given and relatively stable” (Möllering, 2006a, p. 51). Möllering (2006a) continues by stating that “when trust is a matter of routine, [...] the routine is performed without questioning its underlying assumptions, without assessing alternatives and without giving justifications every time” (p. 52). It is thus a passive and habitual sort of trust, which implies taking institutions for granted and building trust in other actors based on this stability (Möllering, 2006a, p. 52). Figure 3 adds to Figure 1 by making the facilitator of trust between two actors – from a neo-institutional perspective – an institution. This institution needs to be trusted itself in order to facilitate trust. Institutions can be the bases for trust insofar as they reduce uncertainties (Luhmann, 1979) and make trust between actors dispensable by removing uncertainty. Under such conditions, institutions become substitutes for trust (Möllering, 2006a, p. 106).

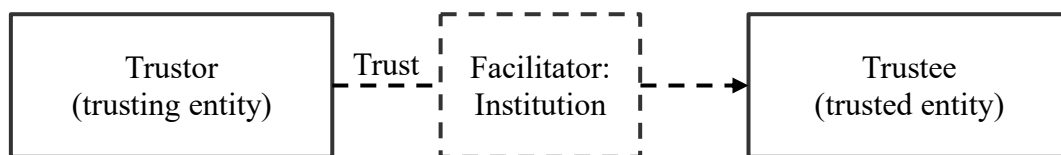


Figure 3: Institution as facilitator for trust and as trustee (own illustration).

The notion of institutional-based trust draws upon Zucker’s (1986) research on trust production mechanisms for economic interaction in the US American economy at the turn of the 19th century. Zucker (1986) defines trust as a „set of expectations shared by all those involved in an exchange“ (p. 54). In the second half of the 19th century, migration movements and instability of enterprises created distances among entities in the economic

system and eroded former mechanisms of individual trust (Zucker, 1986). As a result, institutions became focal points for trust through “formal societal structures, [which depended] on individual or firm-specific attributes (e.g., certification as an accountant) or on intermediary mechanisms (e.g., use of escrow accounts)” (Zucker, 1986, p. 53). Individual or organizational attributes of trust continue to draw on cultural memberships, for example defined roles as in the case of medical doctors (p. 61), shaman or lawyers (p. 63); they can also be expressed in association memberships, professional certificates, educational certificates from renowned universities, or the adoption of certain organizational structures (p. 64). Intermediary mechanisms assure the execution of transactions as expected, for example through usage of banks (p. 61), insurance or brokers (p. 64). At the turn of the 19th century, institutions gained importance for the establishment of trust among actors in the US American economy; in this case, regulation, law, legislation, banks, financial brokers, professions, associations, and bureaucratic organizations were the producers of institutional-based trust (Zucker, 1986).

Möllering (2006a) characterizes rules, roles and routines as trust-producing institutions: “Rules, roles and routines are bases for trust in so far as they represent taken-for-granted expectations that give meaning to, but cannot guarantee, their fulfilment in action” (p. 70). Rules include formal contracts, jurisdictions, trade associations as providers of norms, and technical standards (Lane & Bachmann, 1996). In line with the neo-institutional view, these sets of rules are able to produce trust through common assumptions, meanings, and expectations (Lane, 1997). This is different from reliance on the execution of contract law or avoidance of opportunistic behavior (Lane, 1997, p. 198) as described in rational trust approaches (see above). Rules facilitate (Lane, 1997, p. 198) or complement (Klein Woolthuis, Hillebrand, & Nooteboom, 2005) trust, but this is not always the case. In the case of contracts, their content, modalities (Faems, Janssens, Madhok, & van Looy, 2008; Malhotra & Murnighan, 2002), and functions – apart from strict control and legal execution (Klein Woolthuis et al., 2005) – have influence on whether they facilitate and complement trust between actors. With regard to standards, the institutional-based trust illustrated by Walgenbach (2001) highlights a contradictory case of the ISO 9000 quality standards, which have failed to produce institutional-based trust and instead elicited distrust between buyers and suppliers. Nevertheless, the concept of institutional-based trust through rules has not be dismissed, but further investigated, for example with regard to stages of trust relationships (Bachmann & Inkpen, 2011). Similarly, roles create stable expectations for the actors that perform the role (Möllering, 2006a, p. 67). Möllering (2006a) refers to an example of trust

between actors in temporary work groups on movie sets (Meyerson, Weick, & Kramer, 1996). The study argues that trust between unknown actors is more likely when they treat each other as roles rather than individuals; roles come with a certain scope of tasks and knowledge, and thus standardize expectations (Meyerson et al., 1996, p. 173). Trust through roles implies an assumption of competence and assumes a certain stability in the performed role (Möllering, 2006a, pp. 67–69). Lastly, understood as “regularly and habitually performed programmes of action or procedures” (Möllering, 2006a, p. 69), routines produce institutional-based trust. Their repetitive character leads to predictability. Routines become taken-for-granted and reduce uncertainty in interactions, which makes them facilitators of trust (Möllering, 2006a, pp. 69–70).

Möllering (2006a) identifies two theoretical foundations for this form of institutional-based trust: Natural attitude¹¹ and institutional isomorphism¹². Natural attitude describes a behavior of not questioning and implicitly sharing one’s perception of the day-to-day world with others (Garfinkel, 2004; Möllering, 2006a, pp. 56–57; Schütz, 1970). Institutions manifest rules and shared interpretations (Garfinkel, 2004), i.e. the natural attitude. As a result, the institutionalization of the natural attitude enables actors to trust each other through institutions. This argumentation underpins Zucker’s (1986) understanding of institutional-based trust. From the perspective of institutional isomorphism, institutional-based trust can also be explained by coercive, mimetic, and normative isomorphism. Isomorphism in neo-institutional theory describes the adoption and preservation of structures and practices for the purpose of gaining or maintaining legitimacy. Coerced trust refers to actors that may be inclined to trust when institutions exert light pressure, which is perceived as certitude. Mimicked trust emerges in situations of high uncertainty, where actors trust because they are oriented toward the behavior of others. Normative trust arises from internalized societal roles and norms about when and whom to trust. In all three types of isomorphism, trust of an actor is triggered by institutionalized acts. The resulting trust is thus institutional-based (Möllering, 2006a, pp. 63–65).

Up to this point I have reconstructed how and why institutions facilitate trust. However, with reference to Sydow (1998), Möllering (2006a) argues that in order to elicit institutional-based trust, institutions need to be trusted as well. The relation between trustors and trusted

¹¹ Natural attitude argues from a phenomenological neo-institutional perspective.

¹² Institutional isomorphism argues from an organizational neo-institutional perspective.

institutions can be explained with Luhmann's (1979) and Giddens'¹³ (1990) notion of system trust, given the assumption that institutions can be interpreted as abstract systems (Möllering, 2006a, p. 73). Abstract systems are often trusted as parts of the daily life which lay people frequently interact with although they have limited or no information about how they work (Giddens, 1991, p. 19; Luhmann, 1979, p. 50). Moreover, people do not feel that they are able to influence or change such systems (Luhmann, 1979, p. 50). Airplanes, housing construction, or professional medicine are examples of abstract systems about which users have little knowledge; they do not know about the functionalities of these systems, or the expertise of the people involved in making them work (Giddens, 1990). Nevertheless, people interact with such systems every day and place trust in their dependability (Möllering, 2006a, p. 74). Users' trust in the abstract system is produced at so-called access points, where representatives of an abstract system interact with the user, demonstrating professionalism, soundness, and normality. In the case of the hospital, these access points are found in the doctors behavior; in the case of the airplane, it is the flight attendants who create patients' and passengers' trust (Giddens, 1990, p. 85). But the "taken-for-granted confidence" (Giddens, 1991, p. 23) towards abstract systems can be accompanied by trustors' skepticism. A person that has been disappointed by a conventional medical treatment, for example, might turn toward alternative medicine. Even so, this patient probably still relies on other aspects of the conventional health system, such as food health regulations (Giddens, 1991, p. 23). Luhmann (1979) draws attention to the control mechanisms for complex systems, which are also subject to specialist knowledge, and must consequently be trusted by lay people (pp. 57–58). Möllering (2006a) summarizes that "trust in an institution means confidence in the institution's reliable functioning, but this has to be based mainly on trust in visible controls or representative performances rather than on the internal workings of the institution as a whole" (p. 74). Within Möllering's integrative trust framework, routines comprise passively trusted institutions, or systems as both facilitators of trust and trustees.

Reflexivity

Reflexivity describes active trust building in a reflexive process of interactions between trustor and trustee (Möllering, 2006a, p. 106). Process-based trust is distinct from institutional-based trust in that it is based on "past or expected exchange such as in reputation or gift-exchange" (Zucker, 1986, 53). Zucker (1986) describes how trustors develop trust

¹³ Möllering (2006a) agrees with Lane (1998) and Seligman (1997) that Giddens builds upon Luhmann. Knights, Noble, Vurdubakis, and Willmott (2001) make similar remarks.

based on information they obtain about a trustee. This information stems from the trustor's own experience or reputation, but is not necessarily transferable:

In process-based trust, a record of prior exchange, often obtained secondhand or by imputation from outcomes of prior exchange, provides data on the exchange process. Generally, a considerable amount of person-specific or firm-specific information is required; this information is not readily transferable to other persons or firms, hence markets for process-based trust are unlikely to form. The prevailing model is that persons and firms make investments in process-based trust by creating positive "reputations" or name brands. (Zucker, 1986, pp. 60–61)

Thus, process-based trust can be produced through repeated personal interactions in which the trustee asserts her trustworthiness (Zucker, 1986, p. 62). For instance, when trustees conduct timely payments or carry out on-time-deliveries. As this approach is time-consuming, it limits the selection of transaction partners to those engaged with the trustor in a specific individual process (Zucker, 1986, p. 62). However, process-based trust can also be built without repeated and direct interactions between trustee and trustor. With reputation symbolizing an exchange history, trustors can build process-based trust through symbolic gifts, such as generous warranties, or with systematic brand building (Zucker, 1986, p. 62).

However, reflexivity as a category in Möllering's integrative framework involves some other processual trust building concepts. "Mutual openness and intensive communication" (Möllering, 2006a, p. 100), for example, include the interactions of actors in a reflexive process. Actors exercise their agency, shaping the process of trust building and vice versa. They do so through "signalling, communication, interaction and interpretation" (Möllering, 2006a, p. 79). Moreover, trustor and trustee are free to act. Thus, the respective other remains vulnerable, as the actors involved cannot predict each other's decisions or actions (Möllering, 2006a, p. 99). As the term "process" indicates, trust can develop over time (Blau, 1964; Luhmann, 1979). Initially, actors are sometimes not able to assess each other's trustworthiness. Trust building can be triggered by actors' purposeful interventions, though this is not always the case (Möllering, 2006a, p. 94). The literature reviewed by Möllering (2006a) offers various descriptions for how actors can initiate and shape the process of trust building. Signaling plays an important role here. Still, there is disagreement about whether trust building processes begin with careful rapprochements or with grand gestures (Möllering, 2006a, pp. 86–90). Advocates of the former describe examples of small commitments confirming mutual trustworthiness (Blau, 1964), exchanging presents, drawing on track records (Zucker, 1986), or rationally thinking through each other's intention for a sustained relationship (Lewicki & Bunker, 1996). The other extreme is the request to expose oneself, showing the trustor's willingness to be vulnerable and the trustee's commitment to not betray

the trustor's trust (Luhmann, 1979). A less extreme but still resolute action to kick off the reflexive process of trust building is outlined in Zand's (1972) "spiral reinforcement model of the dynamics trust" (p. 233), which outlines a triad of three actions that signal and reinforce trust. This triad consists of (1) sharing extensive information, one's considerations, and emotions (2) incorporating the other's impact on target setting and procedures, and (3) refraining from mutual control and welcoming interrelations with others. All of these approaches involve activity that brings into motion a process or spiral of further trust building. Signaled trustworthiness and demonstrated trust lead to additional and repeated interactions (Möllering, 2006a, pp. 86–87), which feed back into the nature of the trust relationship itself (Lewicki & Bunker, 1996; Luhmann, 1979; Möllering, 2006a, pp. 89–90). In this process, actors gain knowledge and empathy about each other and their relationship. They learn about and comprehend the requirements and partialities of trustees, which leads to improved anticipation of behavior (Lewicki & Bunker, 1996; Möllering, 2006a, p. 89). Perceived trustworthiness and predictability lead to trusting responses (Möllering, 2006a, pp. 86–87; Zand, 1972). Self-enforcement and path-dependency can also sustain this process (Nooteboom, 1996). Difficulties – jointly experienced, openly addressed, or resolved – among collaborating actors can increase trust (Six, 2005), for example when buyers and suppliers solve problems and master difficult situations together (Möllering, 2006a, p. 188). Familiarization matters as well. Beginning with unfamiliarity, familiarization leads to unquestioned confidence in the uncertain future of somebody or something (Möllering, 2006a, p. 98). This is familiarity (Luhmann, 1979), or the "close acquaintance with something – not only with persons but also artefacts, concepts or emotions previously encountered in the stream of experience and explicitly or implicitly recognizable by the actor again" (Möllering, 2006a, p. 94). This familiarity is a precondition of trust (Möllering, 2006a, p. 98). In the case of buyer-supplier relationships in the printing industry, familiarization not only means being familiar with the industry, but acquiring knowledge about and finding common cause through repeated interactions with business partners on individual and firm levels (Möllering, 2006a, p. 187). Familiarity with repeated situations (Möllering, 2006a, p. 114) and with one's immediately surrounding individuals and institutions (Möllering, 2006a, p. 124) also enable actors' trust.

Although the reflexive trust building process described here is rather a kaleidoscope in terms of differentiating theoretical concepts, it is one of the determining attributes of trust in recent organizational trust research (Li, 2017). This is indicated in the definition of trust as an ongoing process (see above), which draws upon a notion of reflexivity. Finally, with a

specification by Möllering (2006a), the category of reflexive trust building enhances Giddens' (1994) idea of active trust:

Familiarity has to be continuously and reflexively created through familiarization produced by open (even intimate) communication and by being both trusting and trustworthy [...] In sum active trust is trust that needs to be worked on continuously by the actors involved through mutual openness and intensive communication (Möllering, 2006a, pp. 99–100).

In this sub-chapter I have described Möllering's (2006a) integrative trust framework that incorporates several bases of trust and emphasizes on the leap of faith as a mechanism to bridge uncertainty. It will serve as a theoretical perspective and as an approach to organizational trust literature in the subsequent chapters. In the next sub-chapter, I draw attention to the role of non-human actors, specifically information technologies, which have so far attracted little attention in organizational trust research.

3.1.3 How information technologies are implicated in trust

Until now, a review of organizational trust research and Möllering's integrative framework leaves the impression that trust research in organizational studies emphasizes trust between people – individuals, small groups, or organizations. Meanwhile, technical systems are latently considered stable institutions. There are different reasons for the shadowy existence of information technology in trust research in organizational studies. Research on trust in technology is mainly driven by computer science and information systems research. Computer science mainly theorizes trust being embedded in secure systems, which can be trusted because of an absence of vulnerability (van der Werff et al., 2018, p. 400). This is in contrast to one of the main assumptions of organizational trust research, namely that trust exists on the conditions of uncertainty and vulnerability (3.1.1).

Moreover, under the assumption of a strictly psychological definition, trust is a phenomenon inherent to people – machines, on the other hand, are incapable of intentional decisions (Mayer, 2013, p. 906). Even with a broader perspective on trust, at times researchers express the opinion that “things are less interesting since they have no life or will of their own” (Nooteboom, 2002, p. 55). Thus, missing intentionality can render an exploration of trust in technology boring or even impossible. In view of digitization and especially the development of blockchain technology, I disagree and argue that information technologies are not just interesting, but highly relevant for organizational trust research. An organizational understanding of trust keeps a door open for information technologies to be trustees and facilitators of trust (Söllner, Pavlou, & Leimeister, 2013), and assumes that trust is not a

solely psychological phenomenon (Möllering, 2006a, p. 7; Nooteboom, 2002, p. 8). The two roles of information technology are sketched in Figure 4.

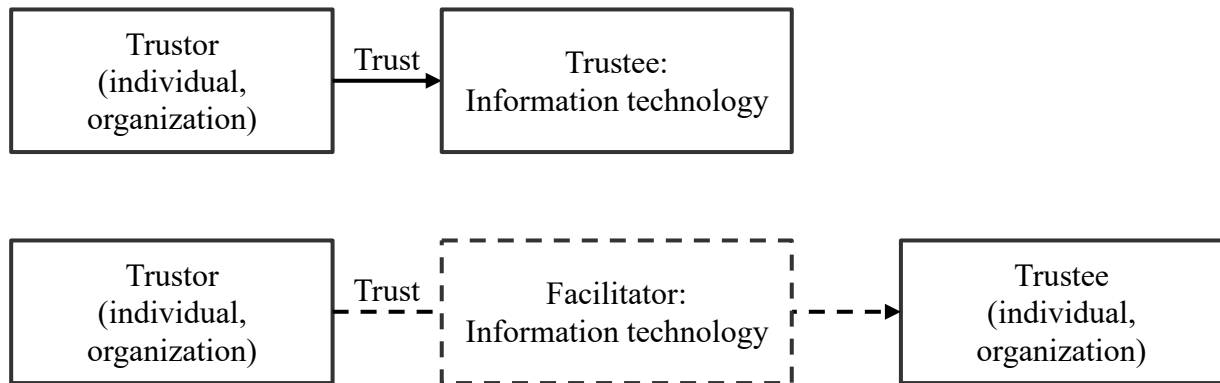


Figure 4: Roles of technology as trustee and as facilitator for trust (own illustration).

In the context of the internet, organizational trust researchers speak of trust cues as elements that contribute to users’ trust in IT artifacts, information technology at a system level, and other users or organizations on online platforms (Möhlmann & Geissinger, 2018; van der Werff et al., 2018). However, trust in information technology is seldom studied in organizational trust research (van der Werff et al., 2018). When I refer to a lack of research on trust in information technology systems, I refer to trust in a “[class] of technology” (McKnight, Carter, Thatcher, & Clay, 2011, p. 9), or trust in a technological infrastructure such as the internet (van der Werff et al., 2018). This is distinct from trust in a specific IT artifact, e.g. a mobile or desktop application.

Overall, research on trust in information technology and IT artifacts builds on the assumption that these actors have no agency (van der Werff et al., 2018, p. 392) as they lack consciousness and have no moral agency (McKnight et al., 2011; Söllner et al., 2013). This leads to an ongoing debate about the extent to which established trust concepts can be transferred or adopted to trust in information technology (Friedman, Kahn Jr., & Howe, 2000; McKnight et al., 2011; Söllner et al., 2013; Söllner, Hoffmann, & Leimeister, 2016). This debate is carried out inside the information systems research literature, rather than in organizational trust research. One reason for this could be that the organizational trust research community’s investigations of information technologies have been scarce. This is also reflected in the latest *Routledge companion to trust research* (Searle, Nienaber, & Sitkin, 2018), which reflects an emphasis on human actors in the organizational trust literature. Worth particular mention, however, is a literature review on individual trust and the internet (van der Werff et al. (2018)). This review has inspired me to complement and bring together several streams of research: Research on trust in and through information technologies within

organizational trust literature, trust literature in information systems research, and perspectives of organizational scholars working in accounting and law. In the following, I use Möllering's (2006a) integrative trust framework (3.1.2) to describe the common ground among these research debates and to specify research gaps.

Reason

Indicators of trustworthiness such as ability, benevolence, and integrity (Mayer et al., 1995) are prominent parts of a reason-based understanding of trust between human actors (3.1.2). The literature reviewed by van der Werff et al. (2018) shows that trustworthiness indicators are widespread in research on trust in information technology and IT artifacts. With the increasing relevance of consumer trust in the context of the internet (Lynn, van der Werff, Hunt, & Healy, 2016, p. 186), scholars have extended indicators of trustworthiness to the trustworthiness of information technologies and specific IT artifacts.

For example, the alternative indicators performance, purpose, and process stem from automation research, where they were used to describe antecedents of operators' trust in industrial automation (Lee & Moray, 1992; Lee & See, 2004). They are also linked to Mayer et al.'s (1995) indicators of trustworthiness. Trustworthiness indicators have been modified and adopted to IT artifacts in general (Söllner et al., 2013) and transferred to specific private user IT applications, e.g. mobile applications (Hoffmann & Söllner, 2014; Söllner et al., 2016). In this context, performance reflects the ability to execute tasks as intended. A technology's purpose represents its benevolence insofar as purpose implies motives for a technology's existence. As automation is not supposed to have intentionality, purpose mainly refers to the machine designer's intent. Process refers to the algorithm's suitability for achieving the operator's or user's goal (Lee & See, 2004, p. 59). Hoffmann and Söllner (2014) suggest that in order to increase user acceptance of IT artifacts, trustworthiness indicators should be considered during software development and during processes of user interface design. Moreover, Söllner et al. (2016; 2013) point out that initial trust by users in IT artifacts does not only involve trust in the IT artifact itself, but is also influenced by users' trust in related actors, particularly the provider. They suggest thinking about trust in IT artifacts as a network among different elements such as user trust in the IT artifact, the provider, the internet community, and user trust in the internet. Measuring user trust along human and technical trustworthiness indicators (Lee & See, 2004; Mayer et al., 1995) shows that trust in the provider has a positive impact on user trust in the IT artifact, while trust in the internet and the internet community do not enhance trust in the IT artifact. On the other hand,

Thatcher, Loughry, Lim, and McKnight (2007) find that user trust in a suite of internet applications is negatively associated with users' internet anxiety.

McKnight and colleagues propose the indicator set of competence, benevolence, honesty, and predictability with the intention of measuring interpersonal trust (McKnight et al., 1998). With regard to information technology, they apply a similar set measuring competence, benevolence, and integrity as a base for users' initial trust in web-vendors (McKnight, Choudhury, & Kacmar, 2002a, 2002b). Wang and Benbasat (2005) argue that online recommendation agents are perceived by consumers "not only as support tools for online shopping, but also as "social actors" (virtual advisors) with human characteristics" (Wang & Benbasat, 2005). Wang and colleagues apply indicators of human trustworthiness (McKnight et al., 2002a) to measure initial trust of consumers in the recommendation agents (Komiak & Benbasat, 2006; Wang & Benbasat, 2005, 2007). Lynn et al. (2016) follow their example by building on Mayer et al.'s (1995) trustworthiness indicators to develop an IT cloud trust label. Komiak and Benbasat (2006) claim that such indicators capture rational trust, but find that they can also increase users' emotional trust in online recommendation agents. A few years later, McKnight et al. (2011) proposed the trustworthiness indicators of functionality, helpfulness, and reliability, which are specific to trust in information technology. According to the authors, these indicators are nevertheless comparable to the above mentioned indicators by Mayer et al. (1995): Ability (which McKnight et al. (2011) refer to as competence), benevolence, and integrity. Functionality of a software is similar to a person's ability in that the trustor trusts the ability of the software to competently perform a task. McKnight et al. (2011) mention the example of payroll software, which is expected to issue accurate payrolls and execute correct payroll taxes (p. 5). Helpfulness refers mainly to software's help function and its disposition to support users in resolving problems that prevent them from performing a task. Lastly, the integrity of a person is similar to the reliability of a software, as both produce predictability of actions. For example, a reliable system is characterized by high uptimes and predictable reactions to commands (McKnight et al., 2011). In a study on users' trust in Facebook, Lankton and McKnight (2011) confirm the theoretical linkage of the conceptual pairs competence/functionality, integrity/reliability, benevolence/helpfulness. Moreover, Facebook users blur human and technology-specific perceptions of trustworthiness by attributing human and technology-specific characteristics to Facebook, trusting it as an IT artifact and as a "quasi-person" (Lankton & McKnight, 2011, p. 32). Contrary to Möllering (2006a), McKnight et al. (2011) do not consider their indicators of trustworthiness as bases for trust, but as consequences or expressions of trusting beliefs by

users who have gathered knowledge through adoption (pp. 9–10). Although Wang and Benbasat (2007) measure initial trust in online recommendation agents, they find that knowledge provision – such as explanations about the recommendation agent – increases users’ initial trust. This trust is not only rational with regard to the trustworthiness indicators, but as the authors suggest, is also the information provided for solving an agency problem between the online recommendation agent and consumer. The information can reduce an information asymmetry between the online recommendation agent and consumer, who may be worried or uncertain about the agent’s behavior. The argument follows the same line of reasoning as the finding that consumers’ trust in e-vendors is partially based on consumers’ calculative belief that an e-vendor has no incentive to cheat (Gefen, Karahanna, & Straub, 2003).

With regard to information technology’s role as a trust facilitator, indicators of trustworthiness, such as those developed by Mayer et al. (1995), serve to explore and measure trust. In cases of online platforms (Möhlmann & Geissinger, 2018), in particular online market places like eBay (Pavlou & Dimoka, 2006) and sharing economy platforms like Airbnb, BlaBlaCar, and Uber (Möhlmann & Geissinger, 2018) users act in a trusting relationship. In this arrangement, the technological platforms act as facilitators of trust between users. While buyers and sellers on online market places do not usually meet in person but instead communicate through the platform, users of sharing economy platforms have more personal interactions, for example on a joint car ride or during dinner at a host’s house (Möhlmann & Geissinger, 2018, p. 31). Nevertheless, eBay’s textual feedback mechanism where sellers comment on past experiences with specific buyers contribute to trust building among buyers and sellers. Buyers’ perception of sellers’ benevolence and credibility¹⁴ draws upon the textual feedback provided by other buyers (Pavlou & Dimoka, 2006). In turn, differentiation of sellers based on their perceived benevolence can incentivize sellers to show goodwill (Pavlou & Dimoka, 2006, p. 409). Moreover, with their ability to ensure users’ accountability through control and sanctioning mechanisms, digital platforms contribute to calculative trust between users (Möhlmann & Geissinger, 2018, pp. 33–34). Driving skills of a BlaBlaCar driver represent her ability; an Airbnb host’s motivation to not only earn money, but enable guests to have a good time indicates benevolence; and the rightness of an apartment’s description represents a host’s integrity (Möhlmann & Geissinger, 2018, p. 31). Following Mayer et al. (1995), this creates interpersonal trust between the users.

¹⁴ Credibility implies competence and reliability (Pavlou & Dimoka, 2006, p. 395).

Other trust building mechanisms, which Möhlmann and Geissinger (2018) call trust cues, and which I subsume under routine and reflexivity, also contribute to create users' belief in other users' trustworthiness.

Routine

When speaking of routine-based trust, we can refer to trust in systems and institutions as well as the role of institutions as facilitators of trust between actors (3.1.2). Institutional-based trust can explain the role of information technology as facilitators of trust. Knights et al. (2001), for example, suggest a biometric identification system as a control mechanism, which because of its ability to reduce uncertainty about one's identity, acts as a potential facilitator of trust between anonymous agents in online trading (p. 321). Literature on online market places and sharing economy platforms also analyzes the unique ability of platforms to create trust between actors who exchange products and services. Although sharing economy platforms tend to circumvent trust building institutions, such as governmental regulations and interventions (Möhlmann & Geissinger, 2018, p. 35), they still draw on other institutional-based trust building mechanisms. Sharing economy platforms and online market places make use of escrow services to execute financial transactions between users (Möhlmann & Geissinger, 2018; Pavlou & Gefen, 2004), they draw on validation processes for data, such as phone numbers or apartment pictures and they involve trusted associations, companies and governmental identification devices in this validation process (Möhlmann & Geissinger, 2018; Pavlou & Gefen, 2004; Sundararajan, 2016). Moreover, sharing economy platforms create trust by displaying a reliable insurance coverage (Möhlmann, 2016; Möhlmann & Geissinger, 2018; Sundararajan, 2016), while online market places give credit card guarantees (Pavlou & Gefen, 2004, p. 42). Besides these references to "legally binding" (Pavlou & Gefen, 2004, p. 37) external trust building mechanisms, digital platforms also produce institutional-based trust between users through feedback mechanisms (Bachmann & Inkpen, 2011; Möhlmann & Geissinger, 2018; Pavlou & Gefen, 2004). Online market places like Amazon and eBay provide public feedback forums where buyers depict the experiences with specific sellers (Pavlou & Gefen, 2004, p. 42). Similarly, sharing economy platforms encourage users to mutually rate one another - hosts and lodgers, drivers and passengers evaluate each other online (Möhlmann & Geissinger, 2018). These mechanisms create buyer's trust in an online market places' seller community (Pavlou & Gefen, 2004), while also facilitating trust between users of sharing platforms (Möhlmann, 2016; Möhlmann & Geissinger, 2018). Pavlou and Gefen (2004) and Möhlmann and Geissinger (2018) refer to

feedback mechanisms as sources of reputation, as they collect data about past experiences. These authors do not theorize feedback mechanisms according to Zucker's (1986) process-based trust, but instead conceptualize them with institutional-based trust perspective. This is because such feedback mechanisms create "transaction norms" and "informal [...] certification systems" (Pavlou & Gefen, 2004, p. 42). Bachmann and Inkpen (2011) also emphasize the behavioral "norms, structures and procedures" (p. 292) that develop among the user community. Rating a seller on eBay is a routine, which enacts a community norm and reinforces the structure that builds trust between buyers and sellers. The data accumulated about specific sellers is a "proxy for the overall trustworthiness of the seller community" in an impersonal virtual environment (Bachmann & Inkpen, 2011, p. 292). Lastly, there are technical security routines and rules, which build so-called "technology trust" (Ratnasingam, 2005) among buyer and seller organizations. Ratnasingam (2005) defines technology trust as "a subset of institution-based trust, drawing from the adherence to technical standards, security procedures, and protective mechanisms that provide technical solutions" (p. 527). The technology itself provides the technical characteristics, which then can be acknowledged as trust building institutions and serve as a base for further inter-organizational trust building (Ratnasingam, 2005).

This leads to cases where information technologies are theorized as trusted institutions or trusted systems. In a presentation for actors involved in the establishment of IT cloud services, Möllering (2011) recommends that cloud providers, users and regulators foster trust in technology through access points. In addition to visible control mechanisms, human representatives can act as access points and take on responsibility, which signals trustworthiness and thus fosters trust in IT cloud platforms (Möllering, 2011, pp. 45–46). Knights et al. (2001) explored the case of biometric smart cards, which were tested at the turn of the millennium for use as identification systems in online commerce. The authors found that users' and the public's trust in this technological system and the system trust (Giddens, 1990, 1991; Luhmann, 1979) in financial institutions behind the card identification system were interdependent (p. 329).¹⁵

McKnight et al. (1998) explicitly applied institutional-based trust – which was initially a concept concerning trust in human actors (Zucker, 1986) – to technology. McKnight et al. (2011) define institutional-based trust in "classes of technology" as "beliefs about a specific

¹⁵ However, organizational scholars also mention low levels of trust by users and the public in emerging information technologies, e.g. IT cloud (Lynn, van der Werff, Hunt, & Healy, 2016, p. 185) or virtual financial services (Knights, Noble, Vurdubakis, & Willmott, 2001, p. 311).

class of technologies [...] composed of situational normality and structural assurance within a context” (p. 8). Situational normality here refers to the predisposition to use similar artifacts in various contexts, while structural assurance relates to seals of approval, and contractual or operational support. Institutional-based trust in information technology and specific IT-artifacts can consequentially lead to trust in a web-based vendor, i.e. an organization represented by and acting through a website. In the early 2000s, when the internet was not yet as ubiquitous as it is today, McKnight et al. (2002b) found that structural assurance on the web positively relates to consumer’s initial trust in a specific web-based vendor. Institutional-based trust elicited through the structural assurance of e-commerce websites – embodied in seals, guarantees, contact information and an appearance perceived as normal – have positive effects on users’ trust in e-commerce vendors (Gefen et al., 2003). Moreover, consumer trust in institutions from an offline context can spill over into new technological contexts. In a research experiment, Stewart (2003) discovers that consumers’ institutional-based trust in established retail stores can translate to their respective online shops when websites present pictures of the physical store (Stewart, 2003). Following the concept of trust transfer, McKnight et al. (2011) find that institutional-based trust in an information technology system positively influences users’ initial trust in a specific IT artifact. On the other hand, Söllner et al. (2016) cannot verify their institutional-based hypothesis that trust in the internet influences users’ initial trust in IT artifacts, though trust in the internet does have a positive effect on trust in an IT-artifact’s provider. These authors conclude that Zucker’s (1986) institutional-based trust, which initially explained trust in human actors through institutions, might not be a suitable theoretical concept for user trust in technology after all. Moreover, McKnight et al. (2011) find that users rely less on institutional-based trust when they have achieved knowledge-based trust through experience. This last point leads us to Möllering’s (2006a) third basis for trust, namely reflexivity.

Reflexivity

Reflexive trust building is a process that draws upon openness, communication, interaction, and information (3.1.2). In information systems research, experience and knowledge-based trust have been underexplored in the realms of trust in information technology (McKnight et al., 2011) and organization studies. Although many of the studies discussed above refer to theories that imply reason and routine-based trust, some of them contain implicit or explicit elements of reflexive trust building. Wang and Benbasat (2007) measure the positive impact of knowledge provision on users’ initial trust in online recommendation agents, and find that

explanations form part of knowledge-based trust building. Lynn et al. (2016) develop an IT cloud trust label, which informs potential users and signals the cloud's trustworthiness, thus permitting users to make a trust decision (that is also based on knowledge). In addition to initial user trust, knowledge-based trust is built through user experiences with specific IT artifacts (McKnight et al., 2011). Familiarity (Luhmann, 1979) increases users' cognitive trust in online recommendation agents (Komiak & Benbasat, 2006) and positively affects trust in sharing economy platforms (Möhlmann, 2016). Such familiarity can arise from users' repeated interactions with sharing services (Möhlmann, 2015). In turn, users' experience-based trust in an IT artifact positively affects their intentions to explore and use that IT artifact more broadly, while also mediating institutional-based trust in the general technology (McKnight et al., 2011). Gefen (2000) finds that familiarity of consumers with an e-vendor's web interface and processes increases trust in the e-vendor. One of the author's contributions to trust theory is that familiarity is not only built in interaction between human actors as outlined by Luhmann (1979), but also in interactions between humans and IT artifacts (Gefen, 2000, p. 733). Familiarity is understood as knowing how to search and inquire about items – in Gefen's (2000) study books – on the e-vendor's webpage. Previous buying experiences with the website or vendor, instructions on how to use the website, information about the vendor organization, and third party information about the vendor are all assumed as pathways toward familiarization (Gefen, 2000, p. 729). Gefen et al. (2003) are not able to prove an increase in user trust through familiarity in their follow-up quantitative study, but find that familiarity leads to the perception of an easy-to-use interface, which positively affects trust in the e-vendor. Thus, although familiarity was not a major aspect for Luhmann's (1979) system trust, a few scholars suggest that users can build trust in IT artifacts, online recommendation agents, sharing economy platforms, and e-vendors based on their familiarity with these artifacts and online organizations. In his presentation at a practitioner conference about trust in IT cloud by the German think tank Münchner Kreis, Möllering (2011) hints at the effects of joint problem solving and cooperative communication systems among providers and users. These processes can build generalized trust among anonymous IT cloud users, between users and providers, and consequently would enhance users' trust in the IT cloud technology (Möllering, 2011, pp. 44–45).

If a user has not yet achieved knowledge and familiarity with an IT artifact, information technology, or e-vendor, the brand and reputation of the provider or e-vendor can play a role for users' trust in the respective trustee. Perceived e-vendor reputation, for example through word of mouth communication, positively relates to users' initial trust in an e-vendor

(McKnight et al., 2002b). Söllner et al. (2016) find that user trust in an IT artifact provider has strong positive effects on users' initial trust in the IT artifact. Theoretically, the authors argue, this trust in the provider is based on its brand. However, in their research experiment, the providers are also the researchers, and their identity is known to the users in the experiment. They also suggest that user trust in the provider might be more relevant for initial adoption, while trust in the IT artifact might be more relevant for continued usage.

Such trust spill-over is also relevant to the trust relationship between sharing economy platform users. According to Möhlmann and Geissinger (2018), users' trust in a provider organization's brand is transferred into trust among the sharing users. Although Möhlmann (2016) argues with reference to Luhmann (1979) and Stewart (2003) that trust in platform providers as systems or institutions transfers to the relationship between users, I see a strong indication for process-based, and thus reflexive form of trust in the platform provider. Trust in the platform provider is – according to the quote above – based on the provider's brand, which is a mechanism that falls under Zuckers' (1986) definition of process-based trust. Furthermore, users' familiarity with a sharing economy platform positively relates to their trust in other platform users.

Besides trust spill-overs, sharing economy platforms and online market places can also facilitate a form of trust, which I consider to be based on reflexivity. In summary, these trust cues build on the provision of information about users. Sharing economy platforms, for example, accumulate “digitalized social capital” (Möhlmann & Geissinger, 2018, p. 34) by connecting user profiles with users' social media accounts on Facebook or LinkedIn. In doing so the amount of circulated information about specific users is increased. Moreover trust is built through the provision of personal data – users' full names, skills, and interests – and by sharing information about the objects of transaction, e.g. the type of car in ride sharing, or the peculiarities of a host's apartment (Möhlmann & Geissinger, 2018, p. 34). Pavlou and Gefen (2004) also hint that comments fulfill an information provision function, which constitutes a basis for buyers to trust sellers (p. 42). As discussed with regard to routine-based trust, I consider the feedback mechanisms of digital platforms also to be based on reflexivity. More specifically, we can understand feedback as a process-based trust building mechanism, as they cumulate users' experiences into proxies for reputation (Möhlmann & Geissinger, 2018; Pavlou & Gefen, 2004). Taking the algorithmic aspects of platforms' infrastructures for building trust and reputation, Kornberger, Pflueger, and Mouritsen (2017) highlight the interplay between power and control. While users exercise control through feedback and evaluation, the provider organization exercises power over the calculative algorithms that

shape how feedback is given. This combination of power and control, referred to as protocol, is characteristic of relational trust-creating platforms such as eBay.

Lastly, from an implicitly reflexive perspective on inter-organizational trust, the adoption of a technological system between buyer and supplier can also build trust between organizations. In the cases of Electronic Data Exchange (EDI) and e-commerce adoption, trust between buyer and supplier is built on practices which occur throughout the adoption process, including acts of mutual openness, information sharing, showing confidence in the supplier's competence, and sharing responsibility (Hart & Saunders, 1997; Ratnasingam, 2005). Trust is also built on dedication by top management, and the accomplishment of high standards for technology and service (Ratnasingam, 2005).

In summary, a review of studies on trust and information technology that have resonated in organizational trust research gives the impression that the literature tends to more commonly look at trust from reason or routine perspectives. This may be because of the widely used indicators of trustworthiness as misconceived proxies for measuring trust (Gillespie, 2015), or it could be the result of emphasizing users' initial trust (McKnight et al., 2011). While organizational trust research in general has started to turn toward a more process-based understanding of trust (Li, 2017), research on trust in and through information technology and IT artifacts affords little attention to experience and knowledge-based trust (McKnight et al., 2011). This is especially surprising in cases which look at technologies during their emergence, i.e. when technological artifacts and relations are relatively unstable. As a consequence, the literature offers few descriptions or explanations about practices of reflexive trust building involving information technologies. Explicit references to the leap of faith are also absent, although I imagine that such a leap is crucial to innovation, where uncertainties about technical development, behavior, and contextual development are high (Nooteboom, 2013, pp. 106–107). Although this uncertainty is an integral subject in the discussion about trust in and through information technology, trust tends to be squeezed into questions about perceived trustworthiness or studies on the intentions to trust and adopt specific artifacts.

Looking at the actors involved in this research, it is striking that trust in general information technology – e.g. the internet or other information technology infrastructures – continues to be an under-researched field (van der Werff et al., 2018, p. 400). Of course, this lack of research depends on how one conceptually distinguishes between IT artifacts and information technology. For example, it is debatable whether online recommendation agents are IT artifacts (Wang & Benbasat, 2005) or technological infrastructures (van der Werff et al., 2018), or if online market places and sharing economy platforms are information technology

infrastructures. What is surprising in this regard is that the distinction between users' trust in platforms and their trust in the respective provider organization is often unclear (Gefen, 2000; Gefen et al., 2003; Möhlmann & Geissinger, 2018; Pavlou & Gefen, 2004). Söllner et al. (2016) conduct and also call for a network perspective when investigating trust in IT artifacts, which would consider both user trust in the provider and user trust in the underlying technological infrastructure. Overall, it appears that research on trust in and through IT artifacts and information technology is user-centric, and spares the relations between technology providers and other actors, such as users (Söllner et al., 2013) or the technology itself. Thus, in organizational trust research, we can embrace information technology as an actor. Doing so follows a call from information systems research to enhance trust research by incorporating multiple actors and investigating the dynamic relations among them:

Research is necessary that examines the dynamic interplay between users' trust in human agents that built a system, human agents that introduce a system, those that support a system, and the technology itself. By examining how trust in different elements of the context and IT interact, one can form a broader understanding of how trust in socio-technical systems shapes value-added technology use. (McKnight et al., 2011, p. 14)

Lastly, trust research generally assumes that IT artifacts (McKnight et al., 2011; Söllner et al., 2013) and information technology systems do not have agency (van der Werff et al., 2018). Some argue that agency cannot be attributed when IT artifacts and systems lack intentionality and morality. On the other hand, online marketplaces and sharing economy platforms impact users' relations to one another (Möhlmann & Geissinger, 2018; Pavlou & Gefen, 2004) and can even constitute users (Kornberger et al., 2017). Platforms defer from each other and change over time as well (Kornberger et al., 2017; Möhlmann, 2016). For example, eBay has evolved from a set of feedback mechanisms into a calculative infrastructure, which today creates its own form of trust through quantification (Kornberger et al., 2017). Consequentially, with blockchain technology, it is now possible for novel forms of trust relations to appear (Möhlmann & Geissinger, 2018, p. 37).

In the following, I complement my exploration of blockchain technology as socio-technical systems with Actor-Network Theory's notion of translation. This will help me consider the unintentional agency of technologies, emphasize on the processual character of trust building in an emerging technology, and incorporate a variety of actors into my analysis. Next (3.2), I introduce the concept of translation and outline how I use it to investigate the role of trust and trust building in emerging socio-technical networks.

3.2 The becoming of actor-networks

3.2.1 Actor-Network Theory and translation

In this thesis, I attempt to enhance organizational trust research by working with the notion of translation as its understood in Actor-Network Theory (ANT). ANT pays special attention to non-human actors and many studies following an ANT perspective focus on the emergence of technologies. As such, ANT is particularly apt for my exploration of trust and blockchain technology. ANT originated from Science and Technology Studies (STS) beginning in the 1980s. STS around this time comprised mainly of empirical studies of laboratory work (Knorr-Cetina, 1981; Latour & Woolgar, 1979) and focused on the social production and legitimization of facts and technologies (Latour, 1987). From an ANT perspective, everything is in a state of flux. As Hernes (2010) points out, ANT “works from an ontology of becoming rather than assuming that entities can be defined in terms of pre-given competencies and capabilities” (p. 161). Classic ANT authors such as Bruno Latour, Michel Callon, and John Law began studying the emergence and change of social infrastructures, describing how dynamic relations and interconnections between social actors transform, evolve, and dissolve over time (Callon, Law, & Rip, 1986; Latour, 1987). With ANT, such relational change is often conceptualized with the notion of translation (Czarniawska & Hernes, 2005, p. 9), a process that describes the assembling of actors into temporarily stable actor-networks (Hernes, 2010, p. 165). The latter are “interrelated [sets] of entities” (Callon et al., 1986, xvi), which temporarily act as one (Latour, 2005, p. 217), e.g. a fact or a technology. The importance of translation in ANT is expressed by Latour (2005), who even as a “founder” of the perspective, struggled with the term “Actor-Network Theory”, and instead advocated for it to be called a “sociology of translation” (Latour, 2005, p. 106). Translation implies entities’ movements (Czarniawska & Hernes, 2005, p. 9), interactions, communications, mutual influences, and networking practices (Krieger & Belliger, 2014, pp. 109–110); it highlights how actors attempt to cope with and stabilize uncertainties thereby turning them into certainties (Callon, 1986b, p. 222). Accordingly, this concept is well suited to studying the prospects of innovation, emerging technologies and infrastructures, which themselves are riddled with uncertainties (Latour, 2005, p. 142, 2005, p. 11). While diffusion theory assumes technological artefacts to be stable entities that are simply adopted (or not), ANT opposes this idea by describing artefacts as they change in interactions with multiple actors (Latour, 1987). A theory of translation assumes “indeterminate entities that are given their identities and roles through the work performed in relation to other entities” (Hernes, 2010, p. 168). Therefore,

the notion of translation seems to speak to the blockchain phenomenon, which at the time of writing is still subject to continuous change and uncertainty.

The term actor¹⁶ – in ANT and its notion of translation – is not limited to human beings, but also includes non-human actors (Hernes, 2010), e.g. technical artefacts. What makes these objects recognizable as actors is their impact on social situations. For discerning a social actor, Latour (2005) asks “does it make a difference in the course of some other agent’s action or not? Is there some trial that allows someone to detect this difference?” (Latour, 2005, p. 71). Latour (2005) illustrates the impact of non-human actors with simple examples: “Kettles ‘boil’ water, knives ‘cut’ meat, baskets ‘hold’ provisions, hammers ‘hit’ nails on the head, rails ‘keep’ kids from falling, locks ‘close’ rooms against uninvited visitors, soap ‘takes’ the dirt away, schedules ‘list’ class sessions, price tags ‘help’ people calculating” (p. 71). These wordplays illustrate how human actions and attention can be influenced by non-human actors. This doesn’t mean that a social actor necessarily initiates or has intention in action. Rather, actors just act, and there are multiple social actors and entities that interfere and interact with one another (Latour, 2005, p. 46). Thus, human and non-human actors have intentional and unintentional agency (Latour, 2005). This is not only the case for human beings and material objects, but also for quasi-objects such as ideas, practices (Czarniawska & Sevón, 2005b), and even trust (Mouritsen & Thrane, 2006, p. 243). However, organizational trust research has not yet accounted for the agency of technical artefacts (3.1.3) or for trust as a quasi-object. In this regard, the notion of translation is a complement to trust research.

ANT studies that have drawn upon Latour’s and Callon’s notion of translation have themselves been translated from STS into literature streams in other disciplines, such as organization studies (Alcadipani & Hassard, 2010, p. 419) and accounting research (Justesen & Mouritsen, 2011, p. 167). The original ANT authors investigated various phenomena, such as research projects on the anchoring of scallop larvae (Callon, 1986b), as well as the becoming and failure of technical innovations, for example British aircraft (Law & Callon, 1992), electric vehicles (Callon, 1986a), and public transport vehicles (Latour, 2002). For nearly the last 30 years, translation has informed studies in accounting (Justesen & Mouritsen, 2011) on the emergence and implementation of accounting technologies and practices. Activity-Based Costing (ABC) has been translated into a “ready-made costing system” (Jones & Dugdale, 2002, p. 125) thanks to a global network of scholars, practitioners, consultants, software, publications, documents, and accounting practices (Jones & Dugdale, 2002).

¹⁶ I refer to actors as entities that act (Latour, 2005, p. 71) and refrain from using the term actant.

Management accounting systems have also been subjects of translation in the Australian healthcare sector (Chua, 1995), although that particular study rejects the agency of the accounting system (p. 117) and stresses its dependency on human “believers” (p. 132). However, what these works in accounting research have in common is their assumption that systems are translated – constructed and shaped – through processes of interaction among assembled actors. As a consequence, many of these systems take on a form which deviates from how they were initially intended and designed. For instance, SAP’s ERP systems were implemented in multinational firms with the hope of increasing control, but ultimately resulted in a perceived loss of control (Quattrone & Hopper, 2005). In inter-organizational relations, stable management control technologies have shaped the relations between partner firms and thus supported translations of partners and resources into network enterprises (Mouritsen & Thrane, 2006). New accounting practices have also changed the relations between cloth manufacturers, department stores, and department buyers, resulting in the construction standard body sizes in the fashion industry (Jeacle, 2003). In the translation of Do It Yourself (DIY) from an economic need into a recreational activity in Great Britain, accounting technologies such as cost savings created an interestment device or “interface” between actors assembled in the movement (Jeacle, 2017). Overall, the sociology of translation has introduced a new theoretical vocabulary to accounting research (Jeacle, 2017, p. 101) and has established new perceptions of accounting and accounting practices (Justesen & Mouritsen, 2011; Robson & Bottausci, 2018). Accounting systems and practices have become material actors that influence others. Translations of accounting phenomena are not just diffusions or implementations, but the adoptions of these technologies are constructions which imply changes as well as the enrollment of multiple actors. Moreover, ANT-based studies refrain from theorizing along categories such as micro and macro, subject versus object, structure versus agency, or technical versus social (Justesen & Mouritsen, 2011, pp. 176–177).

In organizational research, translation-based studies have also become significant, though controversial (Alcadipani & Hassard, 2010; Whittle & Spicer, 2008) approaches to investigating dynamic organizational phenomena. Translation has informed research on the travel of management ideas, knowledge, and practices (Czarniawska & Sevón, 1996; Sahlin-Andersson & Engwall, 2002), such as Corporate Social Responsibility (CSR) (Sahlin-Andersson, 2006), different strategic plans (Hwang & Suárez, 2005), as well as ideas complementary to management, such as union trade learning representatives (Cassell & Lee, 2017). Translation-based studies have also emphasized that institutions (Czarniawska, 2009;

Czarniawska & Sevón, 1996, 2005a; Hernes, 2005), organizations (incl. their work), production, and processes (Czarniawska & Hernes, 2005; Winiecki, 2009), and networks in a socio-ecological system (O'Mahoney, O'Mahoney, & Al-Amoudi, 2017) are constituted by human and non-human actors which continuously perform translations. These studies often dissolve the formal boundaries of organizations and connect them to global ideas, societal problems, and the interests of other actors. Other phenomena of interest for organization scholars include translations of and by IT artifacts and IT projects. Translations of an ERP system have shown that the software and the organizational settings where it was introduced mutually changed each other through their interactions (Locke & Lowe, 2007). Similarly, the translation of a financial reporting application in a municipal government agency required the involvement of several actors, and led to organizational change as well as change in the financial reporting application (Holmström & Robey, 2005). Public authorities' internet web portals have also enrolled actors into markets (Norén & Ranerup, 2005). In open source software projects, multiple IT artifacts, especially the source code, mailing lists, and license agreements, have coordinated and stabilized relations among project contributors and users (Lanzara & Morner 2005). In the case of biological research, a taxonomy database was introduced and jointly developed to legitimize the project and the content it produced, which aimed to benefit biological classifications by solving a problem of lacking legitimacy (Hine, 1995). These studies on IT artifacts and projects – despite their differences in size and characteristics of the actors (including the information technology and artifacts involved) – all use translation as a perspective to describe the emergence of socio-technical systems that are compounded by uncertainty. Uncertainty in this regard encompasses the future state of the non-human actor as well as its relations to other actors (Callon, 1986b).

In my work, I seek to contribute to organizational trust research by drawing upon Callon's (1986b) notion of translation to analyze the becoming of blockchain technology. In Callon's now seminal work (1986b), a diminished population of scallops finds itself in a process of translation with a group of researchers, their scientific colleagues, and the fishermen of St. Briec Bay. The translation process evolves towards the involved actors' production and acceptance of knowledge about the reproduction of scallops, which is shaped by mutual negotiations of interests, identities, and relations. Although some of the involved actors act with intentionality (especially the researchers who initiate the research project), no actor can fully control the translation or its outcome. The becoming of actors assembled around a research project in a network is subject to translation (Hernes, 2010). Callon (1986b) distinguishes four phases, or what he calls moments of translation: Problematization,

interessement, enrolment and mobilization. Although translation narratives tend to be chronological, Callon (1986b) emphasizes that moments often overlap temporally and do not proceed one after another (p. 203). This is also exemplified in the translation case of DIY during the 1950s (Jeacle, 2017).

As the term already implies, problematization creates awareness of a problem and proposes a solution in the interest of the actors involved. In the case of St Brieuc Bay, the problem revolves around stimulating the reproduction of the bay scallops. However, the problem is not immediately evident, but rather constructed by actors, especially the three researchers (Callon, 1986b). In the case of St Brieuc Bay a solution was then proposed, namely a research project on the anchorage of scallop larvae. The sociology of translation describes a “double movement” (Callon, 1986b, p. 204) that constitutes this act of problematization. This double movement comprises the definition of actors and obligatory passage points (Callon, 1986b, pp. 203–206). The definition of actors implies determining the identities and interests of the entities involved. For example, the three biologists identified the scallops, the fishermen of St Brieuc Bay, and the broader scientific community as additional actors in a report. The scallops were identified as a species with certain behavioral features, which was assumed to accept protection devices in order to ensure their reproduction and survival. The scientific community had little knowledge about scallops, however, and was supposed to be curious about the research project and expected findings. The fishermen’s existence depended on the long-term persistence of the scallop population. Although they gained from extensive fishing in the short-term, the diminishing population would force them to decrease their fishing activities. The three biologists positioned themselves as eager to contribute to the body of knowledge on scallops and at the same time serve the goals of the fishermen. They assembled all actors around the research project, which asked if scallop larvae in St Brieuc Bay were able to attach themselves to a protective collector that would support their growth. By promoting the ways in which all actors would benefit from knowing the answer to this research question, the research project established an obligatory passage point that was in everybody’s interest (Callon, 1986b, pp. 203–206). In the translation of DIY, housing shortage and manpower bottleneck was identified as a societal problem, while DIY became an obligatory passage point (Jeacle, 2017). DIY magazines, radio and television, the government, handymen, DIY product manufacturers, and home exhibition organizers acknowledged DIY being in their interest and pledged to solve the overall problem. Jeacle (2017) concludes that “problematization provides a useful means of explaining the emergence of the various actors and the rhetoric deployed by each in making the case for DIY” (p. 107).

Interessement inflicts actors with roles and relations, ensures the becoming of a network (Hernes, 2010, p. 171), and promotes the enrolment of actors (Jeacle, 2017, p. 100). Callon (1986b) uses the expression of “locking allies into place” (p. 206), i.e. connecting actors (Jeacle, 2017, p. 102). Interessement devices support the stabilization of identities and the building of relations between actors. They do so by distancing actors from alternative interpretations (Callon, 1986b, pp. 207–209), or by creating an interface that connects actors in a network (Jeacle, 2017). For the scallop larvae of St Brieuc Bay, interessement devices included the physical collectors on a towline. The towline was placed between larvae and their natural enemies as well as other adverse elements, such as currents. The larvae were thus shielded from other actors, which might have had an interest to modify the scallops’ roles as a protected and recovering population (Callon, 1986b, pp. 209–210). For the fishermen and scientific colleagues, the “texts and conversations which [lured] the concerned actors to follow the three researchers’ project” acted as interessement devices (Callon, 1986b, p. 211). In the translation of DIY, the interessement devices consisted of labor cost savings that would result from lay persons engaging in DIY activities. These interessement devices appeared in a variety of magazines promoting DIY, which repeatedly referred to lower household and public budgetary costs that could be achieved through DIY. As a result, cost savings connected and stabilized the identities of various actors, such as DIY magazines, radio and television, the government, handymen, DIY product manufacturers, and home exhibition organizers (Jeacle, 2017, pp. 105–106).

During processes of interessement, actors loosen or break their relationships to other networks and build relationships with new actors. During this phase, a new network is only hypothetical. A network then becomes reality when actors negotiate, modify, and accept their roles in relation to one another, and behave in accordance with these roles. While interessement has a rather hypothetical character, enrolment refers to the processes of testing, negotiating, and turning assumptions into facts. In Callon’s words (1986b), “interessement achieves enrolment if it is successful” (p. 211). Thus, during enrolment one can often observe arguments, showdowns, and “multilateral negotiations” (Callon, 1986b, p. 211) in which antagonists turn into allies, at least for a while (Belliger & Krieger, 2006, pp. 40–41). During the domestication of scallops, Callon noticed a range of enrolment activities, including silent partnerships, deals, seductions to physical power. While some attempts at enrolment failed, others succeeded. In this respect, negotiations with scallops required some effort. In order to convince scallops to anchor to the collector, the scientists tried to keep away currents, parasites, and other natural enemies. Moreover, they adjusted the technical experiment set-up

so that it would better fit the scallop larvae. Although only a few larvae anchored, the scientists were able to agree with the scientific community that the experiment was a success. After recognizing each other's efforts and expertise in the field of research on scallops, many agreed that a sufficient number of scallops had anchored. The fishermen of St Brieuc approved silently and without further encouragement (Callon, 1986b, pp. 211–213). Jeacle (2017) also points out the enrolment interactions among different actors in her analysis of DIY (pp. 106–107). In this case, enrolment represented the conduct of home improvements, the selling of DIY products, meeting at fairs, promoting products, as well as writing and sharing experiences about DIY. Magazine editors asked their readers to share their own DIY experiences and advice, which lead to letters from readers about their own projects, comments on the magazine content, and DIY product advertisements. These letters were referred to once again in various magazines. Moreover, product manufacturers were engaged by the magazine through the product recommendations in articles and by DIY exhibitions for potential customers. These activities pointed to “the formation of an assemblage, a coming together of these diverse actors to create a powerful actor network” (Jeacle, 2017, p. 106).

Finally, translation leads to a “mobilization of actors who render [...] propositions credible and indisputable by forming alliances and acting as a unit of force” (Callon, 1986b, p. 216). In other words, translation results in a network of actors, a temporarily stable actor-network with one identity (Callon, 1986a). The assemblage of handymen, journalists, manufacturers and retailers who promoted and pursued DIY were related to one another in a network (Jeacle, 2017, p. 108). So, too, was the alliance of the scallops, the scientific community, the fishermen and the three scientists (Callon, 1986b, pp. 218–219). The notion of mobilization centers around the establishment of a network spokesperson. Actors involved in problematization, interessement, and enrolment evolve into representatives of larger groups. Larvae that anchored themselves to the collector represented the scallops of St Brieuc Bay. What was true for them – namely that they anchored themselves to the collector – applied for the species in general. Similarly, those scientists who visited the presentations and read the papers of the three biologists at conferences represented the whole scientific community and agreed with the results on behalf of the community. Not all fishermen attended the talks held by the three scientists, but those who did influenced how the fishermen supported the research project. For a while the three scientists spoke for the whole network (Callon, 1986b, pp. 214–216). In the mobilization of DIY, DIY magazines became the representatives for handymen, manufacturers, and retail traders (Jeacle, 2017, p. 107). As long as the mobilized actor-network was stable, the particular actors and the mutual relations among them are not entirely

visible and thus appear to be a black box. They had a stable identity and DIY users or observers could not tell what social relations constituted this identity. Who would have guessed that DIY was translated together with DIY magazines, radio and television, the government, handymen, DIY product manufacturers, and home exhibition organizers unless a researcher opened the black box? Similarly, researchers have opened the black boxes of the ABC costing system (Jones & Dugdale, 2002), standard body sizes (Jeacle, 2003), and observed the becoming of information systems (Hine, 1995). Black boxes are present “when many elements are made to act as one” (Latour, 1987, p. 131) and the simplification of its components into one identity is asserted (Callon, 1986a, p. 29).

However, mobilized actor-networks or black boxes are only temporarily stable. They erode when actors question them. This is what Callon (1986b) calls dissidence. The scallop larvae refused to anchor in sufficient numbers after the first trials. As a result, fishermen refused to stay away from the area of experimentation and fished the bay. Even the researchers’ scientific colleagues ultimately questioned the project (Callon, 1986b). On the other hand, the case of DIY shows how an actor-network identity can remain stable over decades and sustain multinational corporations such as the furniture store IKEA (Jeacle, 2017).

With blockchain technology, nobody knows whether and how it will stabilize. Still, many people invest hope and money in the technology, contribute to its development, adjust their behaviors to it, and attribute it with distinctive features. This is what makes translation a suitable perspective for investigating the blockchain phenomenon. On the other hand, Callon’s (1986b) translation study does not explicitly relate the concept of translation to trust. Nevertheless, there are explicit and implicit connections between translation and trust in the translation-based studies of accounting and organization research. I explore these connections in the following sub-chapter.

3.2.2 How translation studies talk (or do not talk) about trust

In a research seminar in which I presented my work, I received a comment from a highly appreciated and supportive researcher. According to him, a study that draws upon trust and translation was not very original, as the two concepts are obviously interrelated. The intuition of that researcher was similar to mine, though he was surprised when I told him that there was little research which combined trust and ANT. In the following, I sketch out where our intuitive connection of ANT and translation might derive from. In order to do so, I review studies in sociology, organizational research, and accounting that draw upon the notion of translation and touch upon various ontologies of trust, both implicitly and explicitly. By

ontologies I refer to the circumstance that trust is enacted as various things and is attributed with different characteristics (Woolgar & Lezaun, 2013). Although only some of these studies explicitly refer to Callon's (1986b) framework, I look at them through the lens of the four moments described above in order to identify potential connections for further discussion.

Problematization

Sub-chapter 3.2.1 indicates that the sources of problematization can be diverse. With regard to trust, Jones and Dugdale (2002) identify the construction of a "crisis of trust" (p. 154) as the beginning of ABC's translation. This historical ANT study describes how, in the 1980s, formerly stable accounting knowledge and practices were questioned when "managers no longer accepted taken-for-granted costs" (Jones & Dugdale, 2002, p. 154). This indicates that decreased trust in formerly stable actor-networks, such as accounting knowledge and practices, may trigger the translation of new actors, e.g. a new costing approach. The destabilizing or dissidence of an actor-network comes with former supporters' loss of trust. In response, the actor that constituted an obligatory passage point for solving this problem - ABC - "pledged more trustworthy knowledge" (Jones & Dugdale, 2002, p. 154). Although not labeled as a trust crisis, a similar situation occurred in Australia prior to the development of a management accounting system in the country's healthcare sector. In that case, the public was concerned about a lack of accountability, efficiency and squander of the administrations. Also the medical profession faced "government and community concerns" (Chua, 1995, p. 119). The trust crises consisted of a loss of trust in a system or institution. As Möllering (2006a) points out, "trust in an institution means confidence in the institution's reliable functioning" (p. 74), as does trust in a system (Giddens, 1990; Luhmann, 1979). In these two cases, this institutional form of trust declined as actors questioned the reliable functioning of established systems. These two examples indicate that trust crises can constitute problems, which give rise to translations of new actors.

Interessement

In an ANT-study on network enterprises, Mouritsen and Thrane (2006) describe trust as an aspiration or ideology for relations between human actors within a network. The actor-networks in this study were network enterprises - inter-organizational relations of firms and / or people connected through a network. The partners in this network associated with trust their expectations about non-hierarchical relations, mutual support, and knowledge sharing among network members. Although the authors never labelled this "ideology of trusting" (Mouritsen & Thrane, 2006, p. 270) an interessement device, it nevertheless helped determine

the relations within the network, and to distinguish its identity from other types of enterprises (Mouritsen & Thrane, 2006, pp. 249–250). Framing trust as an ideology for inter-organizational relations follows an assumption of trust research, namely that trust is a precondition for inter-organizational relations (Lane, 1998; Stevens et al., 2015). However, Mouritsen and Thrane (2006) observe that network enterprises did not adhere to this ideology and that trust relations were rather absent. The translation of actors and their relations also seemed to carry the ideology of trust in other directions, as I will illustrate under Enrolment.

Other interessement devices imply additional ontologies of trust. An interessement device, for example, can contribute to an image of reasonable trustworthiness, especially the integrity (Mayer et al., 1995) of an identified problem. In the case of the translation of DIY, the interessement device of labor cost savings supported the problems of a housing shortage and manpower bottleneck. So “the calculative technology of labour cost saving [interessement device] gave credence to the problem for which DIY was the solution” (Jeacle, 2017, p. 106).

In a case whereby standard sizes in the fashion industry were established, Jeacle (2003) implicitly describes how accounting control procedures functioned like interessement devices to reveal an abuse of trust in established relations between actors. While department buyers used to accept the delivery of goods from cloth-makers without quality control, an interessement device in the form of recommendations for incoming controls promised to expose manufacturers that did not adhere to agreed standards (Jeacle, 2003, pp. 365–366). Similarly, transparency on alteration costs per department of stores revealed department buyer’s intentions to hide from management the follow-up costs of their erroneous procurements (Jeacle, 2003, p. 368). In both of these relations, the interessement devices made visible the hidden intentions, which dispelled actor’s trustworthiness. Before the interessement devices came into play, the relations between department buyers, cloth-makers, and store management were more or less taken-for-granted. Their relations seemed to be determined by routines, which were not questioned until interessement devices were introduced in the form of accounting control technologies. Remembering Möllering’s (2006a) words, “when trust is a matter of routine, [...] the routine is performed without questioning its underlying assumptions, without assessing alternatives and without giving justifications every time” (p. 52). From the descriptions in Jeacle’s (2003) case, I cannot tell whether any of the actors were disappointed when interessement devices revealed that buyer’s and cloth-manufacturers’ reasonable behavior could not be taken for granted. Nevertheless, interessement devices in this particular case intervened in routine-based trusting relations; in the other case, these devices supported the trustworthiness of a stated problem.

At the same time there are translations where existing trust between actors contributes to *interessement*. In the translation of an accounting system in Australia's healthcare sector, trusting relations between people and between people and an accounting system, contributed to *interessement*: One hospital CEO was already well acquainted with both the newly proposed accounting system and the university experts involved (Chua, 1995, pp. 123–124). Chua (1995) describes the relation between the hospital and the university experts:

The University team was trusted as a neutral mediator who would ensure that sensitive hospital-specific information would either be kept confidential or be fairly traded among the three hospitals. The two DRG experts, in particular, were well known to staff from all three hospitals. (Chua, 1995, p. 124)

In this constellation, there seems to exist a trust between the hospital CEO and the accounting system, which is based on familiarity (Möllering, 2006a). Moreover, the hospital leadership and hospital staff's trust in the university team appears to be based on preceding trust building processes as well as the institutionalized role of the university experts as neutral actors (Möllering, 2006a). Similar relations also appear in the enrolment phase.

Enrolment

Enrolment is the moment when relations are negotiated and tested. There are multiple ontologies of trust, which appear in these moments of relating actors. Trust in human or in non-human actors can be both the input or the outcome of enrolment; it can also be a problematizing device which lacks trust in an organization.

Mouritsen and Thrane (2006) describe enrolment when they observe that “trust is a test” (p. 271). Network partners referred to trust when expressing how relations between partner enterprises were not determined by trust as suggested by the networks' ideology. Thus, trust became a “problematizing device” (Mouritsen & Thrane, 2006, p. 273) in the sense that it became a moralizing narrative in cases when actors behaved contradictory to the trust ideology of a network – which is most of the time in inter-organizational relations (Mouritsen & Thrane, 2006).

In the translation of standard sizing in the fashion industry, trust between human actors was built during enrolment. Recording deviations from agreed fit sizes incentivized manufacturers to adhere to standards agreed upon by stores and manufacturers. Similarly, the proportional assignment of alteration costs to different departments incentivized department buyers to avoid dishonest actions and enroll in standardized sizing systems. Thus, new accounting practices, which served as incentives aligned the interests of several actors. From a rational trust theory perspective (Möllering, 2006a), incentives explain how trust was

facilitated among department buyers and manufacturers, as well as how managers and controllers established trust in the department buyers. On the other hand, this assertion provokes Möllering's (2006a) argument that rational trust theories "explain trust away" (p. 43) as they explain how uncertainties are reduced rather than dealt with. In this sense, one could assume that incentives, rather than creating trust, actually lowered actor's needs to trust each other. Moreover, accounting practices triggered enrolments of manufacturers with buyers which were described as "co-operative and [...] cordial (Abbott, 1929, p. 182)" (Jeacle, 2003, p. 369) interactions and relations whereby actors strived toward problem-solving in cases of ill-fitting clothes. This example indicates that through mastering critical situations together, reflexive trust building in the buyer-supplier relationships emerges (Möllering, 2006a, p. 188).

Trust in non-human actors played a pivotal role in many other translation cases. Trust served as an input as well as an outcome of enrolment. In the case of a management accounting system in Australia's healthcare sector, trust in the institutionalized role of university experts – similar to *interessement* – seemed to enhance trust in accounting numbers which were fabricated in the project: "Experts legitimated and contributed additional degrees of credibility to the accounting numbers produced" (Chua, 1995, p. 137). Similarly, the enrolment of trusted research institutions in the development of a new, common taxonomy in the biological research community facilitated actors' trust in the developing taxonomy database. The following quote illustrates the function of institutions as facilitators of trust (3.1.2).

The legitimacy of the ILDIS project [development of taxonomy database] to speak for specialists in this family of plants to the world depended on persuading the participants, recognized experts, to lend their names and affiliations to ILDIS. Similarly, the user organizations, publishers, and scientific institutions were their credentials to the project. (Hine, 1995, p. 74)

Existing trusting relations – as described under *interessement* – may also serve as inputs to enrolment processes. In the translation of a municipal government's financial reporting application Holmström and Robey (2005) observe that the politicians' enrolment in the system was initiated through a "positive relation" (p. 178) between politicians and the technicians who worked on the project. I ascribe this relation with a degree of trust, since it helped to gain (financial) supporter by the politicians for an unfinished IT artifact (Holmström & Robey, 2005, p. 178).

Moreover, network members' strong belief in a non-human actor can help enroll other actors. In the case of the taxonomy database, people joined the development of the database

because of the “personal enthusiasm of the main organizer” (Hine, 1995, p. 75). From the case study on the healthcare sector accounting system, Chua (1995) derives that translated non-human actors rely on believers (p. 138). Hence, to start enrolment, actors depend on the confidence and bracketing of uncertainties (Möllering, 2006a, pp. 115–119) by some actors:

A piece of software is weak if left to speak for itself. New inscriptions need spokespersons – people who genuinely believe in their utility and final, comparative advantage over competitors [...] the willingness of someone to do battle on behalf of an untried technology has ultimately to be based on faith because one does not know in advance that one will eventually win. (Chua, 1995, p. 132)

In the case of the healthcare accounting system, there has to be a belief in an idea before the IT artifact is operational or perceived as trustworthy. And even when trials or negotiations – as Callon (1986b) calls them – were already conducted, enrolment seems to require a certain bracketing of uncertainties. This was the case with the scientists in St. Brieuc Bay who “were prepared to believe in the principle of anchorage and [...] judged the experiment to be convincing” (Callon, 1986b, p. 213); it was the case with controllers in an IT project who – based on the information and training regarding the IT system under development – “believed that Powerplay [financial reporting application under development] had potential” (Holmström & Robey, 2005, p. 177). The examples of the accounting system, the taxonomy database, the scientific research project on scallops, and the IT application all refer to non-human actors which invoke a vocabulary of “belief” and “faith” that suspends uncertainty (Möllering, 2006a, p. 111).

According to Zand’s (1972) trust spiral, trust leads to more trust. This appears to be the case in the translation of a financial reporting application where reputation of an IT artifact that was based on first experiences ultimately contributed to the enrolment of more actors. The positive experiences with an IT application served as a reference, and as people spread the word, the enrolment of more people was supported (Holmström & Robey, 2005, p. 181). This indicates that process-based trust in the system (trust in its reputation) (Zucker, 1986) leads to trust by other actors. Trust in non-human actors, which results from past experiences among several network actors also appears in other constellations. In the case of the taxonomy database, the IT system enforced participants’ cooperation in producing data to create a “consensus on a worldwide classification system” (Hine, 1995, p. 74). Hence the joint efforts and negotiations of participants, in addition to the data for the database, were essential in working toward the goal of recording in the database a “stable “best guess” as to the state of the natural world” (Hine, 1995, p. 78). Thus, the reflexive interactions of different participants with each other and with the data helped participants trust the data enough to present it as

stable facts to others. Similarly, in the case of the hospital accounting system, the joint generation of the system in the network led to joint problem-solving and rule agreements for dealing with system deficits (Chua, 1995, pp. 135–136). The direct and playful interaction with the system lead to familiarity with the system (Chua, 1995, p. 132). Together these enrolment activities resulted in a close relation between project participants and the accounting system – so much so that nobody doubted the system in spite of all of its deficiencies (Chua, 1995, pp. 133–137).

Overall, enrolment is about reflexive interactions, which render reflexive trust building visible. Trust based on reason, routine, and reflexivity appears as an input for enrolment, while trust based on reflexivity appears as an outcome of enrolment.

Mobilization and black boxes

The dynamics of translation highlight the ways in which systems become stabilized and how black boxes are made. There are many studies which observe technologies while they are still under development (Hine, 1995), as well as historical studies which open black boxes and investigate the translations that led to a temporarily stable condition (Jones & Dugdale, 2002). Jones and Dugdale (2002) explicitly equate the theoretical concepts of ANT's black boxes (Latour, 1987) with abstract systems (Giddens, 1990) when they theorize the translation of ABC accounting systems: "Looking at ABC today we see a ready-made costing system that has the appearance of certainty and solidity. It is a disembedded global expert system¹⁷ that spans continents [...] It is, in Latour's terms, a 'black box'" (Jones & Dugdale, 2002, p. 125). This comparison¹⁸ implies that system trust (Giddens, 1990; Luhmann, 1979) and the acceptance of black boxes are theoretical constructs, which describe the same temporarily stabilized phenomenon. The term ABC, for example, assembled management philosophies, practices, and ERP systems that were trusted to improve management control (Jones & Dugdale, 2002). This sort of system trust or trust in black boxes is immanent to these systems. Black boxes build on the simplification of connections and hide the production mechanisms of technical systems. As long as the black box mobilizes other actors, trust in a black box implies a trust in its technical and human parts. The detailed interrelations within a black box are difficult to understand for other actors (Callon, 1986a). This necessarily produces uncertainties and dependencies which people respond to with trust (Luhmann, 1979,

¹⁷ Jones and Dugdale (2002) use the terms expert system and abstract system interchangeably.

¹⁸ I want to thank Fabian Muniesa, who drew my attention to the proximity of black boxes and trust in the first place and thus helped me discover this link in the literature.

p. 50). When dissidences that destabilize the black box occur, the actor-network breaks down into a collection of separate actors who have no common identity (Callon, 1986a).

As indicated in the sections on interessement and enrolment, stabilized and trusted actors can mediate between other actors in translation processes. In the mobilization process of the standard body sizing, a broadly accepted actor mediated retailers that did not trust each other. Governmental studies on body measurements “converted standard sizing into a public commodity” (Jeacle, 2003, p. 370), although it had been a business secret of competing retailers and gone unshared even within retailer’s own workforces (Jeacle, 2003, p. 370). In the case of network enterprises, management control technologies mediated the relation between partners in networks. Mouritsen and Thrane (2006) describe the attitude of partners towards the management control technologies in enterprise networks as trusting of the control tool’s ability to predictably organize and execute transactions between firms. This trust was based on a partner’s agreement concerning the tool’s rules (Mouritsen & Thrane, 2006, p. 267) and systematics (Mouritsen & Thrane, 2006, p. 270). They in turn stabilized the relation between partners by creating practices where actors did not need to trust each other’s intentions, but instead rely on management control technology mechanisms (Mouritsen & Thrane, 2006). This case is similar to other phenomena where systems or institutions act as facilitators of trust and as trustees (Möllering, 2006a, p. 74). However, trust in management control technologies was derived from the agency of the system, which outlived even the individual partners in a network (Mouritsen & Thrane, 2006, pp. 271–272).

Dissidences or trust crises

If mobilized black boxes are trusted systems, then dissidences are trust crises. Such crises occur when actors lose confidence in and question the functioning of a system or institution (Möllering, 2006a, p. 74). As examples of problematization show, a trust crisis can give rise to additional translations.

The examples taken from studies of translation make explicit and implicit references to trust, giving us reason to assume that translation is intertwined with different ontologies of trust. A trust crisis is a dissidence which can constitute a problem for translation. The ideology of trust can serve as an interessement device. Other interessement devices, in turn, can give credibility to a proposed problem or render taken-for-granted routines visible. Existing relations between actors serves as an input to interessement as well as enrolment. This includes relations between people, but also between human and non-human actors. Another enabler of enrolment is trust in institutionalized roles and the faith of people in (still

developing) non-human actors. On the other hand, enrolment also creates trust through the establishment of incentives; trusting relations between humans and between human and non-human actors are also established through cooperation, experiences, and problem-solving. In moments of mobilization, black boxes become trusted systems. Relations within these actor-networks include trusting relations facilitated by non-human actors. As most studies either do not explicitly use Callon's (1986b) framework or do not explicitly refer to ontologies of trust, the connections between the concepts which I have outlined in this sub-chapter remain rather speculative. However, my analysis will explicitly relate the two theoretical perspectives of trust and translation outlined before. In doing so I aim to enrich our understanding of trust in information technologies with a process perspective, and with a view which affords attention to the multiple actors involved, including agentic non-human actors. Thus, with regard to blockchain technology – which is still “in the making” (Latour, 1987) – I relate my research question “What is the role of trust in the creation of blockchain technologies?” to three empirical questions: Which ontologies of trust were rendered visible during the translation of blockchain platforms? Which forms of trust and trust building were used? Which attempts failed? In the following chapter I present the methodology and method used to investigate these questions. I then provide an introduction to the two case studies that I analyze as examples of blockchain technology.

4 Methodology, method, and case background

The blockchain phenomenon and the theoretical background I have chosen to study its emergence have implications for my research methodology, method, and case selection. My qualitative research is influenced by ANT and abductive reasoning. In the following, I first describe the collection and interpretation of empirical data (4.1). Thereafter I introduce my two cases – Ethereum and Hyperledger Fabric – and explain why I selected them as examples of blockchain technology used by business organizations (4.2).

4.1 Research methodology and method

In order to describe the translation of blockchain technology and to explore its contribution to trust research, I chose a mainly qualitative empirical research approach. Qualitative research is sensible for exploring, describing, and understanding the social construction of a wide range of phenomena (Flick, Kardorff, & Steinke, 2004). This approach is suitable, given the novelty of blockchain technology and the scarce of focus on trust in information technologies within the literature on trust in organization studies. A mainly qualitative approach is also in line with the trust research community's call for qualitative studies, which seeks to complement trust research's strong bias towards quantitative studies (Li, 2017) and positivism (Isaeva, Bachmann, Bristow, & Saunders, 2015). My empirical research draws upon two cases (Yin, 2014) of multi-purpose blockchain platforms that address business organizations: Ethereum and Hyperledger Fabric. According to the ANT paradigm's methodological suggestions to "follow the actors" (Latour, 2005, p. 12), I follow the two blockchain platforms over an excerpt in time. My case study research has several goals: First, based on the empirical cases of the blockchain platforms Ethereum and Hyperledger Fabric, I describe the emergence of blockchain technology as a socio-technological phenomenon. Second, these cases serve as distinct examples of trust ontologies and trust building mechanisms, which involve technical actors in a translation process.

My methodology is influenced by the descriptive attitude of STS, in particular ANT (Latour, 2005), and by abductive reasoning (Alvesson & Sköldbberg, 2012). As my supervisor phrased it in an early conversation about my research project: "Your method is called describing and thinking." I provide descriptions of both cases through the theoretical lens of translation (3.2) and confront them with theoretical constructs on trust (3.1). First conceptualized by Charles Sanders Peirce (1998), abduction is a search for surprises which motivates scholars to modify or dismiss assumptions and produce new understandings (Reichertz, 2004). This search confronts empirics with existing theory (Alvesson

& Sköldbberg, 2012, p. 4) and provokes critical contemplation (Alvesson & Kärreman, 2007, p. 1265). Typical questions that lead my research include “What is going on here?”; “Can I construct/make sense out of this material in another way than suggested by the preferred perspective/vocabulary?” (Alvesson & Kärreman, 2007, p. 1270); “Is that conjecture interesting?” (Weick, 1989, p. 525). In following these questions my methodology is abductive. Along the lines of translation, my research is guided by principles of ANT and influenced by attitudes from STS’ research on “virtual worlds” as socio-technical networks (Plesner & Phillips, 2014b). As Plesner (2014) articulates:

ANT is a sociological theory with particular methodological implications. The basic assumption is that social phenomena consist of networks of a multitude of human and nonhuman, social and technical elements, and to understand those phenomena, we need to study how networks are assembled. (Plesner, 2014, pp. 18–19)

This “relational ontology” (Plesner & Phillips, 2014a, p. 8) has influenced many researchers of virtual worlds. In my empirical studies I consider blockchain technologies as socio-technical networks (Bijker & Law, 1992; Plesner & Phillips, 2014a, p. 8), actor-networks (Latour, 2005) or virtual worlds; in other words, as “complex ensembles of technology, humans, symbols, discourses and economic structures, ensembles that emerge in ongoing practices and specific situations” (Plesner & Phillips, 2014a, p. 1). Making use of Plesner’s (2014) explicit language, these “terms imply a research strategy of following the gradual establishment of assemblages of elements into more solid parts of reality” (p. 19). The outcome of an ANT-based study is a precise description (Latour, 2005, p. 123). Its purpose is to observe, discover, and describe social relations among observed actors (Latour, 2005, p. 138). Observations and descriptions follow ANT’s methodological principles of agnosticism on behalf of the researcher, symmetry between society and nature, and free association (Callon, 1986b, pp. 200–201). Agnosticism is an open-minded attitude toward actors and their relations. The researcher must not censor the actor’s descriptions, interpretations, or opinions about the social and the natural world, but instead remain attentive to actors’ movements, transitions, and perceptions of the social world. Agnosticism in social sciences is an everlasting center of conflict. While some methodologies, such as grounded theory (B. G. Glaser & Strauss, 1967) and Gioia methodology (Gioia, Corley, & Hamilton, 2013) claim that impartiality towards the object of investigation is possible, others oppose this claim (Alvesson & Kärreman, 2007). According to this opposition, researchers are humans with theoretical foreknowledge and intuition, which cannot and should not be ignored. This is where abduction comes into play and allows me to complement my descriptions with

theoretical foreknowledge. My reflections on organizational trust research using the categories of Möllering's (2006a) integrative trust framework make this explicit. The symmetry of society and nature refers to an interpretive and linguistic equality of human and non-human actors in the descriptions of the researcher. Callon's (1986b) translation vocabulary provides one possibility for adhering to this principle (p. 200). Free association stresses the fluent transformations of actors and their relations. With this methodological approach I hope to enrich a trust research landscape which aims for more epistemological diversity (Isaeva et al., 2015).

My case study research draws upon a broad range of empirical data that I have triangulated (Flick, 2004). With this approach, I aimed to gain knowledge about the translation of two blockchain platforms between 2013 and 2018 and to follow the actors in these respective arenas. Similar to Bitcoin, Ethereum and Hyperledger Fabric were not only too globally scattered and messy to be studied as bounded constellations (Kavanagh et al., 2019, p. 532), but their social interactions were also dispersed among temporary virtual and physical locations. In agreement with Kavanagh et al. (2019), I believe that local context in blockchain's virtual world is less of importance than in other contexts (p. 528). For example, the Ethereum platform was developed, used, and interpreted by people and computers spread around the world; from the Ethereum website one could already see that these actors interacted through conferences, local meetings, blogs, websites, social media, forums, internet calls, and cryptocurrency exchanges (Ethereum, n.d.a). Vitalik Buterin, the inventor of Ethereum, apparently has no permanent residence and keeps his belongings in one travel bag while travelling around the world (Cornish, 2018). When I asked a blockchain reporter for support with establishing contacts to the Ethereum team, I ended up with a list of email addresses from people spread over Europe, North and South America. Blog entries on the Hyperledger Blog span developments in Australia, Asia, Europe and North America. Consequently, I followed the traces of Ethereum and Hyperledger Fabric online and offline and let actors in the field direct me towards historical and current data in various virtual and physical contexts. This interesting and sometimes confusing experience is similar to other ANT-based studies on virtual world innovations, which tend to span frontiers and yield much of their data from cyberspace (Plesner, 2014, p. 22).

In order to grasp the phenomenon at hand, and select cases and information sources, I visited four practitioner conferences, four blockchain meetups, and a hackathon between 2017 and 2018. These events took place in Germany and Ireland – the two countries where I was physically located for my research. However, the empirical analysis presented hereafter draws

mainly upon the triangulation of data collected from fieldwork via cyberspace and interviews (Czarniawska, 2014). To capture the development of the two platforms over time, I collected data primarily through the web and press research, and supplemented these sources with 12 semi-structured interviews. The analysis of documents such as web texts and blogs in combination with other data collection methods like video recordings and interviews is often applied in case study research on virtual worlds (Plesner & Phillips, 2014a, p. 9). The gathering of my data took place between July 2017 and May 2018 and covered information until end of April 2018.¹⁹ During this time, I reviewed the webpages of Ethereum, Hyperledger, and IBM; I retrieved 515 blog entries from Ethereum blogs, the Hyperledger Foundation, and IBM’s international blockchain blogs. These blogs have mainly been written by respective developers, managers, consultants, and PR specialists. Table 1 gives an overview of the different blogs which were used in this study, along with the number of entries from each blog and their publication dates.

Blog	Number of blog entries	Time frame of blog posts
https://blog.ethereum.org/	227	December 31, 2013 – April 1, 2018
https://www.hyperledger.org/blog	143	September 13, 2016 – April 26, 2018
https://www.ibm.com/blogs/blockchain	117	October 20, 2016 – April 30, 2018
https://developer.ibm.com/blockchain ²⁰	30	September 21, 2015 – March 19, 2018

Table 1: Overview of retrievals of blog entries from the blogs of Ethereum, Hyperledger Foundation and IBM’s international blockchain blogs

From the Ethereum and Hyperledger websites, blog entries and their authors, I was directed toward other sources. These sources then pointed at each other and back toward blog entries, e.g. books, white papers, reports, videos on YouTube, websites of blockchain projects and firms, blogs, forums and social media networks. To give an example, blog entries hinted at events such as fairs, conferences, and local meetings, which were sometime video recorded and made accessible on YouTube. I also conducted supplementary searches on human and technical actors involved with the Ethereum or Hyperledger Fabric platform through google.com, linkedin.com, and on the blockchain-specific online news page *Coindesk*. My documentary sampling was supplemented in November 2017 and in May 2018 by a structured press search through Factiva.^{21,22} Here I retrieved articles from eight English and German

¹⁹ I made one exception and incorporated later a Hyperledger white paper Hyperledger (2018g), which reflected earlier statements from the Hyperledger blog.

²⁰ By the time of publishing, this URL was not online anymore.

²¹ Less structured press clippings had been collected previously in order to achieve a general understanding of blockchain technology. On November 20, 2017 I conducted the structured press clipping as described below. In May 2018 I repeated the same search for the time period between November 21, 2018 and April 20, 2018.

speaking high-quality newspapers, business journals, and magazines from the USA, UK and Germany. I used these sources' online and international editions and complemented them with a search of material covering the period between 2013 and April 2018 on the Harvard Business Review website. Table 2 shows a summary of the nine press sources. I conducted the press research on Factiva with the search terms “(Ethereum) OR (Vitalik Buterin)”²³ which yielded 549 publications²⁴ “Hyperledger OR (IBM and blockchain) OR (Linux and blockchain)”²⁵ yielded 213 publications.²⁶ The Harvard Business Review website did not respond to Boolean search operators. Therefore I searched separately for “Ethereum”, which yielded 10 articles – and for “Hyperledger Fabric”, which yielded 1 article.

Headquarters Country	United States of America	United Kingdom	Germany
Press Type			
Newspaper	The New York Times – All sources	The Times (U.K.)	Frankfurter Allgemeine Zeitung – All sources
Business Journal	The Wall Street Journal – All sources	Financial Times – All sources	Handelsblatt – All sources
Business Magazine	Harvard Business Review <i>(no Factiva access, web search on hbr.org)</i>	The Economist – All sources	Wirtschaftswoche Or WirtschaftsWoche Online

Table 2: Overview of press search

My data collection was complemented with 12 semi-structured interviews. These interviews were conducted with actors participating in or observing the emergence of Ethereum and Hyperledger Fabric. All interviews consisted of either one or two interviewees. I interviewed six managers from information technology and/or consulting firms who had worked on blockchain projects, two members of the Ethereum team, one software developer from the Ethereum community, one blockchain reporter, two advisors for blockchain startups, and one information technology professor conducting research in the field of blockchain

²² Factiva is a commercial global news database provided by Dow Jones.

²³ Due to his popularity I complemented the search term Ethereum with the name of its inventor, Vitalik Buterin, in order to grasp information that was related to his involvement with other actors.

²⁴ The number excludes articles filtered as “similar duplicates” in Factiva and sums up the searches from November 2017 and May 2018.

²⁵ Before 2016 Hyperledger Fabric changed its name several times. Thus I complemented the search term with the more generic description of the platform that involved IBM and Linux Foundation, which involved with the platform very early.

²⁶ Excl. publications filtered as “similar duplicates” in Factiva.

technology. Interviews were conducted between November 2017 and March 2018 in English or German. During my visits at conferences and events as well as in the documentary analysis, I noticed that most actors in the field communicated informally. Moreover, trust appeared as a generally sensitive topic (Lyon et al., 2015). Thus, I established initial contacts with interviewees either personally at events such as conferences, hackathons, and meetups or through contacts, especially through the blockchain researcher group at University College Dublin.

I aimed to create an informal atmosphere for interviewees. I asked participants in interviews to tell me about the emergence of the platforms and other actors, their interactions with the platforms and with other actors, the differences between the platforms and trust. Interviews lasted between 45 minutes and 125 minutes. Eight interviews were conducted in person, and three were conducted via Skype. One interview was conducted in person and was continued via Skype because we ran out of time during the first meeting. During the interviews, interviewees were located in Brazil, Germany, Ireland, and USA.²⁷ The dispersion of my interviewees' locations mirrors the globality of Ethereum and Hyperledger Fabric, which also appears in the textual material and video sources mentioned above. All interviews were recorded and transcribed. Quotes in the German language were translated into English for chapters 5 and 6. All data was collected, stored and organized in the reference and knowledge management program Citavi.

As data from online and offline contexts are inextricably linked with each other (Kozinets, 2015, p. 69), I refrained from distinguishing between “the virtual” and “the real” (Plesner & Phillips, 2014a, p. 4). In an ANT sense, I considered these materials as traces in the translation process (Latour, 2005). Once I had selected the cases and started to retrieve written material, I paid attention to actors, events, and relations, which “[made] a difference” (Latour, 2005, p. 71) with regard to trust. I continued doing this with the interview material as well. I repeatedly confronted my empirical sources with categories from ANT and trust research. I interpreted the data by writing descriptions which followed ANT's moments of translation; I also regularly confronted data with trust theories. This was by no means a linear process, but a reflexive and iterative process of gathering data, reviewing and excerpting data, writing descriptions and theoretical interpretations (Alvesson & Kärreman, 2007). When I started my research on blockchain technology, I had no previous knowledge about or practical experience with blockchain technology. With my experience of conducting interviews, my

²⁷ In alphabetical order.

deepening understanding of Ethereum and Hyperledger Fabric's technological dimensions, and my growing knowledge of organizational trust literature, I continuously viewed material which had been gathered at the beginning of my research in a different light later on. I regularly discussed and revised my findings with other researchers in my research group at the Helmut-Schmidt-University between 2017 and 2019. I also discussed interim findings during my research stay with the Management Information Systems Group at University College Dublin and at the EGOS Pre-Colloquium PhD Workshop in 2018. As I never invested in any blockchain project or cryptocurrency or became part of any blockchain community, I had no personal preferences about the outcomes of the technical, regulatory, economic or social development of specific platforms. Also, studies or client projects conducted by my employer, Bain & Company, on blockchain technology have not been part of my research process.²⁸ I travelled light and with curiosity. In the following I explain why I selected the two case studies and provide a brief background description for each.

4.2 Context of the Ethereum and Hyperledger Fabric cases

Over the past years, a variety of blockchain platforms and applications have emerged across the globe (F. Glaser, 2017; Macdonald, Liu-Thorrold, & Julien, 2017). In order to study the social phenomena of translation and trust as they relate to blockchain technology, I chose the platforms Ethereum and Hyperledger Fabric. This choice was based on these platforms' differences and similarities (Yin, 2014). Both served as examples for one phenomenon – blockchain technology. This thesis contributes to trust research in organizational studies, a discipline of business and management studies. Consequently, I decided to select blockchain platforms, which were already being discussed and experimented on by business organizations at the time of my decision in 2017.²⁹ Technically, both platforms structure transactional data in blocks that constitute blockchains.³⁰ Moreover, both provide the basis for programming blockchain-based smart contracts and applications. Both platforms are based on open source software, and have been discussed in public discourse; in both cases, key stakeholders have articulated themselves in cyberspace, e.g. through blogs. Ethereum and Hyperledger Fabric have both been promoted and supported at conferences, local meetings,

²⁸ I was on an educational leave during my research project.

²⁹ Indications from working papers (Valenta & Sandner, 2017; Macdonald, Liu-Thorrold, & Julien, 2017) that Ethereum and Hyperledger Fabric were in the making and at the same time being used by enterprises were confirmed during presentations and conversations at blockchain conferences and meetups that I attended in June and July 2017.

³⁰ This is worth mentioning because there were also platforms emerging under the broader label Distributed Ledger Technology (DLT), structuring transactions differently than in blocks (Iota Foundation, n.d.), (Hedera Hashgraph, n.d.).

online blogs, on social media, and in forums by assembled communities of software developers. On the other hand, although it has a developer community, Bitcoin has been considered less of a blockchain platform for enterprises – at least until 2017. This was the impression that I gathered from visiting conferences, which was later confirmed in interviews when managers from consulting and information technology firms told me they were trying to explain to their clients the advantages of Bitcoin. Lastly, Ethereum and Hyperledger Fabric are platforms which provide a base for applications in multiple industries, for example financial services, healthcare, or supply chains (Valenta & Sandner, 2017, p. 1). Bitcoin was initially a platform for Bitcoin payment (Nakamoto, 2008), and has also been used for the foreign transfer of bitcoins, (Böhme et al., 2015, pp. 222–225) and as financial assets (Dallyn, 2017; F. Glaser et al., 2014). Corda and Ripple (Ripple, n.d.) are other blockchain platforms whose development have been fairly advanced but focused mainly on the financial services industry (Valenta & Sandner, 2017). Bitcoin, Corda and Ripple were therefore not considered as case studies for this research.

On the other hand, Ethereum and Hyperledger Fabric have substantial differences in their ideology, organizational foundation, and technical architecture. Speaking with Swartz's (2017) categories, Ethereum is more on the radical side of blockchain dreams, while Hyperledger Fabric represents a more incorporative project. Ethereum was first announced in 2014 by its inventor Vitalik Buterin, at the time a 19-year old college dropout from computer science who had been passionate about Bitcoin and cryptocurrencies (Cornish, 2018). Bitcoin had been released in the course of the financial crisis and drew on decreasing trust in established institutions, such as the global financial system and national governments (2.1). Involved in a Bitcoin-related development project (Buterin, 2017) and writing for the Bitcoin Magazine (Cornish, 2018), Vitalik Buterin was a part of the Bitcoin community. With a small team of volunteers (Buterin, 2017), his idea was to create a general-purpose blockchain platform which could overcome Bitcoin's technical limitations and make blockchain technology available for applications other than bitcoin transactions (Buterin, 2014i). In 2014, together with his allies, Buterin formalized the economic and legal activities necessary for Ethereum through the Switzerland-based Ethereum Foundation. This foundation gathered funding for the platform's development and created the open source platform in cooperation with a growing community (Gerring, 2016). Hyperledger Fabric was initially developed

starting in 2015 by the multinational information technology company IBM.³¹ Shortly after the platform was transferred to the governance of The Linux Foundation as open source code, it became the first project under its Hyperledger initiative for blockchain development (Cuomo, 2015b). While the Ethereum platform had arisen from the activities of an evolving network of loosely related actors, Hyperledger Fabric was built on the shoulders of a multinational technology company and a renowned foundation for software development.

The technical characteristics of the two platforms differ strongly as well. First of all, Ethereum provides a public platform with one shared database, which is accessible for any user and all software applications. Hyperledger Fabric is a modular software architecture (Androulaki et al., 2018) that can be used to create separate blockchain networks within defined groups; it does not have one common database like Ethereum or Bitcoin where transaction data is made publicly accessible. Moreover, Ethereum relies on the provision of computational capacities by its community for storing data and validating platform transactions. Transaction validation is conducted through a so called proof-of-work consensus algorithm (Wood, 2014), which is similar to the one Bitcoin has employed (Buterin, 2017). Participants have been incentivized with earnings from the platform's own cryptocurrency, Ether. The processing of transactions on the platform is paid for in Ether (Wood, 2014). In 2018, Ether was among the largest cryptocurrencies in terms of total value (Coindesk, 2018, p. 6). Hyperledger Fabric, in turn, has no proprietary cryptocurrency. Moreover, it does not rely on a specific validation mechanism, like Ethereum, but aims at developing a plug and play architecture so that different networks based on Hyperledger Fabric can run with different consensus algorithms. Hyperledger Fabric networks are not intended to run on anonymous participants' computational devices, but on permissioned computational devices (Androulaki et al., 2018), i.e. those determined by a group which has agreed to run a network together.

The following empirical descriptions (5, 6) and the subsequent discussion (7) will show how some of these similarities and differences have had implications for these platforms' translations as well as the ontologies of trust, which have developed there. Although these case studies are structured along Callon's (1986b) translation framework, they cannot be understood as historical or as complete depictions of the field. Moments of translation have temporal overlaps (Callon, 1986b, p. 203), and thus help explain the phenomenon

³¹ When Hyperledger Fabric was transferred to the governance of the Linux Foundation, the project was called Open Ledger Project. IBM's initial platform, which became Hyperledger Fabric was called open block chain (Cuomo, 2015b). Shortly thereafter, it was officially renamed into Hyperledger Fabric.

analytically, not chronologically. My aim is to explore the role of trust in the processes when these platforms were being created. Therefore, I have selected only those snippets from the empirical material, which I consider related to trust. This emphasis has also lead me to focus on those actors, which I saw associated with trust. This emphasis has resulted in an emphasis on human actors. The early stage of the development of blockchain technology and my macro perspective have also revealed a noticeable share of narratives in translation processes. At the time of writing, both platforms are still under development. Thus, only time will tell if and in which form these or other blockchain platforms will become trusted parts of our daily lives or interact with larger technical infrastructures.

5 Ethereum

In this chapter, I explore the role of trust in the translation of Ethereum. I describe the four moments of translation in this case, and reflect on these in relation to Möllering's (2006a) integrative trust framework. Multiple ontologies of trust were borne out of Ethereum's translation between the end of 2013 and the beginning of 2018. As Callon (1986b) points out, "translation is a process before it is a result" (p. 224). This is especially the case with the blockchain platforms Ethereum (5) and Hyperledger Fabric (6). In both cases at the time of writing, it was not clear if and for how long they would become stable socio-technical networks.

5.1 Problematization: Trust crises

5.1.1 Translation

Problems are constitutive to problematization in translation (Callon, 1986b). In chapter 2.1, I outlined how Bitcoin emerged during the course of the global financial crisis – a crisis of public trust in actors of the global financial system (Gillespie & Hurley, 2013), which also found its way into the problematization of Bitcoin. Bitcoin was suggested as a solution to this crisis insofar as it provided an alternative digital currency and technological infrastructure independent of established financial and governmental institutions (2.1). Ethereum's initial problematization was related to Bitcoin's problem in this regard.

One of Ethereum's problems was framed as a dependence on suspicious, yet established organizations and respective technological infrastructures that acted as intermediaries on the internet and in the global economic system. These actor-networks included internet firms, financial services firms, online market places, and governments. Fraud and cheating were assumed to be ubiquitous in economic systems and on the internet. The *Financial Times* quoted the inventor of the Ethereum platform, Vitalik Buterin, recalling his radical (Swartz, 2017) attitude towards the established economic system: "As a teenager, he shared the rebellious cryptocommunity's common attitude: "the system", ie governments, banks and major corporations, "is basically evil, and we needs [sic] to outright resist it and build a new thing"" (Cornish, 2018). In a blog post, Vitalik Buterin presented the problem as one of large organizations betraying investors; the internet was supposed to create transparency, but at the same time create opportunities to present polished information:

Perhaps one of the main unfortunate byproducts of the modern birth of large centralized organizations is that they allow people to effectively cheat [...]

Most people in modern civilization have benefited quite handsomely, and have also indirectly financed, at least some instance of someone in some third world country dumping toxic waste into a river to build products more cheaply for them; however, we do not even realize that we are indirectly participating in such defection; corporations do the dirty work for us [...]

The internet has often been hailed as a solution to many of these organizational and political problems, and indeed it does do a great job of reducing information asymmetries and offering transparency. However, [...] it can also sometimes make things even worse. Online [...] it is easier to appear virtuous while actually intending to cheat. (Buterin, 2015a)

According to Buterin, economic interactions on the internet still rely on intermediary organizations and platforms. He referenced this point in a blog post with the example of eBay and its role in ecommerce:

Escrow is a very important function in commerce, and especially commerce online; when you buy a product from a small online store or from a merchant on Ebay, you are participating in a transaction where neither side has a substantial reputation, and so when you send the money by default there is no way to be sure that you will actually get anything to show for it. Escrow provides the solution: instead of sending the money to the merchant directly, you first send the money to an escrow agent, and the escrow agent then waits for you to confirm that you received the item. If you confirm, then the escrow agent sends the money along, and if the merchant confirms that they can't send the item then the escrow agent gives you your money back. If there's a dispute, an adjudication process begins, and the escrow agent decides which side has the better case.

The way it's implemented today, however, escrow is handled by centralized entities, and is thrown in together with a large number of other functions. On the online marketplace Ebay, for example, Ebay serves the role of providing a server for the seller to host their product page on, a search and price comparison function for products, and a rating system for buyers and sellers. Ebay also owns Paypal, which actually moves the money from the seller to the buyer and serves as the escrow agent. (Buterin, 2014d)

At team and community meetings,³² a co-inventor and developer of the Ethereum platform explicated that corporate organizations and governments could not be trusted. According to hi, this constituted a problem for internet users, as the technological infrastructure of the internet relied on established information technology companies:

The web – and to a large degree the internet – as it stands, is designed around centralized systems and authorities. When you download a web page, when you use a web app or a web service, the first thing that you do is you type in a company's name and the next thing that happens is that your computer asks an authority what that company's computer is, what the address of that computer is. The next thing that happens is that you go to that company's computer and you ask them to please log you into your account with your data and tell you what's going on with your friends – to take Facebook as an example. That's susceptible to bad things. (Ethereum, 2014a, 14:34)

³² Meetings were recorded and the videos were published on YouTube.

Now, the problem is that trust doesn't really scale. So, when you get to multinationals and governments, they can largely do what they want without that accountability that you would get in a small community. As Julien Assange said, what we actually need is transparency for the powerful but privacy for everybody else. (Ethereum, 2014b, 7:39)

Bitcoin was intended as a solution for the problem of users' dependence on intermediaries in the field of online payment that users did not trust (0). When Ethereum was conceptualized in 2013, Bitcoin was perceived as having technical limitations, but was still seen as a solution for the amplified problem of trust on the internet (Buterin, 2014a). Moreover, Bitcoin's development was hampered by debates in the Bitcoin community about the governance of open source code. Bitcoin also suffered the effects of bad reputation. In an Ethereum blog, a team member retrospectively summarized the technical and organizational problems of Bitcoin during the time when Ethereum was invented:

Although Bitcoin's speed of settlement was a huge improvement over traditional systems, it was clear that more innovation could be had by further experimenting with whatever this "blockchain" thing was. At the time, there was much debate about so-called "blockchain bloat" and concerns that additional applications built on the Bitcoin protocol would cause problems scaling. Already, betting platforms had come under fire for creating lots of low-value transactions. There was a stirring in the bitcoin community that continues to this day.

With all these possibilities, how could a single protocol be made to accommodate all the varying needs? As a first experiment, Bitcoin was already gaining quickly in value. What began as a cypherpunk dream had blossomed into an industry. Changes to the core protocol risked billions in value and there was no clear governance in place for proposing and including changes. (Gerring, 2016)

The Economist captured Bitcoin's unfavorable public reputation with its article on "the trust machine" ("The promise of the blockchain," 2015):

BITCOIN [capitals in original] has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the "dark net". ("The promise of the blockchain," 2015)

In one of my interviews, a software developer remembered Bitcoin's negative image and recalled how the Ethereum platform emerged as a new actor in this context: "You think back when Bitcoin was just Bitcoin blockchain, just one Bitcoin blockchain, just one big blob and they used it to buy guns and drugs, you know, trade illegal on the dark web, is the kind of perception" (Ethereum community member, 2018).

In 2013, Vitalik Buterin – a then 19-year old college drop-out and former member of the Bitcoin community (Cornish, 2018) – initiated the Ethereum platform as a solution to these problems. He was joined by people from the Bitcoin community, other software developers, and information technology enthusiasts, and with them developed and publicized the Ethereum platform (Buterin, 2014a). During the observation period from 2013 to the

beginning of 2018, the Ethereum team grew and changed with individuals leaving and joining the team around Buterin (Tual, 2015c; Wood, 2016). What defined the Ethereum team as an actor in the translation of the Ethereum platform was the shared interest of its members in solving the above mentioned problems through information technology. In a blog post, one team member formulated an “intention [...] to deliver a technology aligned with the community at large [...] – not only for our fellow ethereans but everyone – united by raw passion for positive world change” (Alisie, 2014a). This was expressed in the development and promotion of the platform. In an early blog post, Vitalik Buterin described the team constellation and their aim to technically and socially translate the platform globally:

The Ethereum team has expanded to include such distinguished members as [...] [the] head of the Bitcoin Education Project, [...] [the] Executive Director of the Bitcoin Alliance of Canada and founder of the Bitcoin Decentral coworkingspace in Toronto, and [...] [the] founder and chief editor of Bitcoin Magazine, and dozens of other incredibly talented individuals who are unfortunately too many to mention. Many of them have even come to understand the project so deeply as to be better at explaining Ethereum than myself [...] Aside from development effort, there are dozens of people operating around the world in our marketing and community outreach team, developing the non-technical infrastructure needed to make the Ethereum ecosystem the solid and robust community that it deserves to be. (Buterin, 2014a)

But what is the Ethereum platform? In short, Ethereum is a programmable multi-purpose blockchain system (2.2). But before the platform became a technological infrastructure, it was a bundle of concepts described by members of the team in the *White Paper* (Buterin, 2014i) and the “yellow paper”³³ (Wood, 2014). The technical implementation evolved from proofs-of-concept and test networks into the more broadly used Ethereum mainnet (Homestead Documentation Initiative, n.d.c). Irrespective of its material manifestation, Ethereum was presented as a solution to a problem of trust and as such functioned as an obligatory passage point (Callon, 1986b). As the Ethereum platform was supposed to solve for the problem of not trusting intermediaries and organizations beyond the financial industry, the *White Paper* suggested that it be used for financial and non-financial applications:

In general, there are three types of applications on top of Ethereum. The first category is financial applications, providing users with more powerful ways of managing and entering into contracts using their money. This includes sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and ultimately even some classes of full-scale employment contracts. The second category is semi-financial applications, where money is involved but there is also a heavy non-monetary side to what is being done; a perfect example is self-enforcing bounties for solutions to computational problems. Finally, there are applications such as online voting and decentralized governance that are not financial at all. (Buterin, 2014i)

³³ The internet publication *Ethereum. A Secure Decentralized Generalised Transaction Ledger* is commonly referred to as the “yellow paper”.

Its ability to potentially solve for problems beyond the financial industry was attributed to its design as “the ultimate abstract foundational layer” (Buterin, 2014i) for blockchain applications. In a blog post, Vitalik Buterin explained how he expected the Ethereum platform to be useful in gaming, for tracing goods, and for managing the Internet of Things³⁴:

One of Ethereum’s goals from the start, and arguably its entire *raison d’être*, is the high degree of abstraction that the platform offers. Rather than limiting users to a specific set of transaction types and applications, the platform allows anyone to create any kind of blockchain application by writing a script and uploading it to the Ethereum blockchain. This gives an Ethereum a degree of future-proof-ness and neutrality much greater than that of other blockchain protocols: even if society decides that blockchains aren’t really all that useful for finance at all, and are only really interesting for supply chain tracking, self-owning cars and self-refilling dishwashers and playing chess for money in a trust-free form, Ethereum will still be useful. (Buterin, 2015e)

The Ethereum platform was meant to provide the technological base for writing and executing all kinds of programs. These programs are called smart contracts (2.2) and encode interaction logics that can connect multiple Ethereum user accounts.³⁵ In a blog post on blockchain-based actors Vitalik Buterin explained that

a smart contract is a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated. (Buterin, 2014g)

In terms of the above mentioned application fields, smart contracts were envisioned for managing self-owned car rentals, service agreements and dish detergent purchases for dishwashers, or automatic payouts for chess games. Examples of smart contract ideas from Vitalik Buterin illustrated smart contracts’ additional purposes. A smart employment contract between two accounts, for example, could automatically release remuneration for work according to the rejection or acceptance by the owner of a second account. Similarly, insurance smart contracts were expected to automatically release payments in case of adverse events (Buterin, 2014c). Smart contracts were even suggested for organizing value transfers or sharing hard drive space between users, and thus aimed to supersede centrally operated and established payment providers like PayPal, or software companies like Dropbox (Buterin, 2014d).

According to the blog post of another Ethereum team member, one could also create digital tokens with a smart contract, i.e. “any fungible tradable good: coins, loyalty points, gold certificates, IOUs [notes of debt], in game items, etc.” (van de Sande, 2015). These could be

³⁴ For an explanation of Internet of Things see chapter 2.

³⁵ With Ethereum user accounts, I am referring to Externally Owned Accounts (EOAs). Smart contracts could also trigger other contract accounts (Homestead Documentation Initiative, n.d.a).

transferred between accounts and other smart contracts on the Ethereum platform. By programming a wide range of assets or goods on a blockchain, the general idea of tokens expanded on the idea of Bitcoin as a digital currency.

The Ethereum platform's features for programming smart contracts also laid the foundation for other technical actors, decentralized applications (DApps) and Decentralized Autonomous Organizations (DAOs). DApps are user applications that incorporate smart contracts on the Ethereum platform and connect them to regular front ends for smart phones or web explorers (Diedrich, 2016, p. 174; van de Sande, 2016). Such DApps were supposed to make smart contracts accessible for private and enterprise users without programming skills. A Decentralized Autonomous Organization³⁶ was imagined as "an entity that lives on the internet and exists autonomously" (Buterin, 2014g); this entity could own property and enact economic exchanges with technical and human actors. Technically, a DAO should consist of multiple smart contracts which determine its decision and action logics (Diedrich, 2016, p. 181). In a blog post, a team member expressed their wish to make the collective dream of the DAO a reality through the Ethereum platform:

Extending the idea to beyond a simple web project, Ethereum hopes to demonstrate how fully decentralized autonomous organizations (DAOs) can live wholly within cyberspace, negating not only the need for centralized servers, but also trusted third-parties, realizing the dreams of early internet pioneers that envisioned an independent new home of the mind. (Gerring, 2014)

As an infrastructural base layer, the Ethereum platform processed and stored all interactions between Ethereum user accounts as well as smart contracts executions in the form of transactions³⁷ (Diedrich, 2016, pp. 178–179; Homestead Documentation Initiative, n.d.e). These activities were performed differently than in financial institutions and information technology firms, which had mostly centralized servers and proprietary algorithms. The idea of the Ethereum platform as blockchain technology implied that the platform relied on a multitude of network nodes that process the same algorithms in parallel and maintained a shared database with all transactions (Homestead Documentation Initiative, n.d.b). Network nodes were software clients that people could install on computational devices. The algorithm that validated and stored all transactions ran on these network nodes. In the case of the Ethereum platform, the proof-of-work³⁸ consensus algorithm was rather similar to the

³⁶ Decentralized Autonomous Organization was a new rendition of the Decentralized Autonomous Corporation already discussed in the *Bitcoin Magazine* in 2013 (Buterin, 2013a; 2013b, 2013c).

³⁷ The term transaction refers to state transition, which is a value or information transfer between contracts and or accounts. For further details, see Homestead Documentation Initiative (n.d.b) and Wood (2014).

³⁸ Despite disadvantages to proof-of-work as perceived by the Ethereum team (Buterin, 2016b), the Ethereum platform continued to rely on the algorithm during my period of observation. However, since 2014, the platform's developers have nurtured expectations that these consensus mechanisms would be replaced by proof-

algorithm used by Bitcoin. This algorithm validated and verified transactions among a network of nodes, and was not centrally orchestrated. The Ethereum platform³⁹ was permissionless, meaning it was open for anyone to participate in its consensus mechanism (Peters & Panayi, 2016, 244–245) (2.2). The miners – network nodes that participated in the validation – were incentivized to run a network node and participate in the algorithm through payouts in the platform’s dedicated cryptocurrency, Ether (Homestead Documentation Initiative, n.d.f). Similar to Bitcoin, Ether was produced through mining and was also tradeable through cryptocurrency exchanges (2).

Another integral aspect of the Ethereum platform’s identity is its blockchain database, which records all validated transactions in data blocks and stored them on multiple network nodes⁴⁰ (Homestead Documentation Initiative, n.d.h). This includes all transactions that have been processed by the public Ethereum platform⁴¹ since its launch in 2015 (Homestead Documentation Initiative, n.d.d). The Ethereum platform was designed in a way that all network nodes are able to make use of the platform for proposing new transactions. Furthermore, anyone with a computational device capable of storing the entire database is allowed to run a full node. This classifies the Ethereum platform as a public blockchain (Peters & Panayi, 2016, p. 244).⁴²

Another actor was required in order to translate the platform and bring to life the ecosystem of smart contracts, DApps, DAOs, and new tokens. The Ethereum community consisted of people who wished to explore new platforms and discover new economic and technological opportunities in the blockchain and cryptocurrency space. One interviewee from the Ethereum team who used to design the Ethereum website to address the Ethereum community described the Ethereum community of the early years as “people who are explorers [...] People who are curious, people who are developers, people who want to develop things in Ethereum” (Ethereum team member 1, 2018). For the Ethereum community,

of-stake-algorithms in the future (Zamfir, 2016). As discussed in my interview with a blockchain reporter (2018), the latter would change the role of miners and of Ether.

³⁹ This refers to the Ethereum main network network (also called mainnet). In addition to the permissionless and public blockchain of the Ethereum mainnet, the Ethereum software code could also be used within private and permissioned networks (6.3). This section refers to characteristics of the Ethereum mainnet.

⁴⁰ Initially, all network nodes stored the entire database. As it grew, some nodes stored historic data and the current state while others only verified the current state (Ethereum Foundation, 2016b).

⁴¹ This section refers to characteristics of the Ethereum mainnet.

⁴² Initially, the term public referred not only to reading and usage rights but also the permission to participate in the consensus mechanism of a blockchain. Peters and Panayi (2016) draw upon a blog post by Buterin (2015f), who uses the initial meaning of public blockchain and narrow the term down to reading and transaction rights of network nodes. I stick to their definition which has been further systemized, for example by Beck et al. (2018).

the Ethereum platform was a creative and open playground. In a blog post, one of the team members illustrated this metaphorically:

I like to look at the ethereum project as a blank canvas, where anyone can create digital masterpieces. The technology behind it serving as a catalyst, enabling people to unfold their innate playful creativity. If the network and blockchain were to be the canvas, then the paints and colors would be the lines of code running transparently and censorlessly on top. Everyone is invited to cocreate. (Alisie, 2014a)

In an interview, one Ethereum community member who started his blockchain journey with Bitcoin stated that he saw Ethereum distinguishing itself from Bitcoin's bad reputation:

Then I think, you know, they [Ethereum and Ripple⁴³] kind of carved their small area, used the blockchain ecosystem to kind of grow something new, and then they over time they've sort of separated themselves [from Bitcoin] and created this kind of cleaner, cleaner area. (Ethereum community member, 2018)

The Ethereum platform was their obligatory passage point insofar as it provided a variety of possibilities for contributing to Ethereum's promise of a new internet and new economy, and for pursuing community members' own interests in the blockchain space. People could support the Ethereum team by sharing ideas, developing and coding for the core algorithms and adjacent pieces of software, and testing and exploring the platform (Alisie, 2014a; Buterin, 2015g; Hallam, 2014). It was a chance to gain expertise and contribute to an emerging technology – in some cases without financial rewards, in others with financial remuneration (Alisie, 2014b; Steiner, 2014; Wendell, 2015). Once the Ethereum mainnet went live in 2015, members of the community started mining for the Ethereum platform (Homestead Documentation Initiative, n.d.c). Software developers and entrepreneurs could also experiment with and realize their ideas for internet applications, new business models, governance models, and raising funds through programming smart contracts, tokens, DApps, and DAOs (Diedrich, 2016, pp. 58–61; State of the DApps, n.d.; Tual, 2014). Such activities were also pursued by former or even active team members (Consensus Systems, n.d.; DuPont, 2018; Parity Technologies, n.d.) so that the transitions between team and community were sometimes fluid.

Apart from those people building the Ethereum platform and exploring smart contracts, new applications, and business models, other actors – especially those who were interested in cryptocurrencies as investments – were attracted by the Ethereum platform's ability to issue tokens with cryptocurrency. An interviewee with a programming background who had bought Ether and other cryptocurrencies as a youth himself recalled that early investors were mostly

⁴³ Ripple is an open source protocol for blockchain-based payment.

people with a programming background: “If you look at the cryptocurrency community, the early movers, a lot of us were programmers” (ICO advisor 1, 2018). He also recalled how he speculated for rising prices: “I think as any young person who might have a little bit of money [...], throw it to make more money from [cryptocurrencies]” (ICO advisor 1, 2018). An Ethereum team member with a computer science background who had bought Ether described a similar experience:

I had Bitcoins left over from when I used to mine and bought some Bitcoin, when it was 10 dollar a Bitcoin, so the price had risen to like 300 or 600 dollars or something at the time [2014] and so I was able to buy 2000 Ether with one Bitcoin. (Ethereum team member 2, 2018)⁴⁴

Thus cryptocurrency investors, of whom many already had experience with Bitcoin (2.1), perceived Ether and additional tokens that were issued later on the Ethereum platform as new investment opportunities; a new OPP on their cryptocurrency investment journeys. Their hope was to benefit from increases in cryptocurrency value. A blockchain manager, who consulted business clients on blockchain, observed that the price of Ether was important to these investors: “[Ethereum’s] scene is infiltrated [...] by these crypto freaks. There are many speculators, so this coin, the Ether, is in the foreground. This price means a great deal to the community” (Blockchain manager at information technology and consulting company, 2017).

Apart from buying and selling Ether, the programmability of tokens with smart contracts on the Ethereum platform was supposed to enable investments in a decentralized way. On the documentation website *Ethereum Homestead documentation*, which was compiled by Ethereum community members, this was described as a way to avoid trust in fundraisers:

Would you enter in a contract with someone you’ve never met? Would you agree to lend money to some farmer in Ethiopia? Would you become an investor in a minority-run newspaper in a war zone? Would you go to the hassle of writing up a legal binding contract for a \$5 dollar purchase over the internet?

The answer is no for most of these questions, the reason being that a contract requires a large infrastructure: sometimes you need a working trust relationship between the two parties, sometimes you rely on a working legal system, police force and lawyer costs.

In Ethereum you don’t need any of that: if all the requisites to the contract can be put in the blockchain then they will, in a trustless environment for almost no cost. (Homestead Documentation Initiative, n.d.g)

Besides investors, there was another actor with commercial interest in Ethereum, namely the business community. A blockchain manager, who used to work with the platform and the business community described how, apart from investors and speculators, the platform was

⁴⁴ At the time of interviewing, the interviewee was an Ethereum team member. The situation he recalls in this quote refers to a point in time before he joined the Ethereum community, and later the team.

also an obligatory passage point for established firms: “It’s such a mix [...] from crypto speculators to firms like Microsoft, which [...] support the technology [...] and see in it a future for the industry, especially IT industry” (Blockchain manager at information technology and consulting company, 2017). Thus for information technology firms like Microsoft (Ethereum, 2015a) or IBM (Ethereum, 2015b), and consulting firms like Deloitte (Ethereum, 2016b), blockchain technology was a new business opportunity (Blockchain manager at information technology and consulting company, 2017, p. 3). Moreover, the existence of Bitcoin had put banks under pressure (Popper, 2016). As panelists at an Ethereum conference⁴⁵ described, the Ethereum platform was of interest to those banks seeking to pursue their own activities through blockchain technology (Ethereum, 2016c). An interviewee who had interacted with the business community described that whoever wanted to take action in 2014 or 2015 were forced to use Ethereum, as it was the first publicly available and programmable blockchain technology. Another interviewee further described how large parts of the business community continued to observe the technology with extra attention later on, as there was a blockchain hype among the business community. A blockchain manager recalled the early years of Ethereum:

During approximately the first one and a half years of [Ethereum’s] operation, there was no alternative [...] if you wanted to try out smart contracts, this super innovative technology, you had no choice. You could only work with Ethereum. And then the first companies came that also found that interesting, also not only technology companies but also banks [...] All those who dealt with the topic two, two and a half years ago [in 2015 and before] were not getting around Ethereum. (Blockchain manager at information technology and consulting company, 2017)

An Ethereum community member who had worked with the business community on blockchain projects interpreted their motive in 2018 – he stated: “It’s potentially very disruptive” (Ethereum community member, 2018) and concluded from his observations of established companies that “they just wanna keep an eye on what’s going on [...] because there is so much hype now” (Ethereum community member, 2018).

The hype among the business community was fueled by IT evangelists who had a great interest in promoting blockchain technology as the latest innovation. The Ethereum platform served as a reference for them to generalize the benefits of blockchain, while the Ethereum team and community members were a direct source of information. In their book, *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*, Tapscott and Tapscott (2016a) recapped interactions with the Ethereum platform, the team

⁴⁵ Sessions were recorded and the videos were published on YouTube.

and community, and promoted the platform as a technological revolution with far-reaching implications:

July 30, 2015, was a big day for a global group of coders, investors, entrepreneurs, and corporate strategists who think that Ethereum is the next big thing—not just for business, but possibly for civilization. Ethereum, the blockchain platform eighteen months in the making, went live.

We witnessed the launch firsthand in the Brooklyn office of Consensus Systems (ConsenSys), one of the first Ethereum software development companies. (Tapscott & Tapscott, 2016a, p. 87)

In a *Harvard Business Review* article, these authors urged enterprises to get involved with blockchain technology:

In the mid-1990s, smart managers worked hard to understand the internet and how it would affect their businesses. Today, blockchain technology is ushering in the second generation of the Internet, and if companies don't want to get left behind, they'll need to dodge the Innovator's dilemma and disrupt from within. (Tapscott & Tapscott, 2016b)

Similarly, William Mougayar, who supported Vitalik Buterin and the Ethereum platform early on, sold the potential of blockchain to enterprises as a technological solution, process re-engineering opportunity, new governance model, and business opportunity:

Blockchain is not a one-trick pony. It is a multi-headed beast that takes many forms.

If you see it as a technology, then you will implement it as a technology. If you see it as a business change enabler, then you will think about business processes. If you discern the legal implications, you will be emboldened by its new governance characteristics. And if you see it as a blank sheet of paper for designing new possibilities that either didn't exist before, or that challenge existing legacies, then you will want to get very creative at dreaming up these new opportunities. (Mougayar, 2016, p. 38)

Following Callon (1986), constructing problems stimulates translation. It was in the interest of the Ethereum team, the community, investors, the business community and IT evangelists to acknowledge Ethereum – with its smart contracts, Dapps, DAOs and Ether – as an obligatory passage point for multiple problems associated with trust. In the following, I examine these problems from a theoretically informed perspective on trust.

5.1.2 Trust

The problematization of Ethereum drew upon problems associated with two types of actors. On the one hand, problematizations referred to institutionalized actors, for example governments, financial institutions, or technology corporations as trustees. On the other hand, a relatively new socio-technical network, Bitcoin, was implicitly described as a trustee as well. Both aspects of the problematization implied issues with regard to trusting the respective trustees. With regard to institutionalized actors, points of critique included a lack of accountability and transparency, as well as centralized power over information storage and

processing; these explanations were used by the Ethereum team when communicating with the Ethereum community that institutionalized actors should not be trusted. These arguments connect to the observed phenomenon of decreasing public trust in governments (Uslaner, 2014), the financial system (Uslaner, 2014) and ‘institutions of business’ (Harris, Keevil, & Wicks, 2013), especially since the 2008 global financial crisis (Gillespie & Hurley, 2013).

Also Bachmann et al. (2015) hint at a loss of public trust in corporations, governmental, and public institutions, especially in Western societies. Such a loss of trust has not only been fueled by the financial crisis, but also by “a plethora of prominent organizational failures and trust betrayals involving businesses, regulators and governments” (p. 1124). From a system trust perspective, implied in the trust category of routine (3.1.2), the Ethereum team, community, and investors decreased their “confidence in the institution's reliable functioning” (Möllering, 2006a, p. 74). Viewing the problem as one of trusting institutionalized actors, problematization in this case represented a trust crisis similar to ones found in other translation studies (3.2.2).

The second problem, which refers to Bitcoin, was of a different, reflexivity-based nature (Möllering, 2006a). As a solution for the first problem, it had been translated from a dream of cypherpunks into a socio-technical network where bitcoins, information, and physical goods could be circulated. However, from experience, the Ethereum team had problems believing in Bitcoin’s future technical viability as well as the Bitcoin community’s ability to act. Their knowledge about the platform and interactions with the Bitcoin community prevented them from taking leaps of faith (Möllering, 2006a) into the future of Bitcoin. Moreover, the socio-technical network of Bitcoin had developed a bad reputation due to Bitcoin’s strong value fluctuation and stories about Bitcoin’s use for illegal and immoral actions, such as trading drugs or guns. Drawing on Zucker’s (1986) finding that good reputation builds process-based trust, something also implied in Möllering’s (2006a) notion of reflexivity, Bitcoin’s bad reputation also constitutes a trust crisis. The Ethereum community and the business community, as witnesses of Bitcoin’s poor reputation, were also confronted of Bitcoin’s trust crisis problem.

In summary, I find that two trust crises were framed as problems in the translation of Ethereum. On the one hand, there was the routine trust crisis directed toward institutionalized organizations such as governments, information technology corporations, and financial services firms. The Ethereum team, community, and its investors could no longer trust such institutions. On the other hand, Bitcoin, the alternative developed since 2008, also faced a lack of reflexivity-based trust from the Ethereum team, the community, and other enterprises.

I understand these trust crises as losses of confidence, which opened up the trustees' awareness and curiosity for alternatives. According to Callon (1986b), actors' construction of such problems is an integral part of translation. The Ethereum platform was introduced as a solution to these problems, the obligatory passage point, especially for the trustors. Those actors who had little trust in institutionalized technology companies, financial services firms or governments were offered an alternative. This alternative came in the form of a new actors – the Ethereum platform with its smart contracts, DApps, DAOs, and its cryptocurrencies, including Ether. Those actors who had little trust in Bitcoin as an infrastructure or as a cryptocurrency were offered an alternative actor, which had some similarities with Bitcoin, but with a cleaner image. While in Ethereum's problematization trust manifested as trust crises, *interessement* presents an additional understanding of trust. In the following, I describe how trust was introduced as an *interessement* device in Ethereum's translation.

5.2 Interessement: Trusted trustless technology

5.2.1 Translation

Trust can be interpreted as an *interessement* device in the translation of the Ethereum platform. *Interessement* refers to connecting the actors with the help of *interessement* devices. These devices serve as interfaces and as boundaries between actors that allow them to established their own identities and mutual relations (Callon, 1986b; Jeacle, 2017). In this section, I describe three narratives in which the *interessement* device trust was used during the translation of Ethereum. The first was an idealization of the Ethereum platform as a trustless system, one which like Bitcoin (2.3), was based on algorithms and provided incentives for avoiding trust in single entities. The second was the narrative that the Ethereum platform, and blockchains in general, would facilitate a trusting relation between platform users based on guaranteed execution and its auditability. The third was a positioning of the Ethereum platform as a trustee to other actors. These three narratives were often rhetorically combined, as in the following blog post dedicated to the matter of trust, where Vitalik Buterin depicted the role of trust as an *interessement* device for the Ethereum community. In this post, blockchain technology was described as something that would make trust dispensable; at the same time, blockchain systems were framed as devices which could be trusted for maintaining accurate data, which in turn would facilitate trustful economic relations:

If you were to ask the average cryptocurrency or blockchain enthusiast what the key single fundamental advantage of the technology is, there is a high chance that they will give you one particular predictable answer: it does not require trust. Unlike traditional (financial or other) systems, where you need to trust a particular entity to maintain the database of who holds what

quantity of funds, who owns a particular internet-of-things-enabled device, or what the status is of a particular financial contract, blockchains allow you to create systems where you can keep track of the answers to those questions without any need to trust anyone at all (at least in theory). Rather than being subject to the whims of any one arbitrary party, someone using a blockchain technology can take comfort in the knowledge that the status of their identity, funds or device ownership is safely and securely maintained in an ultra-secure, trustless distributed ledger Backed By Math™. (Buterin, 2015c)

I will depict the three narratives more in detail below. In a blog post, Buterin (2015c) observed that “many people are interested in blockchains specifically because of their property of “trustlessness””. The notion of a trustless system was not a new scheme around Ethereum, but was inherited from the Bitcoin network (2.3). By the time the Ethereum platform was being translated, the term had spread to those using or investigating blockchains, especially those with a computer science background. For the Ethereum community, trustlessness meant making trust, especially in single entities, dispensable. The promise of trustless systems appeared conceivable, as the Ethereum platform was constituted by network nodes in a permissionless network, which autonomously determined a synchronous system state⁴⁶ agreed upon among all network nodes, and validated transactions through proof-of-work consensus algorithms (Diedrich, 2016, pp. 144–145). The validation of new transactions was organized in a way that nodes proposed new transactions to the network. In order to do this, the proof-of-work algorithm made them compile various transactions into a block, check whether they were compliant with platform-internal rules, attach the solution of a cryptographic puzzle⁴⁷ to the block, and link the block to the heaviest blockchain in the Ethereum network⁴⁸ (Diedrich, 2016, pp. 146–149). Then, once a proposer suggested a block, a mutual control mechanism kicked in: Other Ethereum nodes verified the proposed transaction block and voted on whether they agreed on the state (Diedrich, 2016, pp. 146–147). With Ethereum’s proof-of-work consensus algorithm, network nodes were in continuous competition for validating new transactions according to pre-determined rules, and to mutually verify each other’s validated transactions (Diedrich, 2016, pp. 147–148). The Ethereum team and IT evangelists claimed that transaction validation through multiple network nodes based on the proof-of-work consensus algorithm (recognized as a secure computing algorithm) created certainty for all entities relying on and using the Ethereum

⁴⁶ This status was called “world state” (Wood, 2014, p. 3) or “the truth” (Diedrich, 2016, p. 126). Diedrich (2016) explains that “the convention is that this heaviest chain is always the chain that reflects the truth of the world state” (p. 146).

⁴⁷ More specifically a hash function.

⁴⁸ This validation within the public Ethereum network based on proof-of-work is also called mining.

platform. Team member Gavin Wood outlined the technical architecture of the Ethereum platform in a publication where he referred to proof-of-work as a secure algorithmic rule: “Mining is the process of dedicating effort (working) to bolster one series of transactions (a block) over any other potential competitor block. It is achieved thanks to a cryptographically secure proof. This scheme is known as a proof-of-work” (Wood, 2014, p. 2). The IT evangelist William Mougayar stated that this algorithm would replace trust:

Trust can be coded up, and it can be computed to be true or false by way of mathematically-backed certainty, that is enforced by powerful encryption to cement it. In essence, trust is replaced by cryptographic proofs, and trust is maintained by a network of trusted computers (honest nodes) that ensure its security (Mougayar, 2016, p. 18).

A similar argumentation came up during my interview with an Ethereum team member at the beginning of 2018:

The fact that the computation and the transfer of the Ether token are backed by cryptography is promising, because generally you have to trust a third party in order to do a transaction, whether that be a central bank or like, if you are doing an escrow service, you have to trust a bank or mortgage company or something like that. But on the blockchain you have these cryptographic hashes or cryptographic problems that are being solved by people as a collective and they are going through and confirming transactions in a public way so that everyone can see if anyone is cheating; so because this data base, this ledger of programs and transactions is being replicated and everyone can always see what’s happening, that provides transparency. And once you provide transparency you don’t have to know everything about the person you are transacting with because you know that the way that you run your transaction is gonna be run the same everywhere and you can verify it very easily. So trust isn’t necessarily built but this quality of trustlessness, the requirement for trust goes away because you have this system that you can trust instead. (Ethereum team member 2, 2018)

A particular rule of the validation and verification procedure was the requirement for every transaction to be signed with a private account key of the transaction issuer. This digital signature was conceived as an additional mechanism for enhancing certainty about the correctness of transactions processed on the platform, and thus reducing the necessity for users to trust. In a non-technical guide on Ethereum written by IBM’s former contact person to the Ethereum team and community, the effect of the signature on trust was described as follows:

Code is deployed to the blockchain in Ethereum as payload of a transaction and thus, is also signed.

This gives blockchain data the unique feature that all its permutations are signed off. All input and all code is signed, and so, by extension, the result.

The important point is how blockchains are based on this primitive of authorization – your signature [private key] – as the central building block of everything a blockchain consists of. As noted before:

Because everything is signed, there is no need to trust. (Diedrich, 2016, p. 117)

Another aspect of the Ethereum platform's idealization as something "trustless" was the incentive scheme for miners that participated in transaction validations using the proof-of-work consensus algorithm. These network nodes were governed by an incentive structure which rewarded them with Ether for participating in the validation of new transactions; incentives also ensured that the ability to validate spread across network nodes so that no single entity would gain power over the network (Diedrich, 2016, p. 147). The idealization of the Ethereum platform as a trustless system drew upon the assumption that the platform could incentivize mining network nodes to not corrupt each other or the platform itself. In his blog post on trust, Vitalik Buterin phrased this accordingly:

When a system is claiming to be "trustless", what it is actually trying to do is expand the possible set of motivations that individuals are allowed to have while still maintaining a particular low probability of failure. (Buterin, 2015c).

Various game theoretical thought experiments documented on the Ethereum blog express the Ethereum team's aim to design and improve a permissionless Ethereum platform. Incentives were designed to push network nodes to execute code and validate transactions for the platform as intended. A summary of a team and community workshop discussion illustrates that the participants' thoughts about a technical characteristic – in this case an alternative consensus mechanism⁴⁹ for the Ethereum platform – were led by considerations about incentives for network nodes and disincentives for potential hacker attacks against the platform. This summary was provided in a post on the Ethereum blog:

A major topic of discussion was coming up with a rigorous and generalizable strategy for determining optimal incentives in consensus protocols [...] can we come up with a generalized way to correctly assign the right rewards and penalties to all participants, using only verifiable evidence that could be put into a blockchain as input, and in a way that would have optimal game-theoretic properties? [...]

A key goal of our approach [...] is ensuring as much incentive-compatibility as possible even under a model with majority collusions: even if an attacker controls 90% of the network, is there a way to make sure that, if the attacker deviates from the protocol in any harmful way, the attacker loses money? (Buterin, 2016e)

These mechanisms of trustlessness were unified in promising the Ethereum community and the business community that the Ethereum platforms' programs would run as written. According to the *Ethereum Homestead documentation*, "the popular term "smart contracts"

⁴⁹ Since 2014, there have been discussions and preparations of the Ethereum team to replace the proof-of-work consensus algorithm in the Ethereum platform with a proof-of-stake consensus algorithm (Buterin, 2014i). By early 2018, there were tests under way, but the public Ethereum platform was still relying on its proof-of-work consensus algorithm (Dameron, 2018, pp. 12–13; Wood, 2014).

refers to [...] programs that execute” (Homestead Documentation Initiative, n.d.h). It provided certainty to all actors that – once a smart contract was submitted to the Ethereum platform – it would run as programmed and enter the system as a transaction, except in cases when validating network nodes agreed to not validate it. In his book *Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations*, a former IBM contact person described this guarantee of execution:

Smart contracts will execute.* [asterisk in original]

It’s about being able to program what should happen, in a way that can’t be changed nor stopped. Except – and that’s the asterisk – if everyone who runs a node agrees to stop the chain. Thousands of people in the case of Ethereum or Bitcoin [...]

This *guarantee of execution* [italics in original] is new. (Diedrich, 2016, pp. 22–23)

Referring back to the gurantee of execution, Diedrich (2016) explains: “How that should work? Basically making sure that 1. every transaction going into the system is signed and 2. everyone in the network executes it to completion” (p. 24).

Trustlessness behaved as an interessement device to the Ethereum community and the business community. According to this narrative, all actors could become connected in trustless relations through the Ethereum platform and its smart contracts. Algorithmic proof via cryptography and mutual verification of nodes, incentive schemes, digital signatures, and guaranteed executions should obviate the need for trust among Ethereum team, the Ethereum community, and business community. Moreover, the positive connotation of the narrative assumed that the Ethereum community and the business community were interested in the ideal of trustlessness in the same way as the Ethereum team. In a talk at the Ethereum developer conference DEVCON1, recorded on YouTube, a consultancy firm software engineer nevertheless warned the audience that trustlessness was not a suitable interessement device for decision-makers in the business community:

A good example that we like to point to is, is the term “trustless”. In this context and in this room the word “trustless” is an extremely valuable component of this technology, it’s seen as a feature of this technology and it’s obviously [...] extremely important. Obviously creating interactions and transaction where you do not need to trust the other side of the transaction. But you go to an ignorant bystander, say the CEO of a bank that you’re trying to sell your solution to and you tell him that your technology is trustless and he’ll tell you that he doesn’t see the value in creating something that has no trust in it. You know it’ll be perceived differently [...] so just keep that in mind as you go out there. (Ethereum, 2016b, 16:49)

This warning put in words a dawning dissent between radical and incorporative blockchain dreams (Swartz, 2017). The ideal of trustlessness was constitutive to the radical blockchain dream and the business community was not likely to agree.

With similar arguments, a second narrative on trust positioned the Ethereum platform as an enabler of economic relations between entities which had little trust in each other. This again would be anyone using and operating the platform, i.e. the Ethereum community, investors and the business community. Relations among those actors were often described as trust. With the words of an IT evangelist “they [blockchain proponents] believe that trust can be and should be part of peer-to-peer relationships, facilitated by technology that can enforce it” (Mougayar, 2016, p. 18). In his guide on Ethereum, IBM’s former contact person phrased the role of the Ethereum platform in creating trust between users and qualified this statement with a hint that the platform was not yet mobilized:

It’s [Ethereum platform] disruptive powers don’t come from how it is such a crypto currency. It’s about how it can create trust and allow for global interaction based on it.

It’s full potential is not realized yet, simply because there is not much interaction at this point in time between contracts on the mainnet [public Ethereum platform]. (Diedrich, 2016, p. 51)

In an interview, a blockchain manager from a consulting firm linked Ethereum’s proof-of-work consensus mechanism to its task to build trust: “Consensus mechanism is what it is because it needs to build trust in a totally trustless environment” (Blockchain manager at consulting company, 2018b). The platform’s guarantee to execute agreements encoded in smart contracts was of relevance once again. Smart contracts were supposedly able to relate multiple Ethereum accounts and their respective key holders in an encoded agreement, and to provide all parties with certainty about contract execution. This was explicated by a member of the Ethereum team in a technical paper:

One key goal is to facilitate transactions between consenting individuals who would otherwise have no means to trust one another. This may be due to geographical separation, interfacing difficulty, or perhaps the incompatibility, incompetence, unwillingness, expense, uncertainty, inconvenience or corruption of existing legal systems. By specifying a state-change system [Ethereum platform] through a rich and unambiguous language, and furthermore architecting a system such that we can reasonably expect that an agreement [smart contract] will be thus enforced autonomously, we can provide a means to this end. (Wood, 2014, p. 1)

Moreover, once deployed on the Ethereum platform, the stored data was suggested to be reliable and auditable. This was especially relevant to the business community targeted by the following IT evangelist: “The Ethereum paradigm revolves around being a network for powering decentralized applications in need of a deterministic, auditable and predictable compute platform” (Mougayar, 2015).

Once a smart contract was executed on the Ethereum platform, the transaction between accounts was documented and could not be modified. With regard to an exemplary Ethereum

smart contract, the IBM contact person explicated which characteristics of the Ethereum platform would make it auditable:

It's [Ethereum smart contract] *really* [italics in original] going out to the *world!* [italics in original] It doesn't go to your screen but instead executes on thousands of computers all over the globe.

Writes to a blockchain are global and permanent.

Plus, its output *and* [italics in original] the program itself cannot be altered after the fact – they are '*immutable*' [italics in original] and permanently stored in the blockchain, with a timestamp. To get the program run, you also have to sign it first. The same as with any data and parameters you send to the blockchain.

Taken together –

immutability

permanence

timestamp

signature and

global availability

have the effect that:

Data and programs on the blockchain are auditable. (Diedrich, 2016, pp. 18–19)

The combination of data being stored on a multitude of network nodes in the hands of many, and verification through a consensus mechanism made the deployed transaction data supposedly permanent and immutable. The digital signature made it possible to trace actions back to a specific account, and the timestamp of the system added another data point to the transactions, which facilitated the reconciliation of historic interactions. This auditability was not limited to a few authorized entities. Rather, smart contract scripts and resulting transactions on the Ethereum mainnet were made publicly available to all network nodes. This made the interactions transparent. A blockchain manager expressed this transparency as complementary to the immutability and permanence of data points:

Ethereum Blockchain, it is just [like Bitcoin], operated by miners and a public blockchain service. All transactions are transparent, all smart contracts are auditable [...] We don't just speak of open source but of open execution because one can really verify and audit the execution of applications. One can tell exactly: "At this point value has been sent from A to B here and this value has caused the following actions and this has led to this and that event and this is how it was meant to be because this smart contract here was deployed on a certain day and it is immutable". All these things are records in a vast ledger. (Blockchain manager at information technology and consulting company, 2017)

In addition, the transparency of agreements and their execution through the public blockchain could signal enterprises' trustworthiness toward their stakeholders. IT evangelists

deduced that enterprises could increase stakeholder's trust by making information transparent through blockchains:

Trust in business is the expectation that the other party will behave according to the four principles of integrity: honesty, consideration, accountability, and transparency [...]

Transparency [bold in original] means operating out in the open, in the light of day. "What are they hiding?" is a sign of poor transparency that leads to distrust. Of course, companies have legitimate rights to trade secrets and other kinds of proprietary information. But when it comes to pertinent information for customers, shareholders, employees, and other stakeholders, active openness is central to earning trust. Rather than dressing for success, corporations can undress for success. (Tapscott & Tapscott, 2016a, p. 10)

Vitalik Buterin related the effects of transparency on trust in private organizations to DAOs. In a blog post, where he took up a question from the Ethereum community, he argued that DAOs would facilitate public trust in those organizations which had transparent governance and operations encoded in DAOs. He asked: "What are DAOs good for? What fundamental advantage would an organization have from its management and operations being tied down to hard code on a public blockchain [...]?" (Buterin, 2015a). Then he explained:

Decentralized autonomous organizations, as a concept, are unique in that their governance algorithms are not just leaky, but actually completely public. That is, while with even transparent centralized organizations outsiders can get a rough idea of what the organization's temperament is, with a DAO outsiders can actually *see the organization's entire source code* [italics in original] [...] not only is it the case that the organization will make it obvious to everyone if they start to cheat, but rather it's not *even possible* [italics in original] for the organization's "mind" to cheat. (Buterin, 2015a)

So, he concluded "the reason why organizations make themselves decentralized/leaky is so that others will trust them more, and so organizations that fail to do this will be excluded from the economic benefits of this "circle of trust"" (Buterin, 2015a).

Lastly, the Ethereum platform was said to provide a base for digital reputation, which could build trust between actors. An IT evangelist formulated public blockchains' general ability to register digital identities of people and attribute them with reputation which could build transactional trust: "The blockchain was designed for a parallel element of transactional trust, where the human is also part of it, but behind the scenes, and that human is represented on the blockchain via their identity and reputation status." (Mougayar, 2016, p. 41). While in blog posts Buterin cheered for Ethereum's ability to create blockchain-based reputation systems (Buterin, 2014i, 2015b), an Ethereum co-founder and community member suggested specific applications and contexts where Ethereum could build trust and create users' reputation. In their book *Blockchain revolution: How the technology behind bitcoin is*

changing money, business, and the world, IT evangelists quoted this co-founder on the trust creating effects of reputation from their interviews. Based on this, they illustrate how Ethereum's transactional data and mutual reviews could build reputation on the blockchain:

The blockchain also enables reputation systems where members can rate one another's performance as collaborators, thereby syndicating trust in the community. Lubin said, "Persistent digital identity or persona and reputation systems will keep us more honest and well behaved toward one another." (Tapscott & Tapscott, 2016a, p. 90)

Potential vendors or lenders [of microcredit] can track their usage and repayment of tiny loans, previously unfeasible, on the blockchain rather than rely on some credit score. "Once a previously unbanked person pays back a microloan, they are on their way to securing more and larger loans to build their businesses," said Lubin. This behavior, when repeated, adds to the reputation score of the borrower [...]

Lubin imagines a future where the "unbanked and underbanked will become increasingly enfranchised as microlending services will enable investors across the globe to construct diverse portfolios of many microloans of which the usage and repayment can be tracked in full detail on the blockchain, using Balanc3's [...] system [an Ethereum-based DApp], for instance." (Tapscott & Tapscott, 2016a, pp. 177–178).

In summary, according to the trustless narrative, the Ethereum platform would be able to establish trust in a trustless environment between different users. These users would be the Ethereum community, investors, and the business community. In this narrative, the consensus algorithm and guaranteed execution were expected to produce trust. Moreover, transparency of smart contracts and DAO code recorded on the public Ethereum platform was emphasized as a potential signal of firm's trustworthiness, and as a way for making interactions auditable. Moreover, it was expected that DAOs would not betray investors, as their smart contract code was public. Attempts at cheating would be discovered in advance and thus be disincentivized. The business community was addressed in particular regarding the aspect of auditable data produced by blockchain. Ethereum-based reputation systems were envisioned to support investors and the Ethereum community in trusting others by drawing on Ethereum's traceable records.

The third function of trust as an interestment device was to promote the Ethereum platform as a trustee. This narrative complimented the two narratives on Ethereum as a trustless system and as a trust-facilitator in trustless environments. The third narrative described the Ethereum platform as a trustee, a "decentralized trustworthy computing [platform]" (Buterin, 2015c). At a meeting with the Ethereum community, recorded on YouTube, a team member stated that "we really want tools that we can use, that are easy to use, but that we can trust. So we trust in that tools. We don't trust in the organization. We trust in the maths, in the nature, not the organizations" (Ethereum, 2014a, 21:53). In a

technical paper, this team member stated his “wish to provide a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about” (Wood, 2014, p. 1). An IT evangelist formulated that the business community’s trust in the consensus algorithm’s reliability and security was a pre-requisite for trusting the transactions. This was especially the case considering the business community’s partial lack of understanding about blockchain platforms.

You could think of consensus as the first layer of a decentralized architecture. It is the basis for the underlying protocol governing a blockchain’s operation.

A consensus algorithm is the nucleus of a blockchain representing the method or protocol that commits the transaction. It is important, because we need to trust these transactions. As a business user, you do not need to understand the exact ways that these algorithms work, as long as you believe in their security and reliability. (Mougayar, 2016, p. 36)

Reasons to trust the Ethereum platform were provided. For software developers in the Ethereum community, the open source code of the Ethereum platform itself was of importance for trusting the platform to act as intended and communicated by the Ethereum team. First, it enabled them to review, try out, and understand the code, and ensure that there was no “backdoor for its developers” (Buterin, 2014f). Buterin explained this in an early blog post before the first test net was released by the team:

The Ethereum project is also excited to announce the alpha release of the open source testnet client to the community [...] This will give people an opportunity to get involved with the project and experiment with Ethereum scripts and contracts, and gain a better understanding of the technical properties of the Ethereum platform. (Buterin, 2014b)

Second, because the entire community and external auditors could review the code, there was reason to assume that the reviews and tests of the masses would improve the code. A team member who was responsible for the platform’s security described in a blog post how reviews on security issues were treated:

We want to keep good track of all issues and only close them once fully resolved and solutions sufficiently tested. Every bug we find is taken care of and will be fixed before [...] release. Feel free to follow us on github [an openly accessible code repository] if you want to keep an eye on the progress. (Steiner, 2015)

The Ethereum community itself pointed out that the decentralized architecture on a multitude of network nodes was supposed to ensure that the platform would be available at any time. Furthermore, this decentralized architecture, in combination with the immutable storage of transactions, should give the community and enterprises confidence that the platform and smart contracts would continue to exist far into the future. This was described in

the *Ethereum Homestead Documentation*: “Every Ethereum node runs the EVM [Ethereum algorithm] in order to maintain consensus across the blockchain. Decentralized consensus gives Ethereum extreme levels of fault tolerance, ensures zero downtime, and makes data stored on the blockchain forever unchangeable and censorship-resistant” (Homestead Documentation Initiative, n.d.h). Moreover, the team claimed that with its decentralized architecture and consensus algorithm, the permissionless Ethereum platform was a “politically decentralized trustworthy computing platform” (Buterin, 2015c). No single actor could manipulate the validation logic of the system or shut it down. The system was trustworthy because, according to the technical yellow paper, “the incorruptibility of judgement, often difficult to find, comes naturally from a disinterested algorithmic interpreter” (Wood, 2014, p. 1).

Lastly, the Ethereum team, IT evangelists, and the business community had an understanding that the Ethereum platform was in a translation process towards mobilization – a moment in the future when actors would not question the Ethereum platform as a black box. Frequently used were analogies to former translations of technologies that were already broadly accepted. Most prominently, examples included the internet (Diedrich, 2016; Mougayar, 2016) and services resting upon it such as online payment (Mougayar, 2016), online video calls, and mobile peer-to-peer messaging (Ethereum team member 1, 2018); former technological innovations, for example the combustion engine (Ethereum, 2016b) also served as illustrations of the early stages of Ethereum’s translation. With the words of an IT evangelist, users’ trust in the platform was still being developed:

Trusting a network of computers that perform mathematical computations instead of a “known, trusted” party that you can see requires a new mental paradigm that we are not used to [...]

As much as we will initially fret over the availability of blockchains as trust services delivery networks, they will be eventually be taken for granted, just as Internet access is taken for granted [for payments] today in most parts of the world. (Mougayar, 2016, p. 70)

In interviews with Ethereum team members, interviewees illustrated their intentions and hopes for the Ethereum platform to become an invisible and trusted technological infrastructure. In this sense, it would be similar to the protocols which constitute the internet, online video calls, or peer-to-peer messaging:

I think Ethereum should be, and eventually is gonna be kind of an underlying layer, kind of like when you are using the internet, there is no reason for you to know that you are using a TCP/IP protocol with a HTTP or hypertext transfer protocol [...] Ethereum is gonna be an underlying layer and it’s gonna be invisible to the user eventually. Right now, because there are [...] [no] user friendly applications to use it, it’s very visible, all the parts of the network, just like how

the internet was hard to use back in the nineties [...] we're kind of in the year 1994 of the internet, it's kind of where Ethereum is in its own realm' (Ethereum team member 2, 2018).

Skype [communications software] used to be a pure peer-to-peer protocol and it's not anymore but [...] there is a bunch of connections that need to be made underneath [...] a huge internet infrastructure that we don't need to care about [...] and now people rely on information and we don't need to think about them, we don't need to understand them, we can just have a call [...] WhatsApp [mobile communications application] has peer-to-peer encryption, point-to-point encryption. She [interviewee's grandmother] doesn't know what that means, she only knows it's a safe place and fast place [...] to share like videos and photos. I want Ethereum to be that [...] where it works, people don't need to understand why, right? (Ethereum team member 1, 2018)

Thus in the third narrative, the Ethereum platform was described as a potential trustee for the Ethereum community, the business community, and any user of Ethereum-based services. The open source governance, the decentralized architecture, and its future technical and societal translation, provided the foundation for the narrative surrounding the Ethereum platform as a trustee.

Overall, trust described in ambiguous narratives behaved as an *interessement* device. It suggested relations among the Ethereum platform, including its smart contracts and DAOs, the Ethereum community, the business community, investors, and potential users in general. The three narratives on trust weaved together characteristics of the Ethereum platform with references to trust. This allowed multiple allies around the platform to be sketched together and the Ethereum platform to be loaded with trust. The proof-of-work consensus algorithm, Ethereum's guaranteed execution of smart contracts, digital signatures, and incentives were all described as characteristics of the trustless system. These could connect users and miners from the Ethereum community and investors through the platform. The business community was expected to be less interested in a trustless system. However, some of these characteristics were also used to argue that the Ethereum platform would facilitate trust. They were complimented by the immutability, traceability, auditability, and transparency of Ethereum's smart contract execution, DAO code, and produced data. In this scenario, investors as well as the business community and other potential users were said to be able to build trust through the Ethereum platform. The platform was at the same time said to become a potential trustee, enhancing trust through its open source character, its decentralized architecture, and its potential for becoming an invisible technological infrastructure. While explicit references to trust served as an *interessement* device in Ethereum's translation, implicit assumptions and the device's trust bases become more easily visible when referring to Möllering's (2006a) trust categories.

5.2.2 Trust

Trust theory has covered many of the aspects of Ethereum's interest-based device. The narrative on the Ethereum platform as being trustless builds on the rationalist paradigm in trust research, whereby self-interested entities take rational decisions to avoid negative outcomes for themselves (Möllering, 2006a, p. 24). The validation of transactions and subsequently the performance of the Ethereum platform relied on the proof-of-work consensus algorithm. It incentivized miners to participate in the operations of the permissionless platform and to perform them correctly. Considerations about alternative consensus mechanisms were dominated by questions of incentives and discussions about avoiding malicious attacks on the platform. Mutual verification of processed transactions by many network nodes assure correct and synchronized data across the network. The decentralized structure, the algorithmic validation, and the incentives were supposed to organize the behavior of the system in such a way that it could provide the team, the Ethereum community, and the business community with certainty that the platform would operate according to expectations. The term trustless explicates the aim to limit uncertainty. It plays with the rationalist assumption that the consensus algorithm, based on game-theoretical considerations and executed by computational devices, replaces trust in centralized systems by relying on logical and secure algorithms. Moreover, the term trustlessness implies making economic relations between economic actors trustless. Users, be it Ethereum community members or business community members, would presumably not have to trust each other, as digital signatures and guaranteed execution of smart contracts were meant to eliminate uncertainty and vulnerability from their interactions.

However, there is a considerable difference between Möllering's (2006a) reason-based trust and the ideal of trustlessness. According to the rationalist paradigm, trustors place trust in others based on their perception that the trustee is incentivized to act to the benefit of the trustor (Möllering, 2006a, p. 43). Thus, while reason in Möllering's (2006a) sense is a (paradoxical) base for trust, trustlessness is a reason-based expectation of not trusting at all within the socio-technical world of Ethereum.

The second narrative about Ethereum as a facilitator of relations relied on similar arguments, but sketched out a relationship of trust between actors who would use the Ethereum platform. The Ethereum platform was described as a trust-facilitator in an otherwise trustless environment. Again, the proof-of-work consensus algorithm was imagined as a facilitator of such trust. Moreover, the narrative described a guarantee of execution to facilitate trust in economic relations between users of the platform. The rationalist perspective

on trust continued in this argument about guaranteed execution. From this point of view, smart contracts executed on the Ethereum platform were a “third party-guarantor and enforcer” (Möllering, 2006a, p. 60) of agreements. They were meant to restrict the ability of platform users to act against the encoded rules. The code itself was considered to be irreversibly executed and documented by the Ethereum platform.

These arguments exhibited a calculative understanding of trust by the Ethereum team and IT evangelists, one which was offered to the Ethereum community, investors, and business community. It stands in contrast to the definition of trust that I introduced in chapter 3.1.2: Trust as a process which deals with “irreducible social vulnerability” (Möllering, 2006a, p. 111). It is trustlessness in the guise of trust. This description carried on in descriptions of DAOs, whose code was supposed to be publicly accessible on the Ethereum blockchain. The underlying assumption was that no organization would publicly launch a DAO that would betray its investors. Thus, investors could trust DAOs, as the transparency of smart contracts signaled trustworthiness and left no room for uncertainty about DAOs’ intentions or operations. Besides transparency prior and during an investment, or other smart contract-based interactions, smart contracts left behind supposedly immutable data. This data was considered auditable, as smart contracts could be traced and events recollected. Although declared to be trustworthy, the mechanism implied a technical control mechanism that could reduce uncertainty between parties interacting through smart contracts.

On the other hand, the same data supplemented with additional peer reviews was suggested as a basis for Ethereum-based reputation systems. The Ethereum co-founder quoted above argued from a reason perspective, i.e. that such reputation systems would incentivize community members to behave well. Moreover, data-based reputation can also be understood through the lens of Zucker’s (1986) concepts of process-based trust and institutional-based trust⁵⁰ (3.1.2), which are also implied in Möllering’s (2006a) concepts of reflexivity and routine. In this theoretical construct, process-based trust is constituted by interpersonal relations and draws upon a series of interactions between the involved parties (Möllering, 2006a, p. 88). According to Möllering (2006a) “Zucker (1986) states that process-based trust is ‘tied to past or expected exchange such as in reputation or gift-exchange’ and informed by ‘a record of prior exchange, often obtained second-hand or by imputation from outcomes of prior exchange’ (p. 60)“ (p. 88). Ethereum’s data-based reputation suggested that investors would be able to gather experience and knowledge about economic exchange partners without

⁵⁰ In the integrative trust framework (Möllering, 2006a), process-based trust is reflected in the reflexivity category, and institutional-based trust is reflected in the routine category (3.1.2).

having to draw upon prior exchange histories. A record of the partners' prior exchanges would be recorded on the public Ethereum blockchain, and could potentially be made accessible to investors through reputation systems. Thus, the Ethereum platform would produce process-based trust based on data of prior exchanges. On the other hand, data-based reputation was supposed to replace existing institutional-trust-producing intermediaries, such as financial institutions, notaries, and contracts, all of which can be considered roles and rules in Möllering's (2006) terms. Data-based reputation, however, also required the parties involved to have shared expectations about Ethereum's role as a provider of immutable and reliable information; it required them to accept the practice of "open execution", which would make interactions transparent. In that sense, the Ethereum platform would act as a new "[system] of rules and meanings that provide common expectations" (Möllering, 2006a, p. 61); in other words, an institutional or routine base for trust between parties who interacted through the platform. Thus, if the public Ethereum platform facilitated trust as a reputation system, this system would merge process and institutional-based trust.

Drawing on Sydow (1998), Möllering (2006a) hints at the necessity of institutions and systems to be trusted in order to facilitate trust. The third narrative in which trust is used as an interessement device prepared Ethereum for its role as a trusted system. Notions of system trust are apparent in the Ethereum team and IT evangelists' visions of the platform's future. From a translation perspective, the Ethereum platform – once unfolded as a technological infrastructure – should be invisible and blackboxed so that everyone would rely on it. In such a state, the Ethereum platform, the Ethereum team, Ethereum community, investors, and the business community would be mobilized so that others would rely on this network as users of specific services and applications. This matches well with what Möllering (2006a) summarizes under routine, namely trust in institutions or social systems. Drawing upon Luhmann's (1979) and Giddens's (1990) notions of system trust, "trust in an institution means confidence in the institution's reliable functioning, but this has to be based mainly on trust in visible controls or representative performances [access points] rather than on the internal workings of the institution as a whole" (Möllering, 2006a, p. 74). Interessement outlines a perspective where the Ethereum platform and other actors are blackboxed and related to potential users as a trustee, whose inner workings do not need to be understood. On the other hand, interessement also outlines trusting relations between the actors within the network. An IT evangelist suggested to the business community that they should use blockchain technology despite their lack of understanding about it. In Möllering's (2006a) sense, they would have to "just do it", and act as if their own uncertainties and lack of knowledge toward

the technology are resolved. At a meeting with the Ethereum community, a team member's claim about trust in algorithms and maths instead of centralized organizations expressed an intention to create a will to believe in the technology. With this, I refer to the will to believe as "a conscious leap of faith" (Möllering, 2006a, p. 121) into a more or less specific other, similar to men's faith in God (James, 1948, p. 107). This unspecific other consisted of the algorithms and math that constituted the Ethereum platform. Potential trustors were the Ethereum team and the Ethereum community. Complementary to this suggestion of a general belief, the Ethereum team also provided reasons for why the Ethereum community and investors should trust the Ethereum platform. These reasons were reminiscent of notions of rationalist trust theory insofar as they relied on the assumption that "people look for good reasons to trust" (Möllering, 2006a, 46). Giving explicit reasons for the trustworthiness of an actor, such as security, high uptimes, and future availability, or independence and incorruptibility, implies an understanding of trust which results from rational considerations on somebody's or something's trustworthiness. In light of trustworthiness indicators (Mayer et al., 1995; McKnight et al., 2011; Möllering, 2006a, pp. 46–50), claims about the platform's security, as well as high uptimes and future availability suggested that it could be perceived as able or competent. Claims of political independence, incorruptibility, and the assurance that there was no 'backdoor' for the developer team suggested that it was benevolent, and had functioning incentives and controls. These trustworthy characteristics were discursively related to the platform's operations on a decentralized network of computer nodes as well as the Ethereum platform's open source code. Lastly, it was also suggested that the Ethereum community and investors would build reflexive trust (Möllering, 2006a) with the Ethereum platform by reviewing, trying, and understanding its various functions. Furthermore, suggestions concerning the team's, the Ethereum community's, investors', and the business community's trust in the platform were subject to enrolment and even mobilization.

Overall, trust as an interessement device suggested relations between the Ethereum platform and other actors. The Ethereum platform was described as a trustless system, as a trust-facilitator, and as a trustee. The suggested trust mechanisms drew on the three bases of trust: Reason, routine and reflexivity. In the next sub-chapter, I examine enrolment, a moment of translation where actors interacted with the platform, and negotiated and tested trusting relations.

5.3 Enrolment: Building trust in Ethereum

5.3.1 Translation

According to Callon (1986b), “to describe enrolment is [...] to describe the group of multilateral negotiations, trials of strength and tricks that accompany the intersements and enable them to succeed.” (p. 211). This also implies negotiating and trying trust in action. Enrolment represents the interactions between the actors which lead to “the formation of an assemblage, a coming together of these diverse actors to create a powerful actor network” (Jeacle, 2017, p. 106). When the enrolment of actors with Ethereum began at the turn from 2013 to 2014, the platform was an assemblage of ideas, far from being ready to use. In 2013, after Vitalik Buterin had “enshrined” (Gerring, 2016) these ideas in the first *White Paper* (Buterin, 2014i),⁵¹ they started to spread; they began enrolling additional team members, the Ethereum platform with its smart contracts, tokens and DAO, the Ethereum community, the business community, and investors, all of whom changed, adopted, used, negotiated, and trusted one another in select instances.

The Ethereum team, with Vitalik Buterin at its forefront, maintained extensive communication with the other human actors. This was pursued via written communication and personal interaction. Written communication included but was not limited to the technical papers about Ethereum, the Ethereum blog, the Ethereum website, social media accounts, discussions with the community in forums (Tual, 2014), and the Ethereum platform’s⁵² publicly available open source code. Books written by IT evangelists and business community members added to these discussions and made stories about blockchain technology and the Ethereum platform available for people who were less familiar with the platform and its online communication channels, mainly the business community. In the introduction of the book *The business blockchain: Promise, practice, and application of the next internet technology*, IT evangelist Mougayar (2016) explicated this translation effort:

Many of its [blockchain’s] smart visionaries were technically inclined people who didn’t focus on succinctly explaining its business implications, or intersections [...] I was determined to make it less dreadful for the rest of us to understand this technology and its ramifications. (Mougayar, 2016, p. 14)

The Ethereum team also involved team members, who had the task of enrolling the Ethereum community. An Ethereum team member, responsible for the team’s communication

⁵¹ The earliest version of the white paper by Vitalik Buterin on the open source platform GitHub dates back to December 2014. According to Diedrich (2016) the original version from 2013 is not available anymore (p. 279).

⁵² The code was available on the openly accessible code repository, GitHub.

and the Ethereum community building, referred in a blog post to the variety of written interactions between the team and the community:

We thank you for your amazing support and participation on social media, including Twitter and of course reddit. Note that because so many of you are tracking a few sites for information on Ethereum, we decided to release all announcements going forward – including change to the protocol or clients [Ethereum platform] – on this blog (the one you are reading now). Finally, note that if you need answers to technical questions, you’ll always be better served by our forums (Tual, 2015b).

In an interview, one Ethereum team member remembered that the Ethereum blog was for a time, the team’s channel for publishing ideas about the development of the platform:

We are always trying to increase our communication of the public, right? And help people to understand what Ethereum is [...] and at some point the blog was the most important blog related to Ethereum, where everyone had any thoughts on it would publish it there. That has changed (Ethereum team member 1, 2018).

The same team member explained to me that he had reworked the Ethereum website to provide the Ethereum community guidance on how to interact with the platform. The site was not yet user-friendly and required some programming skills:

2015 I started to get involved into building the website, right? Someone had built a very basic website for Ethereum, I get involved and I say: “Oh, this website doesn’t explain at all how to use Ethereum [...]”. Back then using Ethereum really meant, you needed to use a terminal and [...] [commands] [...] I started thinking: “Ok, so let’s suppose I am the sort of target user [...]”. So what I started doing is that I started trying out everything that I wanted to do [...] hitting walls, figuring out bugs [...] Cause around then there was no documentation, and I started writing it down, basically writing my history down, writing my steps down, so “here is how you do install Geth [command line tool, which runs Ethereum node]”, “here is how you run Geth”, “here is how you create an account”, “here is how you create your first like little solidity program [smart contracts]”, and I was basically writing all those steps down and I wrote it in a big like documentation [...] and eventually that google doc [documentation] became the Ethereum website [...] that’s sort of still the website today but with adaptations. (Ethereum team member 1, 2018)

Confirming this aim, a community member remembered in an interview that one of his first impressions of Ethereum’s website was that it used to be very informative, instructive and visionary. He described it as a “very nice website, very easy to get up and running, as a developer, they had like test applications” (Ethereum community member, 2018). And he added that there were also “publications and visions of the future and all very well put together” (Ethereum community member, 2018).

Some Ethereum team members started to work on the Ethereum platform as community members or business community members before they joined the team. Even before the Ethereum website provided easy to use information, these actors helped enroll the Ethereum

platform. Based on their general interest in cryptocurrencies and information technologies, they were attracted to the idea of a trustless platform with smart contracts that ran on a decentralized network of computer nodes. Their interactions with Vitalik Buterin as well as their communication and collaboration with the Ethereum team and the community brought them into relation with the notion of trustlessness (the interest device) and thus enrolled them. Some of them recalled these experiences in blog posts and during our interviews:

In January or February 2014, I read about Ethereum for the first time. I watched Vitalik's youtube videos, and I met him in person at the Toronto Decentral Bitcoin Meetups. He obviously knew way more of the tech story than I did, so I became hooked in, this time on Ethereum. Ethereum was the promise of decentralization made accessible to me, someone without much background. It was general purpose smart contracts that could do anything, disrupt any centralized system. It could be and do so many things that it wasn't always clear to me what role ethereum would actually play in the blockchain ecosystem. The blockchain tech story (as I see it) took an exciting turn with Ethereum, and I got to be closer to the action. (Zamfir, 2016)

When Ethereum came along and the white paper came out, I read it and thought "Oh, this is perfect!" You basically take a blockchain, you put programs on it, and it inherits all of the availability and trustless aspects of what a blockchain can provide but for any use case, so it makes it so much more powerful, so that's kind of what drew my attention to Ethereum specifically. (Ethereum team member 2, 2018)

I started getting involved in the community, the community needed help, I started helping them, started helping them with designs, with UX [user experience], with presentation, with anything that anyone needed help. At some point the [Ethereum] Foundation had money to hire people and I took a job. (Ethereum team member 1, 2018)

When I asked whether the Ethereum cryptocurrency already existed at that time, the Ethereum team member added: "No, but it was a community, it was a project, it was an idea, I read the white paper, I figured out that yeah that is a great idea, I want to be part of this" (Ethereum team member 1, 2018) and explained the involvement process more in detail:

I knew something would come along after Bitcoin, right? Something would come along and it would be as big or bigger or as interesting as Bitcoin, and I've started following them all, on Reddit, on Facebook, on Twitter, everywhere: Mastercoin, ColoredCoins, Nxt, Ethereum – Ethereum was just one of them. It just so happened that it was the most active community, so I was following all of them, all the other communities, there were silence and a lot of people were posting things on Ethereum and I started to debate in all those forums and started to get to know people, get to meet them, and that's how I, that's how I got involved. (Ethereum team member 1, 2018)

The idea of a decentralized and trustless general purpose platform as outlined in the *White Paper* (Buterin, 2014i) and discussed and developed through online communication in forums, blogs and other social media, enrolled the Ethereum team and the community. Early community and team members' belief in the platform manifested in their initial contributions

to the platform as volunteers. During this time, they did not receive pay, as the Ethereum team acquired funding in just the second half of 2014 (Buterin, 2014h). As already implied above, the enrolment of Ethereum also drew on personal interactions. Following the example set by the Bitcoin community, from 2014 on, the Ethereum team scheduled local reunions of people interested in Ethereum. These were called meetups⁵³ and following the example of Bitcoin meetups, prompted Ethereum community members to convene in their respective cities. These activities led to a quickly growing network of Ethereum meetups in cities around the world. In a blog post, Buterin described one of the first meetups in San Francisco, which he visited together with another team member:

In the past two weeks our lead C++ developer, Gavin Wood, and myself have been spending a lot of time meeting the local Ethereum community in San Francisco and Silicon Valley. We were very excited to see such a large amount of interest in our project, and the fact that after only two months we have a meetup group that comes together every week, just like the Bitcoin meetup, with over thirty people attending each time. (Buterin, 2014e)

A team member responsible for the teams' communication activities described in a blog post the growth of Ethereum's meetups and he prompted the Ethereum community to organize meetups at their respective locations:

Encouraging the creation of new meetups: we now have an extensive network of 85 meetups worldwide, which is an amazing achievement but not sufficient to handle the overwhelming demand for regular catchups in a format that's appropriate for the local needs and culture. We intend to encourage the creation of new meetups in almost every country and major urban hubs. (Tual, 2014)

In an interview, a team member recalled presenting the Ethereum platform in live demos at hackathons and at meetups, receiving feedback and requests from the Ethereum community. These interactions often led to changes to the Ethereum platform.

Yeah, I was doing a lot of hackathons and meetups, a lot of the things that we did was figuring out how we could help people on hackathons and meetups. We did a lot of live demos of Ethereum working [...] very often the interfaces we built, [...] they would work well in a presentation or in a workshop or in something like that, where we figured out "oh, people who want to get introduced to Ethereum, that's what they need" then we would go back and build that thing. (Ethereum team member 1, 2018)

Some meetups reached considerable numbers of views after the Ethereum team recorded and published them on YouTube.

During hackathons, new team and community members were acquired as the Ethereum platform was made accessible to students for example. Two Ethereum team members discussed these hackathon interactions in their blog posts:

⁵³ Reunions were called after the organizing and scheduling tool [meetup.com](https://www.meetup.com/).

Having been invited [...] at one of these meetups, Ethan and I went to the hackathon prior to the 2014 Bitcoin Expo in Toronto. (Vitalik taught me how to use Merkle trees at this event.) I was thinking about properly incentivizing and decentralizing the peer review system for a couple of weeks, having recently had a paper rejected from an academic journal. Ethan and I tried putting this kind of system together at the hackathon [...] We came in second place at the hackathon [...] We got to meet the whole Ethereum team at the Expo, and we got ourselves invited to the public Skype channels! Charles Hoskinson offered us jobs: It was then, in April 2014, that we started volunteering for Ethereum. (Zamfir, 2016)

The hackathon on transparency was held on November 26th [2014] [...] at CUI Geneva [...]

A diverse group of about 50 people attended the event and we split the presentation in two rooms – one for less-technical people and one for those that brought their laptops looking to build things on Ethereum.

After the presentation [...], we mixed the participants and started the brainstorming session, with everyone thinking about cool ways in which blockchains can be used for transparency in public administration. (Alisie, 2015)

Another personal interaction format for enrolling actors was Ethereum's annual conferences, called DEVCONs. In a blog post, an Ethereum team member recapped the growth of the DEVCON conference between 2014 and 2017:

Devcon0 [in 2014] was an internal developer gathering in Berlin with about fifty people. Devcon1 [in 2015] was held in a ballroom in London with a capacity of 300 people, though closer to 400 people attended. Devcon2 [in 2016] was in a grand ballroom at a hotel in Shanghai with a capacity of 700 people, topping out at closer to 800 participants. We were 2000 participants strong this year [2017]! (Chan, 2017)

Starting in 2015, DEVCONs assembled not only the Ethereum team and the platform, but also the Ethereum community, the business community, and IT evangelists. Video recordings of the presentations and panels published on YouTube documented the enrolment of these actors; moreover, these videos were able to enroll viewers retrospectively.⁵⁴ At conferences, the actors presented and discussed technical and societal visions and goals for the platform, technical developments, and Ethereum-based projects that involved smart contracts, DApps, and DAOs (Ethereum, n.d.b; Ethereum Foundation, n.d.). At these encounters, the Ethereum team, Ethereum community, business community, IT evangelists, and the platform were all enrolled in a network. In a blog post, one team member described the role of DEVCON1 in enrolling other actors: “With the widening interest beyond the core Ethereum community, it was time to spread our collective wings to help the rest of the world see the same ideas that many early adopters had” (Gerring, 2016). Indeed, at DEVCON1, smaller start-ups and

⁵⁴ On October 20, 2018 explanatory videos from DEVCON1 by Ethereum Foundation (2015) and Ethereum (2016a) had 351,701 and 121,335 views respectively. More videos from DEVCONs conferences were available on YouTube playlists by Ethereum (n.d.b) and Ethereum Foundation (n.d.).

projects from the Ethereum community presented their first Ethereum-based implementations with smart contracts; the business community – especially information technology and consulting companies and banks – followed suit (Ethereum, 2015a, 2015b, 2015c; Ethereum Foundation, 2016a; Gerring, 2016). These encounters were also spaces for actors to create ideas for new projects (Higgins, 2016). Interviewees who attended DEVCON2 described how they had been enrolled by the team’s and the community’s expertise, the technical development, the presence of the business community, and the envisioned future of the Ethereum platform. An interviewee from the business community remembered his attendance at DEVCON2:

It was an incredible experience – that [DEVCON2] was the best conference I’ve ever been in my life. Smart people around, that idea that this thing is gonna change the world [...] I felt excited like when I was again back into internet working computing in the early 90s [...] But this was bigger [...] decentralize everything, the entire development suite for Ethereum that was growing and was starting looking a lot like proper enterprise development suite, although it still has problems, still doesn’t work perfectly, [...] you have so many things you can do. But it was really their vision, the vision of the zero knowledge proof, the vision of changing consensus mechanisms to a proof-of-stake, which doesn’t work yet, and I don’t know whether that’s gonna work, but the ability to scale finally at some point. (Blockchain manager at consulting company, 2018a)

An Ethereum community member also mentioned the high quality of people and expertise at hand at the same conference. He emphasized the authenticity of the people and the enrollment of the business community, which altogether fueled the enrollment of more people:

I did go to Shanghai [DEVCON2] [...] I think that was really, it was kind of the beginning of this kind of explosion and growth around that time [...] [I was] really, really enthusiastic [...] you know, they had Microsoft sponsoring the event and they had a stage and everything but like it wasn’t choreographed or stage managed, [...] it was all about the tech and very unpolished presentations. The content was excellent but you know, it wasn’t that kind of corporate plan, stage managed, choreographed kind of conference that you are used to, it was very just authentic, that was the feeling I got from it, you know, and then people from all over the world coming together, and then there was the corporate backing as well; They were all there, the Santander, a big Spanish bank, Microsoft and computer global corporations were sort of there in the background, “what’s going on here? This is really good, so we want to be there from the beginning”. (Ethereum community member, 2018)

Besides these communicative interactions, there were also participatory interactions with the Ethereum platform, smart contracts, Ether, and a DAO. For example, from the aforementioned meetup in San Francisco, Vitalik Buterin described his impression that the Ethereum community engaged with the Ethereum platform through experiments with smart contract and programming adjacent programs as well as building and distributing knowledge:

“People in the community are taking it upon themselves to make educational videos, organize events and experiment with contracts, and one person is even independently starting to write an implementation of Ethereum in node.js [platform for web application development]” (Buterin, 2014e).

The Ethereum team encouraged the Ethereum community to contribute to the development of the Ethereum platform, not only with comments and ideas, but also through direct interaction with the platform. This was accomplished, for example, through testing and experimenting prototype versions and the actual Ethereum platform and engaging in the development of the platform itself. Before the launch of the Ethereum mainnet in 2015, the team launched the so-called bug bounty program, which enrolled the community through joint testing efforts with the Ethereum platform and the team. The team member responsible for the security audit of the platform announced these activities in a blog post:

Prior to the launch, we will also complete a bug bounty program – a major cornerstone of our approach to achieving security.

The bug bounty program will rely on the Ethereum community [...]

Get ready for hunting down flaws in the protocols, Go implementation and network code. (Steiner, 2014)

Moreover, the Ethereum team made testing networks available to the Ethereum community. This allowed them to stress the software before it got released to the Ethereum mainnet. For example, in the run-up to the initial launch of the Ethereum mainnet, Buterin encouraged the Ethereum community to test the limits of blockchain and even offered rewards in Ether:

The purpose of Olympic [test network] is to reward people who try to test the limits of the Ethereum blockchain during the pre-release period, spamming the network with transactions and doing crazy things with the state, so that we can see how the network holds up under high levels of load. At the same time, application developers, data providers, exchanges, and users are encouraged to develop and deploy on the testnet and run nodes – and if you have multiple virtual private servers, spin up as many nodes as you can.

Olympic will feature a total prize fund of up to 25,000 ether. (Buterin, 2015d)

Nevertheless, the team considered the first version of the Ethereum mainnet, which was to be launched by mid of 2015, a playground for developers in the Ethereum community; still far from being a mature and user-friendly software product. A blog post a few days before the launch compared the exploration of the network to the history of American settlement and emphasized on conditions of uncertainty involved in both cases:

[The Ethereum mainnet to be launched] is a live, but barebone implementation of the Ethereum project. It’s intended for technical users, specifically developers. During the [...] release, we

expect early adopters and application developers to establish communities and start forming a live ecosystem. Like their counterparts during the American Frontier, these settlers will be presented with vast opportunities, but will also face many dangers. If building from source and command lines interfaces aren't your cup of tea, we strongly encourage you to wait for a more user-friendly release of the Ethereum software before diving in. (Tual, 2015a)

Nevertheless, the Ethereum community embraced the officially released Ethereum mainnet. Since its launch in 2015, the platform has been run by miners who earn Ether in exchange for operating and verifying transactions with the latest Ethereum software (Homestead Documentation Initiative, n.d.c). Retrospectively, the first release of the Ethereum mainnet turned out to be even more reliable than expected and it motivated the Ethereum community to program with smart contracts and build adjacent applications. This was expressed in the *Ethereum Homestead documentation*:

Even though the [...] release is the first milestone in the Ethereum project and was intended for use by developers as a beta version, it turned out to be more capable and reliable than anyone expected, and developers have rushed in to build solutions and improve the Ethereum ecosystem. (Homestead Documentation Initiative, n.d.c)

In the course of the Ethereum mainnet launch, Ether also became operable as the platform's built-in cryptocurrency. The experimentation and experience, enabled by the digital token Ether and other Ethereum-based tokens, further contributed to enrolment. As specific types of interaction, the buying and selling of cryptocurrencies, including the Ether and other Ethereum-based tokens, also helped enrolled actors. The development of the Ethereum platform itself had initially been funded through a pre-sale of Ether in 2014, one year before the public Ethereum mainnet was finally launched. The pre-sale assembled the Ethereum platform, the team, the Ethereum community, investors, and Ether. In order to gather funding for the Ethereum team and to support activities of the Ethereum community, Ether were sold to investors in a crowd sale against Bitcoins (Homestead Documentation Initiative, n.d.c). It was called a pre-sale, as the Ether was assigned during the sale, but was only produced and usable after the launch of the Ethereum mainnet (still some time ahead). In a blog post that announced the Ether pre-sale, the Ethereum community and investors were explicitly warned about the limitations of Ether's use until the Ethereum platform's release:

Ether will NOT be usable or transferable [bold in original] until the launch of the genesis block. That is to say, when you buy ether and download your wallet, you will not be able to do anything with it until the genesis block launches. (Buterin, 2014h)

Within 42 days the team raised over 31 thousand bitcoin, equivalent to 18 million USD with the sale of over 60 million ETH from the Ethereum community, investors, and the team (Homestead Documentation Initiative, n.d.c). In other words, people invested Bitcoin to

receive a virtual product that was still a concept; something that relied on a platform which was under development. They did so expecting that Ether would later be useable for transfers on the platform and for paying for services on the platform. Ether and the Ethereum platform were subject to considerable uncertainty. Despite the uncertainty and several delays of the issuance period, the sale still attracted high purchase volumes. In the sale announcement, Vitalik Buterin apologized for falling short of the expectations regarding the timeline and thanked the team and the community for their devotion to the project.

I would like to thank the community, and especially those close to the project who have in many cases abandoned their jobs to dedicate their time to it, for their extreme patience regarding the launch of the ether sale. We have been promising that the sale would arise in two weeks for six months, and many team members have endured substantial hardships because of expectations that we set regarding when we would be able to provide funding. (Buterin, 2014h)

The Ethereum team interpreted the investment made by investors as a sign that they believed in the team and the Ethereum platform:

The team was psyched when we got our first million and our second and our third and so on. It was crazy! Believing that we could deliver the Ethereum platform was one thing, but seeing others believe and want to participate it was incredibly inspiring. (Wilcke, 2016)

An interviewee who had invested during the pre-sale⁵⁵ recalled that the pre-sale of Ether was an uncommon way of fund-raising at that time. He invested in order to enroll with the translation of Ethereum and because of the convincing technological idea. His investment, however, was not without skepticism. He recalled: “I was kind of skeptical, I wasn’t sure at all if it was gonna work or not, but it was sounding promising enough that I was wanting to, you know, get in on it” (Ethereum team member 2, 2018). Then he added “it was one of the first, I guess, ways to bootstrap through this type of funding process the development of Ethereum before it was even created” (Ethereum team member 2, 2018). When I asked him whether the funding situation gave him a feeling of insecurity he described that although he believed in the idea of cryptocurrencies, his investments had a gambling flavor and that he risked losing the investment:

Even today, when I deal with cryptocurrencies, it’s kind of this magical internet money, which I really believe in but I’ve never invested more than I can lose. So to me [...] it’s kinda like when you go to the casino or any gamble for fun, but like you know that you can lose that money and you are comfortable with it. (Ethereum team member 2, 2018)

⁵⁵At the time of the interview, the interviewee was an Ethereum team member. At the time of the pre-sale, he was not yet part of the team.

Two interviewees⁵⁶ described how when they were younger, they had been reading about cryptocurrencies on forums. Once the Ethereum mainnet was running, one of them bought Ether when he heard about it from others; the other bought Ether when he saw the price rising. For both, buying and selling cryptocurrencies was an experiment, which then motivated them to acquire more knowledge about blockchain technology and cryptocurrencies.

I didn't really get the technology [of Bitcoin] then at all, but I used to read a lot of forums, [...] and there was people there who are quite into [...] privacy and [...], in methods of encryption and of course cryptocurrencies. So a lot of them were talking about Ethereum, so then I got a little bit of Ethereum, had that as well [in addition to bitcoin]. (ICO advisor 2, 2018)

After recalling how he had sold his Ether and Bitcoin he recalled:

I kinda kept a bit of vague interest and then I think, a couple of years ago [2016] everything started pumping in price quite a lot [...] I said, you know: "What makes these things potentially so valuable?", cause I didn't really know what they were, I just thought, you know, it's just monopoly money on the internet. So I just started doing a lot of research into different cryptocurrencies, [...] buying and selling, but still not really know what they were and I started to learn a little bit more [...] when I buy a new one I learned a little bit about it, but I hadn't really gone into say in depth white paper analysis, it'd be more just reading kind of the concepts, and at that time [2016] it was all just concepts cause nothing, no one really had a product and there was nothing being built at all. (ICO advisor 2, 2018)

I saw it [price of Ether] rising a bit and then I go: "Ok, I buy some and see what happens" and then yeah, I just became really interested in what blockchain can actually do. Just read upon every new cryptocurrency I would find that was coming out, got involved in buying and selling cryptocurrencies. (ICO advisor 1, 2018)

However, there was a less successful investment episode in the enrolment of Ethereum. Temporary mutual trust among the Ethereum team, the Ethereum community and investors and their belief in the technical actor DAO and its underlying Ethereum platform was disappointed. In 2016, an Ethereum-based DAO, called The DAO, was programmed and launched. The initiators were former and active members of the Ethereum team. The purpose of The DAO was to collect Ether from investors and allocate these funds to applicable projects. Investors could transfer Ether to The DAO and receive in exchange tokens proprietary of The DAO along with voting rights. All transactions were operated and recorded by the Ethereum platform. The DAO was specified in a white paper by one of the initiators and programmed according to a decentral approach by the initiators and various members of the Ethereum community (Jentzsch, 2016). During the investment phase, approximately 12

⁵⁶ At the time of the interview, the two interviewees were advising blockchain start-ups on fundraising. Here they recall their past when they were students who bought and sold cryptocurrencies.

million ETH⁵⁷ (approximately 250 million USD) were invested into The DAO by an estimate of 10,000 to 20,000 people (DuPont, 2018, p. 158).⁵⁸ This – at that time – surprisingly high attraction of investments appeared besides controversial public discussions among the Ethereum team, the Ethereum community, and The DAO initiators about The DAO’s technical security (DuPont, 2018, pp. 162–163). *The Economist* concluded that those investors were “believers” and that “in the strange world of crypto-currencies, faith and rationality go together like yin and yang” (“Crypto-investing,” 2016). Blockchain and governance researcher DuPont (2018) summarizes these and subsequent incidents in his online ethnography:

However, [...] on June 17, 2016, The DAO’s code was “exploited” by an unknown individual. This exploit used unintended behavior of the code’s logic to rapidly drain the fund of millions of dollars’ worth of ETH tokens. Immediately, Slock.it [initiators of The DAO], the leaders of the Ethereum platform [Ethereum team], numerous cryptocurrency exchanges, and other informal technical leaders stepped in to stem the bleeding – shutting down “exits” through the exchanges, and launching counterattacks [...] In the end, the whole project was disbanded, with an inglorious “hard fork” rolling back the ostensibly “immutable” ledger. (DuPont, 2018, p. 158)

This hard fork consisted in an irreversible software update to the Ethereum mainnet, which modified the transaction history and refunded drained Ether to investors. It was deployed by the majority of Ethereum nodes after several weeks of discussions and the persuasion of Buterin and other Ethereum team members (DuPont, 2018, pp. 164–165). This meant that the Ethereum team and the Ethereum community jointly manipulated one of the Ethereum platform’s key characteristics to revert the unintended behavior of The DAO – Ethereum’s presumably immutable ledger. Some members of the business community appreciated the Ethereum team and Ethereum community’s learning and the problem-solving. German business magazine *Wirtschaftswoche Online* quoted managers from a bank and a consulting company:

‘That is a good reminder that we need clear rules, standards, and security tests for the blockchain’ said [...] Chief Digital Officer at Deutsche Bank. ‘But it has no impact on our plans and tests with blockchain technology.’

The fast reaction to the incident could boost the importance of Ether, believes [...] blockchain expert at consulting firm EY. Despite all the difficulties, the Ethereum programmers, who are organized in a decentralized way, have dealt better with the flaw than major corporations like Microsoft which have software bugs. (Voß, 2016)

⁵⁷ The total amount of invested ETH represented a share of 14% of all ETH existing at that time (DuPont, 2018).

⁵⁸ For further reading, DuPont (2018) provides a detailed online ethnography of the emergence and downfall of the DAO.

As illustrated in *Wirtschaftswoche Online* IT evangelists also continued to cheer for blockchain technology:

Alex Tapsoctt, co-author of the book ‘Blockchain Revolution’ [...] agrees with this. ‘Blockchains are extremely secure, particularly in comparison with centralized computer systems of companies like JP Morgan, Home Depot and many others, which get hacked on a regular basis.’ (Voß, 2016)

On the other hand, a smaller part of the Ethereum community opposed the hard fork because from their perspective, it breached the principles of the platform that they believed in. Thus, they continued to maintain and use Ethereum Classic, a version of the Ethereum platform and a respective cryptocurrency without the software update (DuPont, 2018, p. 165). The enrolment of these actors had failed at that point and they constituted a separate and alternative network. Nevertheless, the Ethereum team and the majority of the Ethereum community stuck by the forked platform and its currency (Buterin, 2016d). In interviews, Ethereum team members reflected that the Ethereum team, the community, and the investors had been overconfident with regard to the abilities of the Ethereum platform. This included overconfidence in The DAO and with regard to the coherence of the actor-network.

I would say we were overconfident about our cohesion and [...] we were overconfident about “yeah, everyone loves each other, we are great, we are awesome, we will never run into problems” and then we sort of run into problems and then we realized the limitations [...] I think, since The DAO the community has been a lot more conservative with forks and big changes and with security [...] and everyone is taking security a lot, a lot, a lot more seriously and things like that. (Ethereum team member 1, 2018)

When I asked what he meant by taking things more seriously he replied:

I would say that probably people took a lot more risks then and I can’t like pin point anything specific, I would just say that everyone became a little bit more [...] risk averse because we understood what the risks were, right? (Ethereum team member 1, 2018)

According to one of the interviewees, the incident rendered visible uncertainties that arose from the technology and from interrelations among different actors. One team member recalled that “the DAO was unprecedented with the amount of money it raised and because people thought the network was more stable at that point they were more apt to trust it” (Ethereum team member 2, 2018). He continued:

[The DAO] was a major turning point because after that happened, it tested the resilience of the community to make hard decisions about when to do a hard fork and it also highlighted some of the need for security in smart contracts, so up to [...] stuff like [...] formalizing – I think it’s called formal verification – and some other techniques to make contracts secure, had not been fully explored or have been put on the back burner, and now security was at the forefront of [...] this whole deal. (Ethereum team member 2, 2018)

The DAO incident and the subsequent split of the Ethereum platform and the community, made actors aware of the platform's (and their own) vulnerability. The team, the community and investors found themselves in a still ongoing discourse about how to deal with the Ethereum platform's unintended behavior versus its supposedly guaranteed execution and certainty through proof-of-work consensus. Through enrolment, the characteristics which constituted the interest device of Ethereum as a trustless platform turned into negotiable features. The question whether businesses – the established business community and startups from the Ethereum community – could trust the Ethereum platform to preserve funds in spite of smart contracts vulnerabilities raised questions about whether the team and the community should be empowered to break the platform's immutability again. In one of my interviews a blockchain reporter illustrated this as follows:

The repercussions are deep, like seriously and this is like one of [...] my main research topics now [...] the question of lost funds, fund recovery. And it's also a really interesting question for [...] business adoption of Ethereum. So, like Ethereum code Solidity [smart contract programming language] often has bugs and money gets like tangled up in mistakes. And then it's like you can make a little edit to get the money back but ever since the DAO [...] the community is like wounded [...] Vitalik said something like "the DAO is an exception because it was very early on" and like "But we are not gonna do this until Ethereum gets, you know, more mature" [...] but other people say like "we need some kind of insurance, if it's like, you know, our code made a mistake and now a business just lost 20 million or whatever, like we need to be able to, you know, have a degree of insurance responsibility for that money". And yeah, there is that conversation going on (Blockchain reporter, 2018).

However, unaffected by The DAO incident, the business community enrolled with the Ethereum platform through experiments off the Ethereum mainnet, its Ether investments and troubles with immutability. Instead of experimenting on the Ethereum mainnet, they created their own permissioned and private test networks based on the Ethereum platform code.

In an interview, one blockchain manager at an IT consultancy who worked on projects with corporate clients explained that for the business community, Ethereum was the first platform that enabled them to experiment. He hinted at early trials by a Swiss bank, which also presented their project at DEVCON1 (Ethereum, 2015c): "UBS made their first go at smart bonds on Ethereum" (Blockchain manager at information technology and consulting company, 2017). For the business community, experimenting with smart contracts based on Ethereum made blockchain technology tangible and allowed them gain knowledge about its functions. In turn, these experiments enabled employees at established enterprises to relate blockchain technology to their own business processes and guess what its impact could be. A community member who worked on Ethereum smart contract projects with corporate clients

recalled his experiences from those interactions: “[In 2017] I was doing a lot of contracting, blockchain related contracting work and smart contract development [for corporate clients]” (Ethereum community member, 2018). He described how these projects worked in general:

So we have this smart contract platforms publicly available to people and we were gonna go and deploy smart contracts there, and I was sort of helping clients to blockchainize their business processes or explore how they could blockchainize their existing business processes (Ethereum community member, 2018).

He then specified the approach taken by the business community:

To identify blockchainizable aspects of your business you run a proof-of-concept and then by doing that, by going through that process you can understand the technology more, you can actually educate your teams internally, educate your people and people understand a little bit more and then they can see this proof of concept, how it relates to their business and it’s a lot easier to understand. (Ethereum community member, 2018)

This Ethereum community member also expressed that in 2018, the business community was still highly active in developing such proofs of concept. As many of these companies lacked knowledge about blockchain technology, they drew on help from the Ethereum community:

If you go to any of those blockchain conferences and you get talking to people and give them your card, you know, the large proportion of them are gonna be phoning you, looking for you to help them with their implementations [...] I mean even at the moment there is so many large corporations, like you could say Fortune 500 in America, they are all doing proofs of concepts and blockchain, you know, they all need expertise to come in to help to build these proof of concept projects. (Ethereum community member, 2018)

Another blockchain manager at an IT consultancy described how he had developed a pilot on corporate bonds with a bank, a car manufacturer, and the Ethereum platform:

A typical project that we conduct with somebody [was] for example corporate bonds on blockchain [...] And we have implemented it with Ethereum [...] That was the first project in the German industry, with [...] [the car manufacturer and the bank], a financial product on the capital market, implemented on blockchain, and we have contributed to it. (Blockchain manager at information technology and consulting company, 2017)

He emphasized that such projects were just initial trials:

Basically, it’s about automating a book building process and to tokenize the stakes [...] the steps, which were suited, were kinda newly built on a blockchain. Obviously, it’s not a world-changing thing within such an isolated application [...] it’s like first trials, which are just beginning. (Blockchain manager at information technology and consulting company, 2017)

Asked whether the corporate bond had been issued on the Ethereum mainnet, the interviewee conceded that it was realized with a “private blockchain [network]” (Blockchain manager at information technology and consulting company, 2017) based on the Ethereum code. This meant that the network nodes running within such projects were not part of the

Ethereum mainnet, but constituted a separate, permissioned network of their own. Also, the transactions taking place there were not conducted on the Ethereum mainnet, nor was the shared ledger visible. It was a network based on Ethereum code that ran in parallel. This sort of enrolment by the business community of the Ethereum platform was not an isolated case.

In fact, since 2015, Microsoft – in cooperation with a startup from the Ethereum community – has provided a cloud service for the business community to build and experiment with private and permissioned Ethereum networks. These were also presented at DEVCON1 and DEVCON2 (Ethereum, 2015a; Hallam, 2016). In a Microsoft blog post, one Microsoft manager explicated the purpose of the cloud service:

Microsoft and ConsenSys are partnering to offer Ethereum Blockchain as a Service (EBaaS) on Microsoft Azure so Enterprise clients and developers can have a single click cloud based blockchain developer environment. The initial offering contains two tools that allow for rapid development of SmartContract based applications [...]

“Ethereum Blockchain as a Service” [...] allows for financial services customers and partners to play, learn, and fail fast at a low cost in a ready-made dev/test/production environment. It will allow them to create private, public and consortium based Blockchain environments (Gray, 2015).

Besides this technical integration with Microsoft, Buterin and team members who founded startups in the Ethereum community generally supported the business community’s usage of Ethereum code for permissioned networks with private ledgers (Consensus Systems, n.d.; Parity Technologies, n.d.). Following up on conversations at DEVCON1, the bank J.P. Morgan – together with a startup from the community – started to develop the permissioned and private blockchain platform Quorum based on the Ethereum code (Higgins, 2016). When J.P. Morgan’s ongoing efforts were made public in 2016, *The Wall Street Journal Online* emphasized how the enrolment of the bank with the Ethereum platform had occurred despite The DAO affair. Moreover, it described that the bank drew on the Ethereum platform, but aimed to differentiate its data accessibility to comply with different requirements of traders and regulators:

J.P. Morgan engineers say they have found a way to limit access to transactions shared via a network to people who need to know the details, like parties to the trade or a regulator.

The project—called Quorum—is being built off the publicly accessible Ethereum network code [...]

It also is a vote of confidence in Ethereum, which is the network where a separate application created by venture-capital firm DAO was hacked [...]

In recent months, engineers at J.P. Morgan have been jumping into Ethereum to solve a problem that has complicated the use of blockchains at banks: making it private enough for traders, but public enough for regulators. (Demos, 2016)

Also in 2016, Vitalik Buterin released instructions for the business community on how to use the Ethereum code for private and permissioned blockchain networks (Buterin, 2016c). According to a blockchain manager at an IT consultancy, who I interviewed, this happened because “the demand from the industry was too strong” (Blockchain manager at information technology and consulting company, 2017). He explained that with this approach, companies could configure their own blockchain networks into a proprietary IT environment and get rid of the proof-of-work-consensus within their own Ethereum networks. According to him, businesses felt that this implied less risks and more control over the network than was possible with the Ethereum mainnet:

Just as a second step, around a year ago [2016], when Hyperledger followed quickly, still not yet as mature but [...] when the first available releases came out, [...] then Ethereum also made such a release where one could build a private blockchain based on the Ethereum platform. One can take Ethereum’s source code as a product and run it in an own environment. One can configure it, configure mining away and configure proof-of-authority as a consensus algorithm and determine how it should look like and how it should work and also run as a private blockchain, so that Ethereum is basically able to do both at the moment. It can also run as a public blockchain and one can deploy own applications at the risk of an infrastructure, which is beyond control, decentralized and without influence for the one, who deploys his smart contract or on an own blockchain. If three banks did it among them based on Ethereum, they would just configure proof-of-authority and run their own nodes and send transactions among themselves. (Blockchain manager at information technology and consulting company, 2017)

Such negotiations and changes to Ethereum’s data transparency in permissioned networks did not leave the Ethereum mainnet untouched. Already before the launch of the Ethereum mainnet, Vitalik Buterin had acknowledged that “Ethereum, as it stands today, will in many cases inherit the transparency side of blockchain technology much more so than the privacy side” (Buterin, 2014j). The emergence of websites that visualized blockchain data stored on the Ethereum mainnet made Ethereum’s data transparency apparent. On these websites, one could see the recorded transactions, including smart contracts between Ethereum accounts (Reitwiessner, 2016). In an interview, a blockchain reporter described their “amazing comparative charts where [...] you could also visit like smart contract transactions on the blockchain history” (Blockchain reporter, 2018). This enabled the Ethereum community and other actors to review data. However, the flipside of Ethereum’s data provisioning was that this data allowed Ethereum accounts to be traced back to actual owners. In his book on

Ethereum, IBM's contact person to the Ethereum community described that the platform disclosed information in a way that users were not anonymous:

It's not like your name and street address is stored on the blockchain from using it. But the patterns that can arise from using Ethereum accounts can give away so much *meta information* [italics in original] that the owner could be identified from it. (Diedrich, 2016, p. 53)

This contradicted the initial problematization of transparency for large organizations and privacy for users. In a blog post that discussed different approaches for data privacy, Buterin referred to criticism by the business community and acknowledged that the Ethereum community would not want their data to be publicly accessible by third parties:

However, when I and others talk to companies about building their applications on a blockchain, two primary issues always come up: scalability and privacy [...] The other major problem that blockchains have is privacy [...] neither companies or individuals are particularly keen on publishing all of their information onto a public database that can be arbitrarily read without any restrictions by one's own government, foreign governments, family members, coworkers and business competitors. (Buterin, 2016a)

By the end of 2017, an additional feature allowed users to disguise newly added smart contracts on the public Ethereum blockchain through computational encryption (O'Leary, 2017). However, this mechanism was so expansive that it wasn't actually used. The reporter that I interviewed expected this problem to take time to solve (Blockchain reporter, 2018). She summarized that in 2018, the Ethereum mainnet still required additional privacy features in order to be accepted by the business community. J.P. Morgan, meanwhile, built their own Ethereum-based platform with enhanced privacy features:

Ethereum like, most public protocols are horrific from a privacy perspective. Because it's like not just like some random business has your information in the database, it's like, it's on the internet, anyone can access it, which is worse. It's like twitter for your bank account [...] or for your business operations. So it's really fucked [...] It's one of the things I like about Quorum, the private blockchain, because it was such a problem for J.P. Morgan [...] they don't wanna [...] share information without surrendering information ownership, which is a really nice way of putting it, but when it comes to business practices and stuff there has to be a degree of confidentiality and they built that into their blockchain with like new cryptography techniques [...] you can use smart contracts in a way that people can tell who owns the contract and how much money is in it but they can't tell anything about the properties or [...] what kind of system aside from those factors. (Blockchain reporter, 2018)

As an example the reporter added:

Like we made an exchange that I'm gonna trade you oil in exchange for money and we'd coded this into some contract, so it's like visible that you've paid me 10,000 but the oil thing is: No one knows it's oil. (Blockchain reporter, 2018)

Overall, the negotiations about and changes to Ethereum's data privacy addressed a feature of the Ethereum platform, which was originally a supportive element to trust (the

interessement device). The transparency of data in the Ethereum platform was part of the narrative surrounding Ethereum's supposed facilitation of trust. Enrolment, however, made apparent that publicly accessible data was a feature that the business community would not adopt. Thus, the Ethereum team, the business community, and the community made changes to the platform accordingly.

Overall, in its various forms and interactions with Ethereum team, community, business community and investors, the Ethereum platform – including Ether, other cryptocurrencies, smart contracts, The DAO – enrolled these various actors. A translation perspective posits that these actors (including the platform) mutually influenced each other during interaction. In the following, I explore the ontologies of trust implied in these enrolments.

5.3.2 Trust

The enrolment of Ethereum exemplifies several interactions and negotiations between the platform, Ether, other cryptocurrencies, smart contracts, the DAO, the Ethereum team, the Ethereum community, investors, IT evangelists, and the business community. These interactions produce glimpses of trust and reliance, but also breaches of trust. Some of the instances of successful enrolment described above are moments where actors articulate their beliefs and take leaps of faith. Early Ethereum community and team members as well as investors believed in the ideas of trustless interactions and decentralized computing. Even though the Ethereum platform was far from being built, the ideas of continuing the principles of Bitcoin and to combining them with smart contracts, and creating a general purpose platform were perceived as “perfect”, “a great idea”, “powerful” and able to “do anything, disrupt any centralized system”. One can see here a quasi-religious faith held by the Ethereum team, community members and investors – the will to believe in an unspecified other (Möllering, 2006a, pp. 119–121). In the case of Ethereum, this unspecified other consisted of the decentrally maintained Ethereum platform and its smart contracts (as an idea and later the technical system), which supposedly enabled trustless interactions. Some early community and team members implicitly expressed such a belief by volunteering and helping build the Ethereum platform.

Investments in Ether, during and after the pre-sale, also pointed to community members' and investors' cautious leaps of faith. For one community member, the Ethereum platform proposal “was sounding promising”, another investor “got a little bit of Ether [...] kinda kept a bit of vague interest”, another one decided to “buy some and see what happens”. These actions show small leaps of faith, indications of as-if attitudes; actions undertaken as if the

uncertainty of losing investment money could be favorably resolved (Möllering, 2006a, pp. 112–115). Uncertainties were rendered especially visible when investors expressed skepticism about the Ether pre-sale as an unfamiliar practice, and when they acknowledged they lacked knowledge about the technology. Missing information was complemented with hope and curiosity, resulting in the purchase of Ether. This leap of faith was, however, not essentialist, as in the case of patient decisions in medical care (Möllering, 2006a, 121–124). Rather, it was limited as insofar as actors restricted their potential losses. To them, Ether and other cryptocurrencies were perceived as “magical internet money” and “monopoly money on the internet”. At the same time, the continued trading of cryptocurrencies based on these small leaps of faith were part of a familiarization and learning process (Luhmann, 1979). It started from observations and recommendations in online forums, information from the Ethereum *White Paper* as well as the observation of a growing demand of Ether (reflected in rising prices). This in turn led to the wish of some investors to learn and read more about blockchain technology. In this sense, community members’ and investors’ small leaps of faith toward Ether and the Ethereum platform provided impetus for processes of reflexive trust building (Möllering, 2006a).

Ethereum community members, team members, investors, and business community members mentioned the Ethereum platform or Ether in the same breath, which enrolled them deeper into the Ethereum network. Personal meetings among Ethereum team members, other community members, the business community, and IT evangelists at meetups, conferences like DEVCONs, in online communication provided the Ethereum community, the business community and investors knowledge about the Ethereum platform. These meetings also staged places where trust could be built. At DEVCON2, software developers and blockchain managers from the Ethereum community and the businesses community had the impression that the team and the community were authentic, smart, and visionary. From a rationalist trustworthiness perspective (Möllering, 2006a), the Ethereum team’s and community’s perceived authenticity and their visions of the platform can be understood as benevolence (Mayer et al., 1995). Similarly, smart people became an indicator for the team’s and the community’s ability to build and improve the Ethereum platform. Knowledge provision in interpersonal exchanges as well as through online communication channels can be understood as practices of reflexive trust building (Möllering, 2006a). Individuals who joined the Ethereum community, the Ethereum team, and the business community described how it strengthened their belief in the potential capabilities of the Ethereum platform; they also expressed their wishes to further engage in building the platform or working with it. People

who joined the Ethereum community or the team mentioned that YouTube videos by Vitalik Buterin, meetings with the team in person, reading the *White Paper*, descriptions, guidance, and visions on the Ethereum website convinced them that Ethereum was a trustless and promising platform. In the sense of Zand's (1972) spiral of trust, signals of trust by the Ethereum team towards other actors were evident in the sharing of ideas, problems, and emotions in Ethereum blog entries, and in invitations to collaborate. Some community members participated in the spiral by debating, executing tasks, testing, and experimenting. In that sense, the collaboration among Ethereum team members and the community in forums, at meetups, and at hackathons were occasions for a self-enforcing, reflexive trust building process (Möllering, 2006a) between the Ethereum platform, the Ethereum team, and the community. Through these activities, they were familiarized with the platform and at the same time gained influence over the platforms' creation – for example, by reporting bugs through the bug bounty program, working on the user experience, or providing feedback at meetups and hackathons. The Ethereum community's and the business community's experimentation with smart contracts were also acts of familiarization. It is important to point out, however, that this was not familiarization with a stable technological infrastructure, but with a constantly changing actor. When the Ethereum mainnet was launched, the team even warned the Ethereum community about the immaturity of the platform and recommended its use only to programmers. The community nevertheless just did it (Möllering, 2006a, pp. 115–119): Participating in mining and starting to launch smart contracts on the Ethereum mainnet. So, where trust of the Ethereum community, the team, investors, and the business community occurred, it was directed towards the interplay of Ethereum team, Ethereum community, and Ethereum platform.

This interplay of trusting relations was rendered visible through retrospective takes on the DAO incident. The DAO incident illustrated a coming together of actors, which mutually trusted each other. It also signified the partial breakdown of this trust network. Before and throughout the investment phase for The DAO, technical vulnerabilities of The DAO were discovered, but investors nevertheless transferred Ether to it. Through enrolment, rationality from interestment was displaced by faith. Retrospectively, the Ethereum team, the Ethereum community, and investors asserted they were “overconfident” with regard to the “cohesion” among the Ethereum team, community, and investors as well as with regard to the vulnerabilities of smart contracts and stability of the platform. In other words, until the exploit happened, actors temporarily acted with confidence and trust in one other, in The DAO, and in the Ethereum platform. They behaved as though known and unknown uncertainties could

be favorably resolved (Möllering, 2006a, p. 111). The unintended disappointment of the Ethereum team, community, and investors in The DAO incident and the concurrent debates about how to proceed rendered trust in The DAO and the platform visible and subject to breakdown. Finally, the The DAO incident brought the Ethereum team and large parts of the Ethereum community to manipulate the Ethereum platform with a hard fork; it also caused smaller part of the community to split and maintain the former platform along with its currency as Ethereum Classic. This divide shows that this smaller faction prevalingly trusted The DAO and the Ethereum platform with their allegedly trustless characteristics, while the majority of the Ethereum community, investors, and the team implicitly relied on a relational network constituted by the platform, the team, and the community including its mining capacities. Since then, a reflexive trust building process by the Ethereum team, the Ethereum community, business community, the Ethereum platform, and smart contracts has continued to negotiate which practices and platform characteristics are required for supporting and stabilizing trust in Ethereum and smart contracts. This process also acknowledged that smart contracts were subject to unintentional flaws that made other actors vulnerable. The business community's positive acknowledgement of the team's and the community's fast reactions to The DAO incident, as well as these actors' call for reliable structures points to how the business community refrained from acknowledging the notion of trustlessness. They valued joint actions of the platform and the other supportive actors instead of relying solely on the technical platform.

Generally, trust building in the business community was dissociated from the Ethereum mainnet and DAOs. The trials and familiarization carried out in the business community occurred with smart contracts on permissioned and private test networks. Experiments by the business community started with translations of established, but simple business processes into smart contracts. In such settings, they related familiar process to unfamiliar smart contracts and tokens. One example was the well-established financial instrument of corporate bonds. This instrument was represented as a token in an Ethereum network and issued accordingly. By doing such pilots and other proofs of concepts, firms did not fully rely on the Ethereum platform, but saw these interactions as "trials". These were small steps to get to know the technology – a trust building mechanism which Möllering (2006a) describes as a reflexive process between human actors. These trials helped the companies understand the technology and imagine how it could be applied in their respective businesses. Thus, knowledge about and first-hand experience with the technology contributed to the enrolment of the business community. In some cases, Ethereum community members who had gained

experience with the Ethereum platform translated their knowledge to the business community. In such settings, trust in the technology was accompanied by interpersonal relations between the business community and the Ethereum community. The adoption of smart contracts by the business community was not unidirectional. Even though it was enrolled with the Ethereum network, the business community was not disposed to making itself vulnerable to the platform's public data transparency. Together with members of the Ethereum community and the team, they translated the platform into private and permissioned networks; this unconfigured the proof-of-work consensus and Ether, and turned data privacy and permissions into a condition for the business community to further trust the platform. The question of whether transparency actually rendered the Ethereum platform trustworthy or untrustworthy for day-to-day use fed back into the Ethereum mainnet and prompted changes to its privacy settings. Although these negotiations were not resolved at the time of writing, the following chapter describes how several actors were mobilized in temporarily stable networks by drawing upon processes of reflexive trust building from enrolment.

5.4 Mobilization: Daring to rely on Ethereum

5.4.1 Translation

Ethereum was not a mobilized black box that I have opened in my description retrospectively, but an actor-network I observed in the making. Earlier I anticipated that blockchain, including the Ethereum platform, was still an emerging technology (1, 2). However, throughout the observation period, the Ethereum platform “[rendered] entities mobile which were not so beforehand” (Callon, 1986b, p. 216). Hereafter, I describe three assemblages that were temporary manifestations of a mobilized Ethereum actor-network.

In 2017, an assemblage of members of the business community, the Ethereum team, and the Ethereum community founded the Enterprise Ethereum Alliance (EEA). On its website, the EEA claimed that “Ethereum’s intrinsically trusted system is the most promising solution for enterprise Blockchain adoption, given its maturity and multi-purpose design” (“Enterprise Ethereum Alliance,” n.d.b). As *The New York Times* reported, the alliance pursued activities that would advance and mobilize an Ethereum codebase for permissioned and private blockchain networks, i.e. without a proof-of-work consensus and without Ether. The software was primarily intended for use by enterprises:

The group is working to develop versions of the Ethereum software that are battle tested enough to be used in a corporate setting.

Does that mean the world's biggest companies will corner the market on Ether?

The versions of the Ethereum software that companies are building will most likely be used to set up private networks that would be totally separate from the public Ethereum network and that would not use the Ether currency. (Popper, 2017)

This alliance assembled actors – including information technology and financial services firms, the Ethereum community and Vitalik Buterin – that had enrolled extensively with Ethereum to mobilize the platform at enterprises. Quotes from EEA members in the alliance’s initial press release described their translation from enrolment to mobilization. The press release quotes Vitalik Buterin on his expectation that EEA could help standardize a private and permissioned version of the Ethereum platform that could further mobilize the business community:

“The Enterprise Ethereum Alliance project can play an important role in standardizing approaches for privacy, permissioning and providing alternative consensus algorithms to improve its usability in enterprise settings, and the resources the project and its members are contributing should accelerate the advancement of the Ethereum ecosystem generally,” said Mr. Buterin (Enterprise Ethereum Alliance, 2017).

Several members of the business community were quoted on their enrolment experiences with the platform, the team, business and Ethereum community. Based on these experiences, these actors were disposed to further support the Ethereum platform through the EEA:

“J.P. Morgan is an active supporter of both emerging technologies and open source projects. We look forward to continuing to advance the state-of-the-art in blockchain technology with the diverse expertise and collaborative energy of the Enterprise Ethereum Alliance.” [italics in original]

–[...] Chief Information Officer, J.P. Morgan Corporate and Investment Bank (Enterprise Ethereum Alliance, 2017).

“At Microsoft, we are proud to be a founding member and board member of the Enterprise Ethereum Alliance to continue the advancement of enterprise grade blockchain platforms. Participating with the Ethereum community to implement open standards will accelerate deployment of blockchain solutions [...]” [italics in original]

–[...] Principal Architect, Azure Blockchain Engineering at Microsoft (Enterprise Ethereum Alliance, 2017).

“UBS has actively used Ethereum to explore the potential of blockchain technology for the past two years. We are enthusiastic that the Enterprise Ethereum Alliance provides a platform to collaborate [...] for industry-wide adoption of the technology.” [italics in original]

–[...] Global Blockchain Lead and Head of UK Group Innovation, UBS (Enterprise Ethereum Alliance, 2017).

“Like many financial institutions, Santander has been actively exploring the use of distributed ledger technology and Ethereum has been one of the platforms-of-choice on which to build proof-of-concepts and prototypes. With its large developer community, 1.5 years of testing in a public environment, and multiple implementations, Santander is enthusiastic in its support of

the goals of the Enterprise Ethereum Alliance and its goal of developing a single set of standards for using Ethereum in an enterprise setting.” [italics in original]

–[...] Head of Research & Development for Innovation, Banco Santander (Enterprise Ethereum Alliance, 2017)

The founder of one of the first Ethereum software and consulting firms supported private platforms for the business community, which could interact with the public Ethereum mainnet in the future:

“In our enterprise consulting work we advise prospective clients to build a blockchain stack on Ethereum, because private permissioned versions of Ethereum represent the most capable, best hardened blockchain architectures for those contexts. It will grow increasingly important that enterprise builds on private infrastructure that is compatible with the public Ethereum mainnet [...]” [italics in original]

–[...] Founder of ConsenSys, Co-Founder of Ethereum (Enterprise Ethereum Alliance, 2017).

Under the heading of the Enterprise Ethereum Alliance, the Ethereum platform assembled Vitalik Buterin as a member of the Ethereum team, members of the Ethereum community, and the business community. They had experiences in common with the platform and shared the goal to mobilize a version of Ethereum in enterprises. The *Financial Times* put Vitalik Buterin’s translation in a nutshell:

The EEA reflects Buterin’s changing mindset [...]

But he came to realise these people [governments, banks and major corporations] “aren’t that different from people anywhere else”. Purists might call this betraying blockchain’s roots; Buterin paints it as pragmatism, coloured with anxiety about governments with “hundreds of billions of dollars of physical weaponry, plenty of prisons ... increasing amounts of internet surveillance”. (Cornish, 2018)

Another assemblage showed that the Ethereum platform also influenced investment practices as it turned into a new spokesman for investors. These practices, called Initial Coin Offerings (ICOs) became increasingly popular throughout 2017. In an interview, two former investors who consulted start-ups on doing ICOs explained how ICOs (which were mostly conducted through the Ethereum mainnet) functioned:

An ICO today, it’s a method of raising funds for an early stage tech company [mostly distributed ledger technology], where you exchange something [...] usually Ether in exchange for a digital token or sometimes it’s actually a promise for a [...] digital token at some point in the future. (ICO advisor 2, 2018)

So the idea of raising funds directly through the sale of tokens – something which had enrolled investors during Ethereum’s pre-sale and with The DAO – turned into a more popular practice. People continued to speculate on rising prices of tokens and their hopes were

fueled by success stories of cryptocurrency millionaires, marketing campaigns, and mobilized celebrities – as described by the interviewee:

Motivation for buying it [tokens from ICOs] a lot of the time is pure speculative purposes. People buy it because they believe this technology either has hypes surrounding it or that it could get a large volume of users in the future and so it will raise in price. (ICO advisor 2, 2018)

He illustrated the hype as follows:

People have heard a lot of stories [...] For every person like me [who missed out on large fortunes] there is another person who made millions investing [...] so a lot of people now is really starting to kind of enter the public consciousness of [...] “I can make big money of ICOs”. Celebrities like Floyd Mayweather and Paris Hilton are endorsing them. So a lot of people [...] don’t either have the knowledge or the time to go learn about the underlying technology, read white papers and understand them, [...] they just [...] buy into the hype. (ICO advisor 2, 2018)

The second ICO advisor observed: “You can [...] take credit of people which means marketing plays a huge role, and we’re seeing that a lot of ICO’s fundraise have had huge marketing campaigns” (ICO advisor 1, 2018).

At the same time, this mobilization caused problems for uninformed investors. Investors invested in little understood ideas and people. However – as the two interviewees described – the majority of ICOs did not produce functioning products and thus would not be able to generate the expected value:

What actually happens at the moment is, you have a white paper, you put together a good team of people, you get some ICOs celebrities on board, a lot of people invest, and then nothing really happens. You’re supposed to develop your technology but, I think [...] 59% of ICOs from last year either haven’t produced or failed to produce the product they’ve said they would. (ICO advisor 1, 2018)

The crowd a lot of the time aren’t anywhere near as discerning and I think, some people that invest in ICOs would have an understanding over the technology and they would say “right, this is quite revolutionary”, but a lot of people wouldn’t really have a notion, you know? [...] we’ve looked at some and they’ve been actually rubbish and they’ve raised tens of millions. (ICO advisor 2, 2018)

ICO advisor 2 concluded: “It’s a pity because, some of the technology is amazing and potentially really revolutionary” (ICO advisor 2, 2018).

This in turn let actors come to the conclusion that regulatory bodies were required to intervene so that investors could be protected from fraud and information deficits. These opinions were also translated by some of my interviewees: Investors who had become advisors for startups to launch ICOs, a business community member, an Ethereum team member, and a blockchain reporter. All of these actors described how ICOs attracted increasing investments; most claimed that investor protection regulation had to be applied to

ICOs in order to prevent fraud, even though regulatory interventions contrasted the initial underlying idea of transactions without third-party interventions. One of the two ICO advisors I interviewed hinted at missing consumer protection, expected losses, and regulatory restrictions: “I think, because [...] at the moment there is no consumer protection in place and a lot of average Joes are gonna lose a lot of money, the whole mechanism could be kinda restricted” (ICO advisor 2, 2018).

The interviewed blockchain reporter observed that there were startups launching ICOs that did not consider investors’ expectations concerning profit, a situation where regulation should intervene:

People are investing because they think they are gonna make money back, they are not just giving it out of charity, you know, so there is a real failure with a lot of startups to sort of recognize that they have an ethical responsibility – in my opinion – to have some kind of level of return. And this is what the regulations are gonna try to enforce, [...] you have to be really clear that if you are an ICO it’s a donation, you know, or it’s not, [...] otherwise people are like “maybe I’ll buy this token and it will be up 10% until next week” (Blockchain reporter, 2018).

In an interview, one Ethereum team member referred explicitly to the U.S., where he observed regulatory interventions in the form of consumer protection and taxation:

In the U.S. the main regulatory thing is, you know, if you are being a scam – like there is these ICO scams where they ripped off people and they, you know, act like traditional pyramid or Ponzi schemes, and so the regulatory body wants to protect consumers from that and at the same time they want to make sure that the money is taxed correctly (Ethereum team member 2, 2018).

Another ICO advisor explained that from his point of view, current law schemes mainly apply to ICOs and that it was only a matter of time until they would be put into practice:

I think regulation is completely necessary [...] People at the moment they talk about how it’s an unregulated space, and I don’t really think that’s the case. I think law by large tries to be technologically neutral, they try to go for like a principle-based approach, so they don’t say “right, this new technology has come out let’s create a law that will apply to ICOs”, they will look at new technology and see like the underlying principles, what’s actually going on, and how that fits within the existing regulatory landscape. So the biggest thing you’ll notice is people talking a lot about, “this is a utility token”, “this is a security”. All that means is a security is something that can be traded on the capital markets, [...] and the only reason people try to avoid that is because there are a lot of laws regarding the process that you have to go through if you want to offer a security to the public, and that’s because it is a consumer protection point of view [...] But the thing is people are spending a vast amount of money on this before they actually have the token. So of course they are actually expecting a rise of value, so a lot of them are actually securities. (ICO advisor 2, 2018)

The other ICO advisor concluded “pretty much all of them” (ICO advisor 1, 2018) and the second ICO advisor concluded:

So I think that [...] within the next year or two the regulator they are gonna start to come down really, really hard on people, and I don't necessarily think there will be new laws coming in but I just think they will start to apply existing laws really harshly and I think people will actually start going to jail. (ICO advisor 2, 2018)

A member of the business community explicated that translation had modified the anti-institutional idea of cryptocurrencies and that regulatory bodies should flank ICOs:

I don't want to get into the financials of things but I think one thing that needs to be regulated is, once I bid into an ICO and I get KYC [Know-Your-Customer] [...], what is the legal bond between us [the receivers of the ICO and me] at that point? What stops you from running away with the money? (Blockchain manager at consulting company, 2018a)

The blockchain manager added:

I think governments are here to stay, although there are thinkers that think that those type of technology [...] may limit the need of governments, because a government is there to protect you, to give you trust in the institution, so if you can decentralize the trust, then there are things that the government won't be needed anymore [...] but that is extreme, in reality things will still work together. So, I think regulation and protection for the citizens, it is something that probably should happen. I think, it would be a good thing, in my opinion. (Blockchain manager at consulting company, 2018a)

In opposition to the described mobilization of investors through ICOs, the DApp development project CryptoKitties refrained from doing an ICO to fund the project. Among the team were “over a dozen startup founders, crypto-enthusiasts, and award-winning developers” (CryptoKitties, n.d.b). They agreed with the Ethereum community and the Ethereum team that ICOs could harm trust in the Ethereum platform and blockchain technology in general. Therefore, CryptoKitties was deliberately not funded through an ICO (CryptoKitties, n.d.a, p. 7). “ICOs are a powerful funding tool, but abuses with the model and a lack of practical use cases are sowing mistrust in the technology they're supposed to empower” (CryptoKitties, n.d.a, p. 4). Their product was the game CryptoKitties, which was built as a DApp. Users of the game could collect, breed, and trade virtual kittens, which were encoded as tokens on the Ethereum mainnet. Transactions were made in Ether and the actions of the game were executed as smart contracts on the Ethereum mainnet (CryptoKitties, n.d.a, p. 6). On the other hand, the game also had data and software elements, which were centrally maintained off the Ethereum network. The blockchain reporter who had observed Ethereum-based DApps criticized such off-chain operations. Employing central user databases, web-interfaces, and proprietary code instead of open source code fundamentally contradicted Ethereum's interestment:

My problem with DApps is I don't think any of them are actually DApps, or maybe I'm sort of a DApp purist or something [...] I can't think of a single DApp, which is like a Decentralized

Application [...] CryptoKitties as a start-up, it's got a central server database of like all people who use it, you know, it's got a web interface, which is totally centralized, all of these other things, it's got proprietary software, like how the kitties are produced, for example, it's not open source (Blockchain reporter, 2018).

The CryptoKitties initiators observed that enrolment concerned mostly investors and community members with knowledge on blockchain technology. The purpose of the game – which they described in a white paper – was thus to mobilize consumers with blockchain technology:

Existing blockchain projects typically limit their audiences to early investors or a relatively small group of people with highly specialized knowledge or interests. Even then, most of these projects are either concepts or works in progress: their practical product remains nebulous. (CryptoKitties, n.d.a, p. 4)

According to the CryptoKitties white paper, large scale adoption of blockchain technology was hampered by a lack of education and understanding for non-financial applications:

By normalizing the practical application of smart contracts and cryptocurrency transactions, we will empower everyday consumers with a basic fluency in distributed ledger technology. Likewise, by showcasing a practical use for blockchain technology outside of the financial industry, we hope to broaden the public's understanding of the technology and its potential application. (CryptoKitties, n.d.a, p. 2)

Indeed, by the end of 2017, right after its launch, the Ethereum-based game temporarily mobilized a considerable amount of users and Ether. One month after its introduction, *The New York Times* reported: “Since CryptoKitties was introduced a month ago, 180,000 people have signed up. They've spent about \$20 million in ether, and more than 10 kitties have sold for over \$100,000” (Bowles, 2017). Interestingly enough, this mobilization shed light on Ethereum's emerging state of development – the high amount of transactions temporarily slowed down the Ethereum mainnet (Bowles, 2017) and all transactions had to go through the time consuming proof-of-work consensus mechanism.

The three examples of mobilization as well as the previously described enrolment (5.3.1) present a phenomenon implicit to the notion of translation. As translation is a coming-together of actors that mutually influence each other (3.2.1), Ethereum's mobilized actor-network deviates in some aspects from the intentions expressed in problematization and interessement. The Ethereum platform's convergence to other actors, such as previously existing business organizations, investment practices, and gaming lead to changes in the platform's initial concepts. Permissioned vs permissionless and public vs private characteristics as well as the degree of decentralization of DApps and involvement of new actors such as regulation became subject to negotiation. The Enterprise Ethereum Alliance, ICOs, and the

CryptoKitties game exemplified how the Ethereum platform, supported by the Ethereum team and community, mobilized the business community, investors, and new potential actors: The regulators and the private users. Callon (1986b) argues that “intermediaries which result in a sole and ultimate spokesman can be described as the progressive mobilization of actors” (p. 216). While in the case of the Ethereum Enterprise Alliance a private and permissioned platform became spokesmen of the business community, the public and permissionless Ethereum mainnet spoke for investors and private user gaming. During my observation period, both versions of Ethereum were connected through Vitalik Buterin and members of the Ethereum community. Time will tell whether they will split into two actor-networks or remain connected.

5.4.2 Trust

To open a mobilized black box implies investigating how it became an actor in which others have confidence, even if this confidence is temporary. With confidence I refer to the category of routine and Möllering’s (2006a) definition of system trust or trust in institutions: “Confidence in the institution’s reliable functioning, [...] based mainly on trust in visible controls or representative performances rather than on the internal workings of the institution as a whole” (p. 74). As mentioned before, the case of Ethereum has not opened a black box in retrospect, as in some of the studies reviewed in chapter 3.2.2. However, even though the presented case has observed Ethereum in the making, the described mobilizations indicate a collective confidence in the Ethereum actor-network. ICO participants, the investors, and issuers relied for some time on the functioning of the Ethereum mainnet to carry out transactions and represent value. For some investors, this was not a matter of understanding the Ethereum platform or the project in which they invested. Instead, what Giddens (1990) calls access points – in this case marketing campaigns and celebrities – motivated these actors to entrust their money to ICOs. Here, I implicitly follow Möllering (2006a), who broadens Giddens’ (1990) notion of human access points to representative performances in general. Moreover, the stories of successful investments in cryptocurrencies – a more process-based (Zucker, 1986) phenomenon – fueled the trust of new investors. Within short time, it became a practice that even scammers confided in and used. Disappointed expectations about positive visions for the future, along with purposeful frauds, lead to a consent within the actor-network that control (Luhmann, 1979) in the form of regulatory customer protection was not visible. Public transactional data of ICOs was apparently not perceived as a control mechanism.

CryptoKitties is another example that shows how users and the providers of the game trusted in the reliable functioning of the Ethereum platform. While the providers had a solid technical understanding of Ethereum, the internal workings of the platform were less relevant for users. They were introduced to smart contracts and Ether as elements of gaming, a practice which they were probably already familiar with. The fact that the platform initially had difficulties coping with CryptoKitties' transaction load showed, however, that it was not yet reliable.

Lastly, the formation of the Enterprise Ethereum Alliance shows how enrolment of the business community and Ethereum community as well as the trust building that came along with this enrolment (5.3.2), led to commitment to further mobilize the Ethereum platform. An initial press release refers to Ethereum as a trusted platform. The firms quoted there referred to several years of experiences with the platform, its team, and the community. These actors concluded that the actor-network should be mobilized. In order to do so, they founded the alliance, which was thought to structure the process of developing a private and permissioned enterprise version of Ethereum. If it worked out, it would become an acknowledged institution, providing rules (3.1.2) for the development and use of Ethereum by enterprises. Unfortunately, at the time of this writing, I cannot tell if this will be the case.

This leads me to the last point on aspects of trust in Ethereum's mobilization. Möllering (2006a) emphasizes the necessity of uncertainty to talk of trust. Trust means acting "as if [social vulnerability and uncertainty] were favourably resolved" (Möllering, 2006a, p. 111). The different ways of mobilizing the Ethereum actor-network display such trust, as they show how actors preliminarily relied on the platform despite its evident technical immaturity.

Overall, I have observed various ontologies of trust along the translation of Ethereum. Trust crises have appeared as problems, trust has been used as an interessement device, trust has appeared as an input to enrolment and trust building has been used to connect several actors in Ethereum's actor-network. On the other hand, trust has also failed and been missed throughout Ethereum's translation. In the following chapter, I analyze and explore the ontologies of trust in the translation of Hyperledger Fabric – a case of blockchain with different technological characteristics, which came from a more incorporative background.

6 Hyperledger Fabric

In this chapter, I delineate the translation of a less radical, but more incorporative blockchain platform, namely Hyperledger Fabric. The case renders visible ontologies of trust which at first glance appear similar to the Ethereum case. However, the platform and the actors involved are different, as is the foundation of trust crises and interestment devices, existing trust relations, trust building processes and the mobilized network.

6.1 Problematization: Different trust problems

6.1.1 Translation

Hyperledger Fabric was a blockchain software whose initial code base was programmed over the course of 2015 and 2016 by the multinational firm IBM as well as a smaller financial services IT company called Digital Asset Holding (Cuomo, 2015b). IBM was a provider of IT software, services, and hardware for business customers in search of new and promising business fields. As a *The New York Times* article on IBM's blockchain activities described, "IBM's eagerness to find new businesses to make up for the erosion of its traditional hardware, software and services offerings" (Popper & Lohr, 2017a). The development of Hyperledger Fabric from 2015 onwards on followed previous experiments with other blockchain systems over the course of 2014 and 2015. A former IBM employee recalled working on a white paper that was later translated into the Hyperledger Fabric code: "As architect of the IBM Blockchain group, I wrote the first white paper for IBM's open Blockchain, which was later contributed to the Linux Foundation's Hyperledger" (Diedrich, 2016, p. 337). This employee had also been part of IBM's ADEPT team, which investigated blockchain technology for the Internet of Things (IoT); he also served as IBM's contact person with the Ethereum team (Diedrich, 2016, i). So IBM's blockchain investigations resulted in a report on blockchain and the IoT (Brody & Pureswaran, 2014), IoT test networks that incorporated Ethereum's code base ("Blue Horizon," n.d.a; Higgins, 2015), and IBM's turn toward permissioned and private blockchain technology.

The first report, *Device democracy: Saving the future of the Internet of Things*, authored by the IBM Institute for Business Value, emphasized the economic potential of connected consumer devices in the Internet of Things. One of the problems presented in the report was that internet users could not trust established actors, such as governments or corporations, to manage or protect the data of their IoT devices:

The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT solutions built as centralized systems with trusted partners is

now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data. (Brody & Pureswaran, 2014, p. 4)

On the other hand, this report stated that one could not simply eliminate central authorities from the Internet of Things, as it assumed IoT devices to have the potential to harm one another. Blockchain technology in general was proposed as an obligatory passage point (Callon, 1986b) to solve these problems: “The IoT represents a case of billions of players, not all of which can be trusted – some even malicious – with a need for some form of validation and consensus. And for this, the “blockchain” offers a very elegant solution” (Brody & Pureswaran, 2014, p. 7). This could, according to the report, lead to an “Internet of Decentralized, Autonomous Things” where users would define smart contracts that would govern the relations of IoT devices, and where devices would act according to prescribed rules (Brody & Pureswaran, 2014, p. 8). The similarities of this initial problematization and OPP in IBM’s publication and Ethereum’s problematization are not surprising when one considers the proximity of the Ethereum network and the IBM report. In the report, the authors acknowledged feedback from Vitalik Buterin and another Ethereum team member (Brody & Pureswaran, 2014, p. 15). Subsequent test networks were built with Ethereum code and presented at DEVCON1 by IBM’s Ethereum contact person (Ethereum, 2015b).

From this and other experiments, IBM concluded that blockchain was a promising technology, but that existing actor-networks with public and permissionless blockchain technology could not fully mobilize enterprises – IBM’s customers (Cuomo, 2015a). In blog posts that announced the development of Hyperledger Fabric, IBM representatives praised blockchain technology: “Blockchain is big” (Cuomo, 2015b) and “blockchain is a technology for a new generation of transactional applications” (Hamm, 2015). In another blog post, it was stated that “IBM’s interests are in the application of blockchain to permissioned, business to business networks” (Palfreyman, 2016a). Together with the Linux Foundation and “a community of likeminded organizations” (Cuomo, 2015a), they founded the Hyperledger project⁵⁹ to further translate their idea of blockchain technology as an open source software. IBM and Digital Asset Holding programmed the initial Hyperledger Fabric code and donated it to the Linux Foundation (Cuomo, 2015b). Among the project’s 20 founding members⁶⁰ under the Linux Foundation’s roof were several “centralized authorities” (Brody

⁵⁹ The name was Open Ledger Project before it got renamed into Hyperledger project.

⁶⁰ Accenture, ANZ Bank, Cisco, CLS, Credits, Deutsche Börse, Digital Asset Holdings (DAH), DTCC, Fujitsu, IC3, IBM, Intel, J.P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group (MUFG), R3, State Street, SWIFT, VMware and Wells Fargo.

& Pureswaran, 2014, p. 4) such as information technology firms and banks – the same authorities which had been objects of criticism in IBM’s first problematization in the *Device democracy: Saving the future of the Internet of Things* report. Untrusted authorities were not Hyperledger’s pressing problem, however. The former problematization was replaced with new problems to which Hyperledger Fabric presented the solution - the new obligatory passage point (Callon, 1986b). Among these problems was a reference to trust.

Business relations between organizations were said to often lack trust. Actors compensated for this lack with control and trust facilitating mechanisms. These were, in turn, often time consuming and costly, as organizations did not share information – again due to a lack of mutual trust. An IBM report described this vaguely: “In business, trust is incredibly hard to engineer and impossible to guarantee. Until now, we’ve relied on instruments and institutions to be surrogates for our trust” (Brill et al., 2016, p. 16). A blog post by an IBM representative put the problem in a nutshell: “Unfortunately, lack of trust is a major issue in business that prevents transactions from being settled in a timely manner” (Lowry, 2017d). This general problem was translated to multiple industries, for example financial services or supply chains in trade and production. International money transfers used to take long time due to the involvement of several financial institutions who did not trust one another and spent time reconciling each other’s information. This was also described in an IBM blog post:

It takes several days for your international payments to clear [...] because cross-border payments involve multiple intermediaries, include significant costs and are subject to local banking standards. These intermediaries have trouble trusting each other and any discrepancies or errors can cause major delays. (Lowry, 2017a)

The logistics industry was also said to face problems keeping track of their assets as they moved from actor to actor but with little willingness to share information among each other. This particular problem was described in an IBM blog post during its announcement of a partnership with the global shipping company Maersk:

Supply chains have excelled at gathering [...] data to improve efficiencies in trade. However, increases in data have not been paired with an increase in trust. Data is kept within an organization, unable to benefit partners across a supply chain.

There are some significant challenges that plague current supply chain practices:

Organizations are wary of threats from competitors, choosing to protect data instead of sharing with partners.

Blind spots persist across the supply chain as organizations lose track of products and paperwork. (Lieber, 2017)

Related problem descriptions also surfaced in an interview with a manager from an information technology company, which built blockchain networks with Hyperledger Fabric. To illustrate the prevailing control mechanisms for ensuring that shipping containers were handled as requested, this manager explained how a client shipping company employed people to observe the movement of containers in ports:

This is a company which employs 150 people. Every day they pay them a full salary to do nothing else besides sit around in the harbor and observe with binoculars whether certain ships have been unloaded or not because this is information, which they need and do not get in any way, digitally or in analogue [...] Well, these really are digital medieval times. (Blockchain manager 2 at information technology company, 2018)

The problem of a lacking trust due to non-transparent supply chains was also visible in perceived counterfeiting risks. Such risks were topical for several industries over the years, as summarized in an IBM blog post:

Counterfeiting is a global problem that affects a wide range of industries such as luxury goods, clothing, food products, pharmaceuticals and more. Proving or disproving the authenticity and quality of an asset can be a challenge because traditional supply chains are long, complex and lack transparency. (Mauri, 2017)

The problem of transaction partners not trusting each other sufficiently to share information, and their subsequent effort of mutual control, was eventually addressed by blockchain technology – an obligatory passage point. In another IBM blog post, it was said that “blockchain can break down these barriers [in international trade] by increasing trust, accountability and transparency, enabling untrusted parties to work together” (Yumang, 2017b). According to IBM, this was made possible by blockchains’ technical architecture, as the firm described in its blog:

Blockchain is a digital technology for recording and verifying transactions. It has demonstrated the ability to radically reduce the time it takes to settle a multi-party transaction, while at the same time being resistant to tampering. Blockchain technology, and the new business processes written on it, will certainly transform industries, reimagining stagnant approaches to supply chain, trade settlement or any applications where value is exchanged. (Cuomo, 2015b)

In an interview, published on the Hyperledger blog, with a blockchain developer from another information technology company that also applied and contributed to the development of Hyperledger Fabric, the developer agreed:

My view is that blockchain solves one extremely general problem: suppose you want to have a database or computing environment that needs to be distributed among multiple users who don’t fully trust one another. How can you build this efficiently? The answer is blockchain. While this general problem may seem narrow at first glance, it turns out that it encompasses a huge amount of potential use cases and applications, ranging from finance to supply chain to IoT and more. (Hyperledger, 2017c)

This problematization implicitly introduced different kinds of organizations, all of whom shared a common interest in conducting transactions on blockchain networks. These organizations were potential blockchain network participants. They included enterprises from supply chains to financial services, mobility services, healthcare, as well as public sector and governmental organizations. They had in common the trust problem described above. Moreover, these companies were promised to benefit financially from organizing processes and delivering services through blockchain (Cuomo, 2015b). Further, foremost banks and other financial institutions had a delay in processing value digitally, and were threatened by Bitcoin's disintermediation of financial institutions. As interviewed managers from information technology and consulting companies, which applied Hyperledger Fabric for financial services firms observed:

I guess at the beginning they [banks] were of course all terrified by the topic of Bitcoin. That is something which is destructive. You can transfer money from A to B without a bank, even across national borders [...] And it is clear that banks often have this role of an intermediary and if there is this possibility now, to do the same without intermediaries, it is clearly threatening to them. And thus, it is a topic where they say: "This is actually strategically important. We need to access this." (Blockchain manager 1 at information technology company, 2017)

In the end, it is a digitization process, which is just starting because what banks have claimed still years ago to be decentralization or digitization was worth nothing. The management boards of banks may have referred to having computers as digitization, but the processes or the basic elements of the financial industry have not been digitized at all. It is only through blockchain that technology appears, which allows for the transfer of values and their administration, purely digital, without paper and without physical values, as a technology for securitization. And that is the real reason why banks got started already two, three years ago [2014, 2015] to look at the technology. (Blockchain manager at information technology and consulting company, 2017)

Thus, the potential blockchain network participants were perceived as having several interests in translating blockchain technology in their industries and adapting themselves. However, they were warned not to rely on existing blockchain technology. Some features of public and permissionless blockchains like Bitcoin and Ethereum, such as publicly available information about transactions between pseudonymous accounts recorded on blockchains, were problematized by IBM, as the following excerpt from a blog post shows:

As we study applications of Blockchain, it is becoming apparent that Blockchain does not have some of the characteristics required by business. For instance Blockchains are public networks,

even though member identities are protected under a private key, a user could “snoop” on the network and deduce transaction patterns of members. (Cuomo, 2015a)

Ethereum in particular had some problems that would disqualify it as a trustee and as a trust facilitator in business networks. Its publicly available data, in combination with anonymous accounts, were described as making the Ethereum platform unusable for business customers.

In interviews with two blockchain managers from an IT company that built Hyperledger Fabric-based blockchain networks for corporate clients and contributed to the Hyperledger Fabric code, several problems with regard to the Ethereum actor-network were illustrated. One of them started laughing when imagining an insurance company as a blockchain network participant, logging anonymously into a potential blockchain network of insurance and re-insurance companies: “It is totally clear, they [insurance companies] do not log on anonymously to something and say: “I have a case of loss and who then somewhere in the anonymous network can just [interviewee not finishing the sentence, laughing]?” (Blockchain manager 1 at information technology company, 2017). Another manager from that information technology company problematized the publicly available data in combination with pseudonymous user accounts:

In today’s Ethereum network you can see all transactions, its entire history. They are still hashed, so you cannot see the content. Due to pseudonymity you don’t see who sent what. We did a test [...], it is relatively easy, with common open source analytics tools I can find out for you in an Ethereum network who does how much business volume with whom [...] And we must not have such effects in a business network and I just have to know who I am dealing with. (Blockchain manager 2 at information technology company, 2018)

Experiences with public administration as potential blockchain network participants showed that some were reluctant to accept Ethereum. In our interview, the blockchain manager quoted above described the case of a startup, which traced the provenance of diamonds. This startup’s initial Ethereum-based system had been rejected by a governmental entity because of technological characteristics, such as its public data structure:

Ethereum does not work with most administrative bodies. We’ve seen this with Everledger, Everledger is a company, which digitizes diamonds. It’s a well-known case. They started with Ethereum and were thrown out by the first African government agency because they said: “We do not accept it on this base, on this technological base with the way it is implemented with pseudonymity and many other things.” (Blockchain manager 2 at information technology company, 2018)

Both managers from this information technology company, which worked with Hyperledger Fabric, also criticized Ethereum for relying on miners – people who ran the system on potentially unsecure hardware and had influence on hard forks.

If I now take Ethereum and this one runs it [network node] somewhere in China, this one in India, this one takes a very secure infrastructure, very expensive, somewhere in a German cloud data center, then it's all rubbish. Because that's unnecessary. The chain is exactly as fast and secure as the slowest [node] in the network and as the least secure one in the network. (Blockchain manager 2 at information technology company, 2018)

It's a topic for enterprises or a group of companies choosing a network, to choose it [Ethereum] as a strategic platform and in the worst case you depend somehow on someone, who decides "ok I do a hard fork now and reset the thing to a state from, I don't know, one and a half years ago". Obviously, for an enterprise that's a no-go. (Blockchain manager 1 at information technology company, 2017)

Another point of critique on permissionless blockchains like Ethereum, explicated by IBM, was that they were not able to comply with several regulatory and legal requirements – for example, data protection regulation or financial regulation. In a blog post, an IBM manager stated that permissionless blockchains did not comply with data protection laws: "In a permissionless blockchain, where a pseudonymous node from across the world can join and participate in the validation process, satisfying these [data protection] regulatory requirements is not possible" (Cuomo, 2016). The manager from an information technology company quoted above recalled a regulatory incident related to Ethereum: A project that used Ether for payments, but where cryptocurrencies were not accepted as currencies by financial regulators. This meant that enterprises could potentially not use them and still conform to law.

They've implemented it on the base of Ethereum because they thought it was an elegant solution because it already had the Ether built-in [...] Apparently they didn't know [...] that cryptocurrencies are not classified as currencies. In a business environment this means it's not usable because legally it's not a purchase but bartering. So, if at the bakery they offer to exchange my roll, so to speak, against bitcoin, it is bartering. It's not a purchase. That's provisionally ok for me as a private person. It doesn't work in a business context. I am liable for VAT, etc. I can't do this [...] It's legally impossible. (Blockchain manager 2 at information technology company, 2018)

Moreover, the Ethereum team was perceived by the above mentioned blockchain manager as lacking business capabilities. This deficit had been translated into the Ethereum platform: "You can tell by looking at the basic implementation of Ethereum that Vitalik Buterin and his friends, who have founded the thing, have never worked at a company. They did not know about the requirements which exist." (Blockchain manager 2 at information technology company, 2018).

Another issue mentioned was that it "[attracted] hackers" (Blockchain manager 1 at information technology company, 2017). In this case, reference was made especially to The DAO incident (5.3.1). The latter had also raised doubts with regard to the reliability of

Ethereum because of the unexpected change of the platform based on team and community decisions during The DAO incident, as a blockchain manager explained to me:

Especially with Ethereum, one could observe several issues, when, I'd say, things had gotten way out of hand and then they somehow sort of reset the thing, forced a fork and the whole thing suddenly went into a different direction. (Blockchain manager 1 at information technology company, 2018)

Hyperledger Fabric was presented⁶¹ as a blockchain technology which did not cause such problems. Moreover, it was framed as suiting potential blockchain network participants in translating blockchain technology for their own purposes. First, it was a software that potential blockchain network participants could use to build their own blockchain networks (Cachin, 2016), often with the help of information technology and consulting companies. Within these networks, they could determine which entities to incorporate into transaction processing and ledger storage (Cachin, 2016). Thus, Hyperledger Fabric was designed as a software for permissioned blockchains (Cachin, 2016). Moreover, it was supposed to allow for various consensus mechanisms and did not depend on Bitcoin's and Ethereum's proof-of-work consensus (Androulaki et al., 2018, p. 4). As alternative consensus mechanisms did not rely on monetary incentives (Gaur, 2017b), Hyperledger Fabric had no built in cryptocurrency (Harrison, 2018) like Ethereum's Ether. However, it was able to create and transact tokens, which could represent assets or monetary values (Androulaki et al., 2018, pp. 10–11). Similar to Ethereum, Hyperledger Fabric also allowed for programming and executing smart contracts⁶² (The Linux Foundation, 2017). The transaction processing, consensus, validation, storage of data, and reading access could be restricted to certain entities (Androulaki et al., 2018; Cachin, 2016; Palfreyman, 2016b). The transaction ledger which was shared among permissioned blockchain network participants was composed of immutable data blocks (Androulaki et al., 2018, p. 9). With these characteristics, Hyperledger Fabric was intended for application in several industries, for example financial services, food, luxury goods, or trade logistics (Androulaki et al., 2018, p. 2). It was in the interest of IBM and other information technology and consulting firms, the Linux Foundation and the developer community (which I introduce below) to establish Hyperledger Fabric as a standard for programming blockchain networks (Hyperledger, 2017f).

⁶¹ Timing of Hyperledger Fabric releases: Over the course of 2016 and 2017 Hyperledger Fabric pre-versions were released after IBM had contributed its code base (Behlendorf, 2017b) to the Linux Foundation. The official production release of Hyperledger Fabric 1.0 took place in July 2017 (The Linux Foundation, 2017) and was followed by software updates (Hyperledger, 2018d).

⁶² Smart contracts were called chaincode in Hyperledger Fabric (Androulaki et al., 2018). In the following I continue to use the term smart contract, as do experts in the field, facilitating comparisons between Ethereum and Hyperledger Fabric.

Although presented as a reasonable solution to the trust problems described above, the technical platform of Hyperledger Fabric could neither develop its code, nor translate itself into a broadly accepted technology all on its own. The initial code base by IBM and Digital Asset Holding from 2015 was intended as a “starting point, not a destination” (Cuomo, 2015b). Other actors joined to support and translate it. These actors were the Linux Foundation – the official host of the Hyperledger project, the developer community, potential blockchain network participants as well as information technology and consulting firms, including IBM.

The Linux Foundation was an organization that described itself as being globally recognized for mobilizing open source software. In its press releases, it used to describe itself as such, mentioning the importance of its technical artefacts, knowledge, and encounters that supported the translation of open source projects.

The Linux Foundation is the organization of choice for the world’s top developers and companies to build ecosystems that accelerate open technology development and commercial adoption. Together with the worldwide open source community, it is solving the hardest technology problems by creating the largest shared technology investment in history [...] The Linux Foundation today provides tools, training and events to scale any open source project (The Linux Foundation, 2015).

It was in the interest of the Linux Foundation to mobilize blockchain technologies for businesses, as it did with other technologies before, as open source software governed in the interest of multiple actors and accessible for everyone. The Linux Foundation’s executive director echoed this in the first press release on the Hyperledger⁶³ project: ““As with any early-stage, highly-complex technology that demonstrates the ability to change the way we live our lives and conduct business, blockchain demands a cross-industry, open source collaboration to advance the technology for all”” (The Linux Foundation, 2015). To enforce this translation, the Linux Foundation hired Brian Behlendorf as executive director of the Hyperledger project. In an interview, one blockchain manager called him a “[pioneer] on the internet” (Blockchain manager at information technology and consulting company, 2017) while Behlendorf called himself a “veteran of free and open software projects” (Behlendorf, 2017a). In the interest of the technology and the Linux Foundation, his role was “to help bridge the companies who wanted to incorporate blockchain in their products and the developers” (del Castillo, 2016). This Behlendorf quote stems from the blockchain specialist online press, *Coindesk*. This bridge meant to assemble, with the Linux Foundation, a developer community for Hyperledger Fabric. The assemblage should establish Hyperledger

⁶³ In the press release the Hyperledger project was still referred to as Open Ledger Project.

Fabric as the software used by potential blockchain network participants as well as by information technology and consulting firms. The principle aim was to develop Hyperledger Fabric according to the requests from these actors.

The developer community of Hyperledger Fabric sought to organize and deploy the technical development of the software. The developer community was constituted by the maintainers, the contributors, and a set of technical artifacts that exchanged code and related information. According to the Hyperledger project definition by Behlendorf, the Hyperledger Fabric developer community required:

1. An identified set of software developer “maintainers” who are responsible for the development process, culture, and general technical direction of the project, and engaging the public [...]
2. A bounded set of artifacts, including one or more Git repositories, a bug tracking/issue database, a wiki, a set of mailing lists, and other developer resources [...] tied together as part of the same particular project, and which the maintainers directly and the broader community indirectly are responsible for keeping updated and active. (Behlendorf, 2016)

Moreover, contributors were encouraged to submit requirements and proposals, to report bugs and to propose change requests, and to engage in discussions as well as to take on tasks like fixing bugs and implementing changes (Hyperledger, n.d.a). As an actor, the developer community held knowledge about Hyperledger Fabric and had the ability to make technical changes. As IBM had written large parts of the initial Hyperledger Fabric code, its developer community had “nearly no diversity of contributors” (Behlendorf, 2017b) at the beginning, but consisted mainly of IBM developers (Hyperledger, n.d.c). The intent was, however, to translate Hyperledger Fabric into an actor supported by a more diverse developer community (Hyperledger, 2017j).

Information technology and consulting firms were interested in establishing themselves as blockchain experts and promoting the technology for generating business with clients. For IBM Hyperledger Fabric was the dominant foundational platform on which they based their adjacent IBM Blockchain product and other services (Gupta, 2017, pp. 34–36). It was their OPP. For other information technology and consulting firms, Hyperledger Fabric was an additional blockchain technology that served clients in developing blockchain use cases and building permissioned blockchain networks. It was an alternative OPP to Ethereum (5.1.1). In interviews, two managers from different information technology and consulting firms explained that they were open towards various blockchain technologies when Hyperledger Fabric appeared. Hyperledger Fabric was not the only OPP, as managers considered other blockchain platforms too:

We have used, with regard to smart contracts, [...] Ethereum and Fabric by Hyperledger [...] This is because there is no real choice, yet. Many new solutions are coming up and I guess we will not have to restrict ourselves to these two solutions in the future and Fabric by Hyperledger came to market after Ethereum. (Blockchain manager at information technology and consulting company, 2017)

“The Ethereum smart contract capabilities were really interesting to us [...] and after that we moved to Hyperledger [Fabric] which doesn’t mean that we are [only] coding on Hyperledger now, we are coding on multiple platforms” (Blockchain manager at consulting company, 2018a).

For potential blockchain network participants that did not trust public blockchains (especially Ethereum) to run their business processes, Hyperledger Fabric was an obligatory passage point. Potential blockchain network participants included different kinds of organizations ranging from large enterprises, to startups, governmental entities, auditors, and other professional organizations – all of whom wanted to apply blockchain technology. It was in these actors’ interests to solve for both of the trust problems mentioned above: The lack of trust among business partners and issues with permissionless blockchains.

Many of the potential blockchain network participants were already mobilized in other actor-networks – for example, in regulatory arrangements that influenced their actions. It was not in the interest of these actors to circumvent or destabilize these regulations, but rather continue complying with them. In a Hyperledger blog post, a member of the developer community was quoted on his experience with different blockchain technologies regarding regulation:

“[...] Even though we have worked with Bitcoin’s blockchain and Ethereum since the early days, enterprises are very different. Different industries have different regulatory requirements and business needs [...]” – [...] Founder of HACERA, Hyperledger Fabric maintainer and a co-release manager of Hyperledger Fabric 1.0 (Hyperledger, 2017f)

Among these regulations were for example data protection as well as financial regulations whose influence was described in the following quotes from the IBM and Hyperledger blogs and websites:

Let’s start with regulatory compliance, and the data protection principles that have been put in place by a number of acts and directives. As examples, consider the Gramm-Leach-Bliley Act in the U.S. financial sector, the Health Insurance Portability and Accountability Act (HIPAA) for the U.S. healthcare industry, and the European Union’s Data Protection Directive. What each of these examples illustrates is that companies are often required by governmental or regulatory authorities to know who processes their data, and to constrain where this processing takes place. (Cuomo, 2016)

The regulation of financial transactions influenced the identification of participants in financial transactions: “In many use cases, the identity of the participants is a hard requirement, such as in the case of financial transactions where Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations must be followed” (Hyperledger, n.d.b).

Overall, Hyperledger Fabric’s problematization drew on the construction of two trust problems. One was a lack of trust between business partners. The other was the untrustworthiness of the Ethereum actor-network. The actors involved were the Linux Foundation, Hyperledger Fabric, the developer community, IBM and other information technology and consulting firms, potential blockchain network participants, and regulations. This problematization was preceded by a crisis of trust in established actors on the internet, such as governments or corporations. As described in IBM’s report *Device democracy: Saving the future of the Internet of Things* (Brody & Pureswaran, 2014), this crisis revolved around a lack of trust in these institutions’ ability to manage user data or to protect the data of IoT devices. The displacement of this first problem in the course of Hyperledger Fabric’s development suggests that the trust problem had to suit actors and their interests. It was not IBM’s and the Linux Foundations’ intention to destroy trust in established actors of the internet; moreover, Hyperledger Fabric’s characteristics did not suit this problem. The less aggressive problem of a lacking trust between business partners and shortcomings of the prior generation of blockchain technology appeared more suitable.

6.1.2 Trust

In the case of Hyperledger Fabric, problematization drew upon issues regarding trust. One problem was presented in the *Device democracy: Saving the future of the Internet of Things* report (Brody & Pureswaran, 2014) before IBM developed Hyperledger Fabric. The trust problem illustrated above was similar to the one discussed in the case of Ethereum (5.1.2). Any reliance of internet users on privacy protection by powerful organizations that maintained, governed, or transacted the internet was described as a phenomenon of the past. With reference to the NSA leaks by Edward Snowden – which revealed unauthorized data surveillance by US governmental institutions as well as information technology and telecommunications corporations (G. Greenwald, 2013; G. Greenwald, MacAskill, & Poitras, 2013) – internet users’ trust in “centralized authorities, whether governments, manufacturers or service providers” (Brody & Pureswaran, 2014, p. 4) was discarded. Thus, with its unreliable instead of “reliable functioning” (Möllering, 2006a, p. 74) system trust in the internet was ascribed with a trust crisis. On the other hand, in the field of IoT, devices could

not trust each other without these trust facilitating institutions, as some software-controlled devices could have malevolent agency and harm each other. Following Ethereum's reason-based narrative of trustless interactions (5.1), blockchain technology could replace the necessity for trust and organize the interactions of IoT devices in a way that they would not harm each other. Users would not have to trust established centralized institutions.

The second trust problem involved business partners who did not trust each other. This issue was partially contradictory to the first problem. Nevertheless, it turned into the dominant problematization for the translation of Hyperledger Fabric. Suffering from a different trust crisis, established organizations became the protagonists. Until the idea of blockchain technology surfaced, potential blockchain network participants already relied on each other for the processing of goods, money, and assets. However, they were said to not trust each other without additional routines for trust. This led to mutual control. For example, data was reconciled, the transportation of goods was surveilled, or interactions required institutional-based trust mechanisms such as certificates (Zucker, 1986) (3.1.2). The lack of trust between potential blockchain network participants was identified as a costly and time consuming problem, which hindered organizations from sharing more information with each other.

Problematizing public and permissionless blockchains could furthermore help convince actors that Hyperledger Fabric, more than any other blockchain technology, was the right solution to this problem. Negative statements about Ethereum drew on all three trust bases, illustrating why potential blockchain network participants could not endow it with trust. First, the technology did not show the ability (Mayer et al., 1995) or functionality (McKnight et al., 2011) to conduct transactions between organizations. Public and permissionless blockchain technology did not protect data and the mining infrastructure made service provision unreliable. The Ethereum team was also perceived as lacking the ability (Mayer et al., 1995) to sustain a blockchain network for enterprises. In addition, the Ethereum network and Ether did not fit with some regulatory rules (Möllering, 2006a) – something which hampered the acceptance by potential blockchain network participants. Lastly, unsuccessful reflexive trust building brought about by failed enrolments of Ethereum (for example the DAO scandal (5.3)) as well as rejections of the system by governmental authorities, served to damage Ethereum's reputation.

Overall, a trust crisis of public and permissionless blockchains – in the sense of damaged trust – and the absence of trust between business partners served as two central problems which framed blockchain technology as an OPP. The turn from the first to the second problem was supported by struggles in the enrolment of Ethereum's actor-network. This case also

shows how the trust problem and the identity of an OPP are interrelated. With its particular features for enterprises, Hyperledger Fabric was suggested as a solution to a trust problem that the public Ethereum network was not able to solve. During intersement, Hyperledger Fabric's identity and its relations to other actors were further elaborated.

6.2 Intersement: Other trusted actors

6.2.1 Translation

Hyperledger Fabric's translation used two trust narratives as intersement devices. One narrative explained how blockchains in general facilitated trust between multiple parties, especially between business partners. The second narrative dealt with Hyperledger Fabric and the data that Hyperledger-Fabric-based systems would produce as trustees. References to the notion of trustless interactions were rare and intertwined with statements about blockchains ultimately facilitating trust between business partners. This was emphasized in the following excerpt from IBM's book *Blockchain for dummies* (Gupta, 2017):

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with; it's that you don't need to when operating on a blockchain network.

Blockchain is particularly valuable at increasing the level of trust among network participants. (Gupta, 2017, p. 10)

A start-up software engineer who had worked with Ethereum and Hyperledger Fabric was quoted distinguishing Hyperledger Fabric from trustless blockchain platforms in a Hyperledger blog post: ““Hyperledger Fabric is strongly tailored to enterprise customers [...] Whilst public blockchains focus on ‘trustless’ networks, Hyperledger is specifically tailored to meet the needs of business customers [...]” [...] Software Engineer [...]” (Hyperledger, 2017f). This quote suggests that enterprises did not demand trustless blockchain technology.

According to the first trust narrative, blockchains would be able to facilitate trust between untrusted entities when these entities participated in blockchain networks. This was due to the consensus mechanism – regardless of which sort of consensus mechanism – and the immutability of transaction data distributed among blockchain network nodes. This narrative described potential interactions among blockchain network participants as “trusted transactions”⁶⁴ (Dudley, 2017a; IBM FinTech, 2017, 2:35) or “trusted exchange” (Dudley, 2017a; Gunther, 2018; IBM FinTech, 2017, 7:19). Potential relations between entities that operate on a joint blockchain network were described as mutually controlling and trusting. The emphasis was not on one-on-one relations between entities, but on the relational network.

⁶⁴ In the quoted blog post the quoted expressions were ascribed to a key note speech by IBM's CEO.

These relations were determined by the consensus and data immutability of blockchain systems. Thus, the operating mechanisms of blockchain systems staged Hyperledger Fabric as a trust facilitator or enhancer, and differentiated blockchains from other IT systems. An IT company blockchain manager who built blockchain networks with Hyperledger Fabric for business clients and formed part of the developer community explained this as follows in an interview:

I can enforce trust within a network on a technological base, so I can, in a way, guarantee trust within an untrustworthy network. This has two layers, two elements. The first element is consensus. Consensus means that I cannot just make any changes to data or processes, without the network validating it, deciding whether it's correct or not and only then it is written. And that's fundamentally different from any database known today. That does not exist there [...] So, I can't write data or change data independently, nobody can, nobody in the network. Full stop. Everyone else has a look at it. The second layer is the technological layer, the way blockchains are built and implemented, namely something like immutability [...] And this [...] is the ledger, is fully distributed, which means everyone within the network always holds exactly that. (Blockchain manager 2 at information technology company, 2018)

The manager added:

This is also the case with [Hyperledger] Fabric [...] once a block is written, once this transaction exists, I can't change it anymore. I can't get rid of it, I can't delete it, I can't manipulate it, I can't do anything with it. Well, and this enforces trust because everybody in the network knows, once I've written it I can't change it anymore. If I say this is the price for the service that I've delivered, then it is documented, everybody can see it. (Blockchain manager 2 at information technology company, 2018)

The quote indicated that a shared data set was ultimately attributed with creating trust between blockchain network participants. Due to the mutual control among blockchain network participants and the synchronized character of the shared ledger, blockchain was often referred to as “the single source of truth” for business networks. In several blog entries and in IBM's *Blockchain for dummies*, it was suggested that this single source of truth facilitated trust: “If a lack of trust is causing friction, blockchain's shared ledger can provide increased visibility into transaction and asset histories to improve trust” (Gupta, 2017, p. 38) and “by using a shared version of the truth on blockchain, trade partners can interact with greater trust” (Lang, 2017). This view was shared by members of the developer community. The Chief Marketing Officer of DAH, the startup which had contributed to the initial Hyperledger Fabric Code, stated in a video on Hyperledger that “blockchain will change our clients' business [financial services] by allowing them to neutralize data infrastructure so that they can all rely on the same, single source of truth” (Hyperledger, 2017e).

On the other hand, Hyperledger Fabric was not only supposed to facilitate trust between blockchain network participants. It also depended on trusting relationships between the blockchain network participants. This dependence was due to Hyperledger Fabric's consensus mechanisms, which hinged upon the assumption that "participants are known and trusted" (Gupta, 2017, p. 16). It did not rely on Bitcoin's and Ethereum's proof-of-work consensus mechanisms. A Hyperledger white paper argued that "the operating assumption for Hyperledger developers is that business blockchain networks will operate in an environment of partial trust. Given this, we are expressly not including standard proof-of-work consensus approaches with anonymous miners" (Hyperledger, 2017g, p. 4). The Hyperledger Fabric documentation outlined that Hyperledger Fabric's consensus mechanisms relied on the participation of permissioned members only. Moreover, the choice of a consensus mechanism for a permissioned network depended on the other types of trust building mechanisms in place between blockchain network participants:

The Fabric platform is also **permissioned [bold in original]**, meaning that, unlike with a [...] permissionless network, the participants are known to each other, rather than anonymous and therefore *fully* [italics in original] untrusted. This means that while the participants may not *fully* trust one another (they may, for example, be competitors in the same industry), a network can be operated under a governance model that is built off of what trust *does* [italics in original] exist between participants, such as a legal agreement or framework for handling disputes. (Hyperledger, n.d.b)

Moreover, permissions were based on digital identifications. By restricting the participation in the consensus mechanism to certain digital identities, Hyperledger Fabric could rely on consensus mechanisms, which did not assume the malicious behavior of nodes. This distinguished it from trustless blockchains, which relied on proof-of-work, as the following excerpt from the Hyperledger Fabric documentation describes:

Permissioned [bold in original] blockchains [...] operate a blockchain amongst a set of known, identified and often vetted participants operating under a governance model that yields a certain degree of trust. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which may not fully trust each other. By relying on the identities of the participants, a permissioned blockchain can use more traditional [...] consensus protocols that do not require costly mining [proof-of-work]. (Hyperledger, n.d.b)

Thus, the interestment device described trust among blockchain network participants as both an output of and a precondition for blockchain technology. Hyperledger Fabric was said to facilitate trust, as it created data shared among participants as a single source of truth. The technology was able to create such data through consensus mechanisms and the immutability of data. However, according to the narrative described above, consensus mechanisms considered for Hyperledger Fabric required a certain degree of (pre-existing) trust among the

blockchain network participants. Thus, trust was assumed to be based on permissions, which were assured through digital identities as well as adjacent trust building mechanisms, like legal arrangements. The interessement device described the roles and relations of potential blockchain network participants and of Hyperledger Fabric, connecting them with a trust narrative. At the same time, it also distanced Hyperledger Fabric from other actors (Callon, 1986b, pp. 207–209). Immutability and consensus as trust facilitating characteristics distinguished blockchain technology, including Hyperledger Fabric, from other IT technologies. The permissioned access distinguished Hyperledger-Fabric-based networks as trust facilitators from permissionless blockchain networks like Ethereum.

The second narrative proposed answers to the rhetorical question: “Who will you trust with your trust network?” (Hyperledger, 2018c, p. 45) – a question which was spelled out in a Hyperledger presentation document that argued how and why actors would trust Hyperledger Fabric. This presentation depicted Hyperledger Fabric and its data as trustees; it also drew in other actors that would help potential blockchain network participants, information technology and consulting firms, and the developer community trust Hyperledger Fabric and its respective data. In a video-taped interview at the IBM Interconnect 2017 fair, an IBM manager called blockchain “a trusted database” (SiliconANGLE theCUBE, 2017, 5:12). Blog posts referred to it as “blockchain’s trusted and shared system of record” (Haziot, 2018) or as “trusted data” (Kelley, 2018).

Overall, the Linux Foundation and the developer community aimed to establish Hyperledger Fabric as a standard for blockchain programming. This was echoed in a Hyperledger blogpost: “Hyperledger is an open source collaborative effort created to advance blockchain technology [...] for a cross-industry open standard” (Hyperledger, 2017f). A similar sentiments was expressed in interviews. One manager from an information and technology firm that contributed to the Hyperledger Fabric code stated:

We try to establish a certain [...] industry standard by [...] joining such a consortium [Hyperledger project] and then generating as much momentum as possible, so that [...] many and also powerful companies come together, so that we can say this [Hyperledger Fabric] is what the consortium finally acknowledges as a common standard. (Blockchain manager 1 at information technology company, 2018)

Asked about “where [they hoped] to see Hyperledger and/or blockchain in 5 years” (Hyperledger, 2018b), members of the developer community answered in an interview on the Hyperledger blog that Hyperledger would “[provide] a backbone for strong, private blockchains to various industries [...] An accepted standard similar to Linux” (Hyperledger, 2018b).

The joint development of Hyperledger Fabric as an open source code was expected to support this ambition. A participatory approach was viewed as a way to enabling a variety of actors to trust the software, including the developer community, other information technology and consulting firms, as well as potential blockchain network participants. In a white paper on Hyperledger, this was argued as follows:

Open source builds trust [bold in original]

Blockchain represents a perfect opportunity to benefit from open source, since the concept of trust is woven deeply into all blockchain technologies.

Blockchain systems are engineered to enable direct, peer-to-peer transactions between parties who don't fully trust one another, or don't trust any central authority to validate transactions or settle disputes. Therefore, it's essential for these parties to trust in blockchain technologies.

We believe that an open, collaborative approach that invites participation from all stakeholders is the most effective way to build trust for enterprises – enough trust for them to widely and rapidly adopt blockchain technologies. (Hyperledger, 2018g)

In addition to the open source approach, some of Hyperledger Fabric's technical characteristics, (some of which are described above) also served as arguments for why potential blockchain network participants would trust Hyperledger-Fabric-based networks as well as trust the data recorded within such networks. "Trusted business networks" (Gaur, 2017a) were thought possible thanks to the immutability of data produced by Hyperledger-Fabric-based blockchain systems. It was claimed that such data could prevent manipulations by blockchain network participants or external entities, such as hackers.

If I can prove [...] to the regulating authorities [...] that this is a dataset that is unforgeable, which is based on these procedures and which is in a way something that represents the truth for us as a business network and for you as a regulator. And if now, for example, the audit comes, he doesn't have to visit the company anymore [...] instead – at the touch of a button – [...] he just receives all relevant data. Thus they are interested and they are especially interested whether it is blockchain technology or a central database. Because with a central database, I don't think so. Because there is an administrator, who can independently manipulate or tamper data or they can be manipulated from outside. (Blockchain manager 2 at information technology company, 2018)

Additional arguments for why potential blockchain network participants would trust Hyperledger Fabric were centered around the decentralized transaction validation which was executed only by participants with prior permission and their shared control over the network. A manager from an IT and consulting firm who had designed and implemented Hyperledger-Fabric-based blockchain networks with network participants, explained this mechanism to me in an interview:

It [Hyperledger Fabric code used by the IT and consulting firm] is a standard blockchain code by Hyperledger. Everybody trusts this blockchain, this concept, this configuration. Everybody is an equal [...] player in the network. The network is decentralized, runs [...] not in a single data center, centrally somewhere, but everybody runs his own node and all together it results in a decentralized system, just not open to the public but for involved partners. (Blockchain manager at information technology and consulting company, 2017)

Moreover, IBM's book *Blockchain for dummies* (Gupta, 2017) argued that Hyperledger Fabric's ability to determine different data access rights for participants in blockchain networks would enhance their trust in the technology: "Privacy is maintained through cryptographic techniques and/or data partitioning techniques to give participants selective visibility into the ledger" (p. 11). These arguments were complemented with continuity as well as the flexibility of Hyperledger-Fabric-based networks. These attributes should ensure potential blockchain network participants that joint business processes and data would persist in the future, but also be adapted to changing circumstances. It was argued that continuity was based on the shared control among permissioned participants of networks mentioned above: "Because it's [the ledger] not owned or controlled by any single organization, the blockchain platform's continued existence isn't dependent on any individual entity" (Gupta, 2017, p. 11). Flexibility was explained as the result of smart contracts, which could be programmed within networks: "Because business rules and smart contracts (that execute based on one or more conditions) can be built into the platform, blockchain business networks can evolve as they mature to support end-to-end business processes and a wide range of activities" (Gupta, 2017, p. 11).

These arguments, which drew on the technical characteristics of Hyperledger Fabric, were complemented with additional trust producing and trusted entities. Regulation was one such entity. Hyperledger Fabric intended to comply with regulations of multiple industries. An IBM blog post argued that "the Hyperledger Fabric is built from the ground up [...], intended to be applied across many regulated industries and use cases" (Dudley, 2017a). Its permissioned and private attributes were primarily used as arguments in favor of Hyperledger Fabric's compliance with several regulations, such as data protection laws and financial regulations. An IBM blog post stated: "We argue that for most business purposes, permissioned blockchains are the only choice that can enable compliance with data protection regulations" (Cuomo, 2016). An industry-specific example for Hyperledger Fabric's compliance with data protection regulation can be found in IBM's blockchain concept for patient data handling in the healthcare sector:

Without violating regulatory requirements, it will be possible to collect, store, protect and share health data and enable its real-time use. The Health Insurance Portability and Accountability Act (HIPAA) limited the use of health data [...] With blockchain, a massive amount of records can be used (Sharma, 2017).

For the financial services industry, anti-money-laundering legislation and KYN guidelines that requested financial services providers to identify their customers, were connected to the permissioned and private characteristics of Hyperledger Fabric. A Hyperledger white paper referred to this as follows:

Compliance guidelines like “Anti-Money Laundering” and “Know Your Customer” require that banks and service providers can verify a customer’s legal identity and give them clearance to do transactions. These requirements drive the adoption of permissioned and private blockchains, since public blockchains can risk compromising a participant’s privacy and confidentiality. (Hyperledger, 2018g, p. 13)

Another regulatory requirement for financial services was certified IT hardware. One information technology firm claimed that it ran Hyperledger-Fabric-based blockchain networks according to standards that met the demand of potential blockchain network participants from the financial services industry. This was explained by a manager in an interview. Referring to an example from banking he explained that “banks have to certify their hardware layer for certain types of transactions” (Blockchain manager 2 at information technology company, 2018). He emphasized: “There is only one hardware in the world, which has this certificate and this is the one that [is used here]. In order to enable everyone in such a construct to comply with their regulations” (Blockchain manager 2 at information technology company, 2018).

Other trusted entities, which were drawn into the narrative as warrantors with experience and reputation were IBM, the Linux Foundation, its Open Governance Model, and the developer community. IBM often hinted at its long lasting experience in relevant fields of enterprise information technology, including former open source projects and recent collaborations with clients in the development of Hyperledger Fabric. The blog post announcing Hyperledger Fabric stated:

Why IBM: We have deep expertise in transaction processing, distributed computing, security, cryptography and a long history of bringing communities together and legitimizing open source. To make Blockchain ready for business we will bring our technology prowess as well as be the stewards for the open community around Blockchain similar to what we’ve done collaboratively with the Openstack, CloudFoundry and Node.js foundations. (Cuomo, 2015a)

In an interview at IBM Interconnect 2017, one IBM manager emphasized that the first version of Hyperledger Fabric was developed based on IBM’s experience with different industries:

The Hyperledger version one that was announced earlier this week, [...] is dramatically different from the underlying blockchain and bitcoin in other platforms [...] Because it's really built primarily based on the requirements that we have gathered by working with hundreds of clients, right, in financial services, in supply chain, in public sector, etc. (SiliconANGLE theCUBE, 2017, 2:29)

Thus, other information technology and consulting firms and potential blockchain network participants were invited to trust Hyperledger-Fabric-based on various aspects of IBM's experience: Its history with necessary technologies and open source projects as well as interaction which it had with clients during the development of Hyperledger Fabric. The reputation of Digital Asset Holding, a member of the developer community, was also drawn in: "DAH brings a great deal of credibility in the financial applications space. It's great to have them on board" (Cuomo, 2015b). With regard to the Linux Foundation, experience and reputation with the governance of open source software played a role in the trust narrative surrounding Hyperledger Fabric. The Linux Foundation had a reputation for developing open source software, as the following quote in an IBM blog post illustrates: "I cannot say enough good things about the Linux Foundation. When it comes to open governance, the LF [Linux Foundation] is the gold standard. They are both credible and efficient" (Cuomo, 2015b).

The Linux Foundation's Open Governance model was translated to the Hyperledger project in order to organize the Hyperledger projects, including the development of Hyperledger Fabric within the developer community. The long established Linux Foundation Governance model was said to enhance trust of the developer community in the software development project, and ultimately the software itself. This was argued with reference to the transparent decision-making process, the acknowledgement of high quality contributions by the community, the independence from specific firms, and the assurance of the process within the Linux Foundation over many years. A blog post on the Hyperledger website stated that "the model has worked for the Linux Foundation for 15+ years and therefore has been purposefully passed down to each open source project" (Hyperledger, 2017i). A Hyperledger white paper explicitly related the Open Governance Model to developers' trust in the software:

Open governance means that technical decisions—such as which features to add, how to add them, and when to add them—are made by a group of community-elected developers drawn from a pool of active participants. Anyone can participate in Hyperledger by becoming a contributor and/or maintainer.

Becoming a developer or maintainer translates into one thing: trust. You know how decisions will be made and how people will be selected to make these decisions. Hyperledger is vendor-neutral and technical contributions are based on meritocracy. (Hyperledger, 2018g, p. 7)⁶⁵

With its tight relation to the Linux Foundation, the Hyperledger project aimed to build similar trust in the Hyperledger brands, including Hyperledger Fabric, as Brian Behlendorf stated in a Hyperledger blog post:

The most valuable role the Hyperledger Project can play is to serve as a trusted source of innovative, quality-driven open source software development community, creating modular, open source components and platforms [...] Hyperledger will forge a brand that will be seen widely to reflect the accepted default “safe” deployment platform for enterprise teams, and be seen as a great home for active collaboration around new technologies, only then our mission will be accomplished. (Behlendorf, 2016)

Similar to the first trust narrative, the second one also suggested relations between several actors, thus serving as an intersement device in the translation of Hyperledger Fabric. It described Hyperledger Fabric and the data that it produced as trustees. Potential blockchain network participants were described as trustors once again. Moreover, the developer community was related to the technology as a trustor, as were information technology and consulting firms. All three sought to acknowledge Hyperledger Fabric as a standard software. The way to achieve this was through collaboration during the translation of Hyperledger Fabric in the open source project. Moreover, Hyperledger Fabric’s characteristics, such as data immutability, permissioned access, shared control, flexibility, and continuity were viewed as enhancing potential blockchain network participants’ trust in the software and in the data. Lastly, the trust narrative connected (presumably) trusted and established actors to Hyperledger Fabric, including regulators, the Linux Foundation, its Open Governance Model, IBM, a certified IT infrastructure, and recognized members of the developer community.

6.2.2 Trust

The first narrative intertwined the characteristics of blockchain technology with trust among potential blockchain network participants. Blockchain technology was described as their trust facilitator. At first sight, blockchain’s role as a trust facilitator calls for a perspective which views the technology from a routine and institutional perspective (Möllering, 2006a). Blockchain technology’s and specifically Hyperledger Fabric’s consensus and data immutability can be theorized as algorithmic rules. These rules were expected to facilitate the exchange of assets, data, or values between several parties. Participants in the blockchain

⁶⁵ This document adopted descriptions of the Open Governance Model and trust from the earlier blog post (Hyperledger, 2017h).

network were expected to share expectations in the form of institutionalized rules, although they did not necessarily trust each other otherwise. These rules were not societal or legal norms, as in the integrative trust framework, but were algorithmic rules. The data produced within these blockchain networks – referred to as a “single source of truth” – can be interpreted as actors with the institutional role of an available and reliable transaction data source. This was thought possible although such a role was not yet stabilized.

On the other hand, the narrative spoke of blockchain technology as a trust enforcer. This seems to be a paradox from an organizational theory perspective, where trust is conceptualized as a voluntary action (Möllering, 2006a, p. 119). This “enforced trust” implied control mechanisms, which should ensure that blockchain network participants would not manipulate transaction data and stick to their agreements. The consensus-based validation of transactions and the immutability of data were described as mechanisms of mutual control. Such control mechanisms should prevent blockchain network participants’ opportunistic behavior. In theory, the characteristics of blockchain, consensus, and immutability should reduce uncertainties regarding the behavior of blockchain network participants and thus produce trust in a rationalist sense. Hence, the narrative described trust according to a reason-based (Möllering, 2006a) understanding – something which emerged out of mutual control mechanisms enforced by blockchain technology.

Moreover, as a pre-requisite for constituting blockchain networks, this narrative drew in “partial trust” among blockchain network participants. Its consensus mechanisms were not intended to secure the network from every possible malicious behavior carried out by network nodes. Partial trust was supposed to be based on two elements: First, the trust relation that existed between potential blockchain network participants, and second, the computational identification of legitimate participants to permissioned Hyperledger-Fabric-based networks. The first basis refers to institutional-based trust (Zucker, 1986) according to which the exemplary legal agreements can serve as a reference for engendering trust among organizations acting as blockchain network participants. Similarly, rules (Möllering, 2006a) established as programmed governance models with blockchain networks could serve as an institutional basis for trust among participants. The second element, identification, follows a reason-based (Möllering, 2006a) argument. It considers “known, identified and often vetted participants” as actors, whose integrity has been assured and who are aligned with a “common goal”. These arguments are similar to those of rationalist trustworthiness indicators and principle-agent theory (3.1.2). Thus, the “partial” trust based on information about the identity of other entities in the network was based primarily on reason and routine. It did not rely on

mutual openness, but on a minimum amount of mutual information and institutional securities. Rather than a leap of faith (Möllering, 2006a), this fits with an understanding of “partial trust” and “trusted and known parties” according to computer sciences’ understanding of trust as an absence of vulnerability (van der Werff et al., 2018, p. 400). Overall, the narrative described trust based on reason and routine as both a pre-requisite for and a result of Hyperledger-Fabric-based blockchain networks.

The second narrative, which suggested trust in Hyperledger Fabric and its data, drew on Möllering’s (2006a) notions of reason, routine, and reflexivity. It was expressed in the Linux Foundation and the developer community’s aspiration to mobilize Hyperledger Fabric as an established software standard among all actors. Their goal was to translate Hyperledger Fabric into a trusted system (Giddens, 1990; Luhmann, 1979). However, the narrative also acknowledged that this was not yet the case, and offered further routine-based arguments for why several actors could trust Hyperledger Fabric. It suggested that potential blockchain network participants could trust the data produced because of the “procedures” that led to the immutability of data. Instead of reviewing procedures at another blockchain network participant’s premise, auditors could trust the data and the algorithmic rules within a blockchain network. Shared expectations among blockchain network participants regarding how data was produced should lead to trust. Moreover, power and control over the rules and devices, which were executing them, were supposed to be shared and not hidden in an inaccessible data center. In addition, Hyperledger Fabric’s characteristics, such as data privacy settings, continuity, and flexibility promoted the software’s ability (Mayer et al., 1995) or functionality (McKnight et al., 2011) for coping with the requirements of organizations that considered participating in blockchain networks. These were rational arguments for the trustworthiness of the software. Other actors played a role in the trust narrative as well. Regulatory provisions – interpreted here as sets of rules – were related to Hyperledger Fabric as a way to align expectations and thus facilitate trust. This message was directed towards potential blockchain network participants, who were already subject to regulatory requirements and whose trust in the software could be enhanced by coupling it with regulation. In turn, IBM, renowned members of the developer community, the Linux Foundation, and its Open Governance Model were associated with Hyperledger Fabric. In the narrative, these actors’ reputation in enterprise software development was emphasized. In this way, the narrative subtly called on reflexivity-based trust among potential blockchain network participants, information technology, consulting firms, and potential members of the developer community. The relation, for example of the reputable Linux Foundation to

Hyperledger Fabric, paved the way for a reputation spill-over (Stewart, 2003) to Hyperledger Fabric. Moreover, the narrative suggested that actors could build trust in Hyperledger Fabric throughout its enrolment as an open source software development process. The following sub-chapter sheds light on how interessement was turned into enrolment and explores which trust mechanisms influenced this process.

6.3 Enrolment: Building trust in Hyperledger Fabric

6.3.1 Translation

At the core of Hyperledger Fabric's enrolment was the software proposed during interessement, which was meant to be enrolled in a network of trustors. "Interessement achieves enrolment if it is successful" (Callon, 1986b, p. 211). Thus during enrolment one can often observe arguments, showdowns, and "multilateral negotiations" (Callon, 1986b, p. 211). Hyperledger Fabric was a potential trustee for IBM, other information technology and consulting firms, the developer community, and potential blockchain network participants. However, throughout the studied time-period, IBM recognized that the software for permissioned blockchain networks – Hyperledger Fabric – still had some "vulnerabilities" (Shaw, 2017) to potential security attacks. Its initial code base was programmed by IBM in 2015 and further developed by the developer community, which launched the official production version Hyperledger Fabric 1.0 in mid-2017 (Cuomo, 2015b; Hyperledger, 2017f).

However, the first actor that trusted Hyperledger Fabric, even before it became a software, was IBM. From 2015 on, IBM's management decided to turn their belief into action and to invest in the translation of blockchain technology, despite technological and social uncertainties. IBM's former Ethereum contact person recalled this in his book. He initially had to convince critics within the firm about the potential of blockchain technology. This turned into euphoria within the firm:

For a short while I was one of the lone standard bearers – Yoda and I – of IBM's fledgeling IoT-blockchain research, ADEPT. We got heavy internal flak. I kept getting the word out and a little later it could not be enough blockchain for IBM IoT. (Diedrich, 2016, p. 337)

Other internal research and development teams also presented blockchain projects to IBM's management. An article in *The New York Times* reconstructed how IBM's director of research and the IBM CEO were enrolled with the idea of blockchain technology via the problematization and interessement brought forth by employees. The director of research was quoted: "“That was the ‘aha’ for me” [...] [he] said. “This was not really about digital payments, but establishing trust in transactions in general.” He called it “a technology that can

change the world.”” (Popper & Lohr, 2017b). Once internally enrolled, IBM built the initial code base of Hyperledger Fabric and donated it to the Linux Foundation. In a blog post, an IBM manager stated that:

IBM is all-in with this open approach to blockchain, and is contributing tens of thousands of lines of code written over the past 6 months by IBM Researchers and Developers across Research Triangle Park, North Carolina, Almaden, California, Zurich, Switzerland, as well as our labs in Bangalore and Delhi. (Cuomo, 2015b)

In 2017, IBM’s blockchain activities and investments were still described as “[big] bets” (T. Greenwald, 2017; Popper & Lohr, 2017b) in various newspaper articles. The translation of Hyperledger Fabric remained uncertain and IBM did not earn profits from it, but expected to do so in the future.

IBM enrolled the Linux Foundation in the translation of Hyperledger-Fabric-based on IBM’s positive experience with “selling or building business [from Linux software]” (Blockchain manager at information technology and consulting company, 2017) as well as the Linux Foundation’s reputation for successful open source software development (6.2.1). In a blog post, IBM described this commitment with the foundation as “throwing our weight behind the Linux Foundation’s open ledger project [Hyperledger project]” (Hamm, 2015). When joining the Hyperledger project, new employees of the Linux Foundation confirmed in a blog post that they were attracted to the Open Governance Model and the foundation’s reputation: “I was attracted to the Hyperledger project because of its solid community leadership and the integrity of the Linux Foundation” (Hyperledger, 2017d). Together, IBM and the Linux Foundation pursued the enrolment of other actors into a network that could mobilize Hyperledger Fabric⁶⁶.

With its Hyperledger director, Brian Behlendorf, IBM, and the Linux Foundation enrolled Hyperledger Fabric, the developer community, other information technology and consulting firms, and potential blockchain network participants. A manager from an information technology and consulting firm who built blockchain networks with Ethereum and Hyperledger Fabric described the active role of the Linux Foundation and IBM. In an interview, he differentiated the evolving network from the Ethereum network:

So, these two worlds [Ethereum and Hyperledger] develop in parallel. Both open source, but with, [...] different communities at the moment. The Linux Foundation is doing a lot in terms of community building, but it’s a different community, it’s an industrial community. At the meetups one often sees the consultants and, well these classic, well IBM guys. (Blockchain manager at information technology and consulting company, 2017)

⁶⁶ And the other Hyperledger projects.

Later in our conversation he specified Brian Behlendorf's role: "It [Hyperledger community] is actually an open source community [...] [Brian Behlendorf] is in charge of building this construct and well, obviously uses all channels of the Linux Foundation to build the community" (Blockchain manager at information technology and consulting company, 2017). The quotes also hinted at meetups, which – similar to Ethereum – enrolled the developer community, information technology and consulting firms, and potential blockchain network participants. A Hyperledger blog post about a meetup mentioned that "Hyperledger Meetup groups make up a key part of the Hyperledger ecosystem. Participation in a Hyperledger Meetup group is open to anyone – employees of a Hyperledger member company, Hyperledger contributors and developers, and people just passionate about blockchain technology" (Sridharan, 2017). The manager quoted above described how he had hosted several Hyperledger meetups in Germany and that apart from consultants, developers and potential blockchain network participants also attended to learn about the technology:

There are meetups that help him [Brian Behlendorf]. I've already hosted three or four meetups for Hyperledger. Well, developers go there. Also people from the industry go there because they have heard about it and maybe want to understand it better. (Blockchain manager at information technology and consulting company, 2017)

Thus, the meetups seemed to create a welcoming environment where technical information about Hyperledger Fabric (Hyperledger, 2017a), experiences from implementation projects (Hyperledger, 2017b; Shugol & Stamou Fotini, 2017; Sridharan, 2017), and problems and interest narratives (Kiran, 2017a, 2017b) could be shared among various actors. At the beginning of 2017, the Linux Foundation counted "38 different meetup groups all around the world" (Hyperledger, 2017a); a year later there were "over 100 Hyperledger meetup groups around the world" (Hyperledger, 2018f).

The intention of enrolling actors through knowledge about Hyperledger Fabric led Brian Behlendorf and IBM representatives to talk about Hyperledger Fabric at panel discussions, presentations, booths at financial services and payment fairs (Dudley, 2016; Haynes, 2017; Wallis, 2017; Winman, 2016) (0), and blockchain conferences (Dudley, 2017b; Ferris, 2017b; Gargolinski, 2017; Lowry, 2017b; Richer, 2017b; Wedgwood, 2017), as well as on webcasts (Ghaneei, 2016; Lowry, 2017c; Yumang, 2017a). They also used blogs, websites, and books – some of which some were reviewed for this analysis – to explain the technology and present stories of successful enrolments in order to enroll additional blockchain network participants in new projects. Hackathons (Brakeville, 2017a, 2017b; Ferris, 2017a; Harrison, 2017; Rampen, 2016) and developer conferences (Dudley, 2017b; Richer, 2017a; Stowell, 2018)

were especially important for enrolling software developers as members of the developer community, information technology and consulting firms, and potential blockchain network participants. The underlying assumption was that developers opted for the software they were familiar with. As one manager of an information technology firm who participated in such events described: “Today developers indeed may not take decisions but influence decisions, for example through their selection and they take what they know and what they do not know they simply tend not to take” (Blockchain manager 1 at information technology company, 2018). In an IBM blog post, the announcement of a developer conference explicitly related the aspect of confidence in technology to the event:

How confident are you that [blockchain network development] will be a good investment of time and money? [...] gaining confidence is an area where it’s easy to get help.

[...] Come learn, network, talk technology, or ask our technical experts for help. (Stowell, 2018)

At these events, developers came into direct contact with the Hyperledger Fabric system, allowing them to try it and talk about it with knowledgeable people.

Moreover, at these venues and in dedicated meetings, established information technology and consulting firms, and potential blockchain network participants were directly approached by IBM’s blockchain representatives. Blockchain managers from different information technology and consulting firms recounted this experience. One stated in an interview that “[Hyperledger Fabric] develops through a push by IBM and the Linux Foundation to the large enterprises” (Blockchain manager at information technology and consulting company, 2017). Another recalled how he was approached by IBM and that the brand made him accept Hyperledger Fabric rather quickly:

It was them approaching us, from IBM directly saying this is our product. And I brought them in because it [Hyperledger Fabric] says “this is branded by IBM”, then I started studying it [...] I saw that there was demand of that and then we trained our team. It was IBM approaching us (Blockchain manager at consulting company, 2018b).

A representative of an information technology and consulting firm that used Hyperledger Fabric to program blockchain networks also mentioned the technical architecture of the first releases as being “very neat” (Blockchain manager at information technology and consulting company, 2017). This led to the impression that they could continue using it in the future to serve their enterprise clients and that the software would mobilize more actors. In a Hyperledger blog post, a CTO of an information technology and consulting firm delivered the following quote:

“[...] As an early adopter of Hyperledger Fabric, we witnessed the open-source/open-governance software development from the early days of version 0.6 to the recent version 1.0 release candidate. We are impressed by the completeness and sophistication of the architecture and believe it will be the fundamental platform for large scale blockchain deployment in the enterprise.” – [...] Co-founder and CTO at BlocLedge (Hyperledger, 2017f)

The software’s translation among several actors and the early experimenting was enabled by its accessibility to everybody on the internet. In an interview, a manager of an information technology and consulting firm described that “everything is open source. The code is on GitHub [an openly accessible code repository], one can reconstruct everything very well, who has committed and one can download, start and test everything. Yes, typical open source project” (Blockchain manager at information technology and consulting company, 2017). After “over a year of public collaboration, testing, and validation in the form of POCs and pilots” (Hyperledger, 2017f) among 159 developers, Hyperledger Fabric 1.0 was released in 2017. Members of the developer community were quoted with positive experiences with the Linux Foundation and its Open Governance Model, with IBM, and the other members of the developer community. The activities seemed to have enrolled the developer community as well as suggest trust in the future performance and mobilization of Hyperledger Fabric. On the Hyperledger blog, the CIO of a developer community was quoted as follows:

“[...] We are very pleased with our collaboration with IBM and the tremendous progress over the past year in developing Hyperledger Fabric to meet the requirements of the wider financial industry. The high standards, attention to quality and rigor with which this open source project has been governed gives us the confidence in Hyperledger Fabric as a DLT platform for large-scale enterprise use cases.” – [...] Chief Information Officer, CLS (Hyperledger, 2017f).

IBM and other firms that contributed to the Hyperledger Fabric code-based products and services on the platform, thus making themselves dependent on Hyperledger Fabric and the developer community that sustained it. These decisions were said to be grounded in the collaborative experience within the developer community and with the Hyperledger Fabric platform. The CIO quoted above announced that: “Hyperledger Fabric is a foundational component of CLSNet – a service we are developing for bilateral payment netting of FX trades” (Hyperledger, 2017f). Another member of the developer community was quoted on joint learning:

“[...] It was a privilege to manage a release built by 28 companies who allocated over 150 engineers; we have learned so much from each other. This has motivated us, at HACERA, to build [...] a framework allowing participants and organizations to seamlessly secure and protect sensitive data and information on blockchains [...]” – [...] Founder of HACERA, Hyperledger Fabric maintainer and a co-release manager of Hyperledger Fabric 1.0 (Hyperledger, 2017f)

Another development community member was quoted comparing their experiences with Hyperledger Fabric against Ethereum. Hyperledger Fabric was perceived as better for building permissioned blockchains for enterprise customers, something which mirrors the interessement narrative.

“After building solutions on both Ethereum and Hyperledger Fabric 1.0, we found Fabric to be the superior platform for enterprise-grade blockchain applications. Since Hyperledger Fabric was designed to meet key requirements for permissioned blockchains with transaction privacy and configurable policies, we’ve been able to build solutions quickly and flexibly [...]”

– [...] CTO, IT People Corporation (Hyperledger, 2017f).

The enrolment of the developer community, in turn, gave other information technology and consulting firms the confidence to use the Hyperledger Fabric platform to serve their needs. In a case study by the Linux Foundation, the CTO of a startup that built blockchain platforms was quoted on this aspect: ““With the community behind it, we gained the confidence that Hyperledger Fabric would have longevity, would evolve quickly, and would meet more of our requirements [...] So that’s what brought us to Hyperledger.”” (Hyperledger, 2018a).

The Linux Foundation re-told these commitments in order to build the developer community’s reputation and to bolster the image of Linux’s governance of the projects: “Companies deploying blockchain internally, and those building products and services based on Hyperledger projects, tell us they trust Hyperledger because our technologies are built in the open by a broad community” (Hyperledger, 2018g, p. 7).

The enrolment of another type of actor, namely potential blockchain network participants, was supposedly built on their positive attitude towards blockchain technology. In a blog post, an IBM consultant who worked with Hyperledger Fabric and Ethereum blockchains described how potential blockchain network participants, as clients of IBM, expected blockchain technology to be of such future importance that they were eager to experiment and accept its early flaws:

Luckily there is a huge amount of goodwill in the world of business blockchain. The use-cases are so diverse and the potential for disruption so large that businesses are willing to overlook the immaturity of the technology as they explore the opportunities in their industry. (Lucas, 2016)

Several trust aspects from interessement resonated with the blockchain network participants and enrolled them. A manager of an information technology and consulting firm observed that blockchain network participants trusted Hyperledger Fabric because the technology was directly linked to the IBM brand. In an interview he said: “It is like the saying that no CTO in the world has ever been fired for buying IBM. If in doubt one picks an expensive and well-known supplier and hopes that they solve the problem” (Blockchain

manager at information technology and consulting company, 2017). Moreover, the narrative that Hyperledger Fabric – in contrast to Ethereum – was tailored to enterprises resonated with potential blockchain network participants. So much so that they actively reached out to consulting firms for blockchain projects and asked for a software that they barely knew. A consulting company manager recalled in an interview that “clients are really asking for Hyperledger because it has that enterprise flavor that Ethereum doesn’t give them” (Blockchain manager at consulting company, 2018a). He furthermore explained:

They [clients of consulting firm] tend to trust, they tend to trust more large enterprises sort of platforms, so they are all into the Corda [another blockchain platform] space and they even don’t know what that is, then when they go deep in their research they realize “ok that’s not for us”. But then they, everybody, they’re really, really asking for Hyperledger [Fabric]. (Blockchain manager at consulting company, 2018b)

As the above quote indicates, technological knowledge was a secondary aspect for some potential blockchain network participants when enrolling with Hyperledger Fabric. Besides the brand and Hyperledger Fabric’s image as a blockchain for enterprises, potential blockchain network participants enrolled with Hyperledger Fabric because of the enrolment of other blockchain network participants:

Hyperledger [Fabric] is also open source, but who looks at, who of the users has the skills to analyze the source cod. Well, one simply trusts the other users. The others use it, thus there must be something to it. (Blockchain manager at information technology and consulting company, 2017)

Information technology and consulting firms worked with potential blockchain network participants on blockchain projects. They often conducted workshops with their clients and jointly determined arenas for experimenting with Hyperledger Fabric; they then built exemplary networks, the so called proofs of concept, and small scale products which could be used by blockchain network participants (Deloitte Ireland, n.d.; IBM, n.d.; Oregui & Kumar, 2017; Palfreyman, 2016a). In a Hyperledger blog post, representatives of an information technology firm stated that interactions with potential blockchain network participants accustomed them to the technology: “Run design thinking workshops and ideation engagements to collaborate, innovate, and experiment to find the right solution. This helps familiarize the key stakeholders with the enabling technologies” (Oregui & Kumar, 2017). In such interactions the suggested trust facilitating effects of Hyperledger Fabric were also negotiated and complemented. Although blockchain network participants seemed to confirm the enterprise-flavor of Hyperledger Fabric and requested its permissioned and private characteristics, they complemented new Hyperledger-Fabric-based networks and transactions

with established rules and roles. A manager from an information technology company explained that when his clients processed transactions through Hyperledger-Fabric-based networks, they accompanied these processes with regular contracts: “Today we still live in a parallel universe. Everything that [...] happens on chain needs to be legally covered according to old custom” (Blockchain manager 2 at information technology company, 2018). With reference to these two approaches, he added that “hopefully, there will be [...] a consistent standard one day, so that you say I now accept both and their legal relevance is equal. We do not have that today” (Blockchain manager 2 at information technology company, 2018).

Moreover, to transfer values in the new network, they did not rely on new cryptocurrencies, but drew in a regulator approved digital currency. This was mentioned by the above quoted manager: “We take one [digital currency], which is like established at the exchange, which is accepted by the respective regulatory authorities” (Blockchain manager 2 at information technology company, 2018). Preferably enterprises relied on transfer mechanisms with established fiat money issued by traditional banks:

I told them [potential blockchain network participants] everything you will do here, you can do just with real money. The only thing we need is a banking partner. And then we drew [...] [the bank] in [...] So, and now we simply have an additional [...] account [...] I can now buy all kinds of value-added services and I do not use a cryptocurrency but I use real money. (Blockchain manager 2 at information technology company, 2018)

On the other hand, information technology firms found difficulties regarding trust when enrolling blockchain network participants. A manager from an information technology firm illustrated how a Hyperledger-Fabric-based network became enrolled through negotiation processes with potential blockchain network participants, contracts, and design considerations:

I think, objectively speaking, it is very difficult to set up such a network because many companies have to come together and secure contracts and consider how they somehow design a business process, which should run on such a ledger. And it is primarily nothing technical – no matter on which platform it is going to run later – but it is a complex negotiation process. (Blockchain manager 1 at information technology company, 2017)

IBM, for example, recommended its clients enroll in blockchain networks with actors that they already trusted first, and then gradually acquiesce to new ways of interacting with and through the platform: “You get going with Blockchain in small scenarios with business partners that you trust, sharing information that is not sensitive that allows you to get going with Blockchain technology, understand it and grow into more high value scenarios” (Ghaneei, 2016).

Moreover, uncertain regulatory implications surrounding Hyperledger Fabric and the data it produced interfered in the enrollment of blockchain network participants. A blockchain manager from a consulting company recalled that – although his firm experimented with clients and with the technology – some clients refrained from further mobilizing some of the networks due to regulatory uncertainties:

That's where [...] plenty of clients [have stopped]. So they have experimented only but they are now in a wait-and-see what the regulator is gonna do, so they're working on use cases where regulations won't apply [...] Yeah, we have worked on regulated industry; those won't go live [...] and it's a big topic. There is the financial services regulations, there is the GDPR [European data protection] regulation and many other things. (Blockchain manager at consulting company, 2018b).

According to Callon (1986b), “to describe enrolment is [...] to describe the group of multilateral negotiations, trials of strength and tricks that accompany the intersements and enable them to succeed” (p. 211) (3.2.1). In the case of Hyperledger Fabric, enrolment involved the coming together of Hyperledger Fabric, information technology and consulting firms, the Linux Foundation, the developer community, and potential blockchain network participants. In their interactions, these actors negotiated and modified the proposed trust relations. They did so by sometimes trusting the technology and each other or by entering in trust building processes with the technology and with each other. I will further elaborate on this process in the next sub-chapter.

6.3.2 Trust

The enrolment of Hyperledger Fabric entails reflexive trust building and leaps of faith by several actors. IBM's creation of the initial Hyperledger Fabric code base and their continuous efforts to enroll other actors was based on IBM's leap of faith toward the idea of a blockchain technology for business. Members of the firm believed that Bitcoin and Ethereum characteristics would “change the world”, and thus impact IBM and its clients' technical systems. The firm also believed that blockchain technology could be translated for and with enterprises. What journalists called IBM's “bet”, and what IBM described as “all-in”, signifies their enrolment with an uncertain technology. At the same time it highlights the firm's willingness to believe (Möllering, 2006a, pp. 119–121) in Hyperledger Fabric's future benefits for their clients and for IBM.

Information technology and consulting firms and potential blockchain network participants agreed with IBM's belief in the disruptive potential of blockchain technology as well as Hyperledger Fabric's “enterprise flavor”. A blockchain manager from a consulting firm expressed his and his clients' spontaneous trust in Hyperledger Fabric when Hyperledger

Fabric was new to them. These initial leaps and the willingness to use Hyperledger Fabric were based on IBM's brand and on the experiences of others. These were both process-based (Zucker, 1986), and thus reflexive (Möllering, 2006a) forms of trust, which led to trust spill-overs (Stewart, 2003). Such spill-overs occurred before actors had a clear purpose for the software and before they started gathering more knowledge. The "goodwill" toward the technology endured despite Hyperledger Fabric's technological immaturity. Leaps of faith (Möllering, 2006a) towards the Linux Foundation by IBM, and by people who joined the foundation as employees, were also conducive to enrolment. Their trust in the foundation was based on the Linux Foundation's good reputation and on former positive experiences in their collaboration, i.e. process-based (Zucker, 1986).

Other, more lasting reflexive trust building actions similar to Ethereum's enrollment, also enrolled the developer community, information technology and consulting firms, and potential blockchain network participants. In this case, the actors involved also familiarized (Luhmann, 1979; Möllering, 2006a) themselves with the technology through verbal, textual, and visual communication about the technology as well as through direct interactions with the technology. Moreover, these interactions helped the information technology and consulting firms, the developer community, and the blockchain network participants gather knowledge about Hyperledger Fabric and gain positive experiences with the technology. These two aspects of reflexive trust building (Möllering, 2006a) were intensified in Hyperledger-Fabric-based development projects, which firms conducted with early versions of the software. From these interactions, an information technology firm derived an opinion that Hyperledger Fabric was professionally designed, and that Hyperledger Fabric would become broadly used by enterprises. Their trust was expressed through their design of products and services that were dependent on Hyperledger Fabric. Aside from positive experiences with the software, reflexive trust building with other actors also played a role in enrolment. Another IT firm that contributed to the Hyperledger Fabric development emphasized the "collaboration with IBM" and their experiences with the Linux Foundation's Open Governance Model as bases for their trust in the future expansion of Hyperledger Fabric. "Successful interaction where trust is at stake" (Möllering, 2006a, p. 183) between business partners not only built mutual trust, but also enhanced trust in the technical actor. Moreover, the experienced usefulness of the Linux Foundations' governance rules was said to be recognized as a routine-based trust building mechanism toward Hyperledger Fabric. The IT firm expressed that it trusted the software, as it had been part of a process of shaping Hyperledger Fabric, and was convinced of the positive impact of IBM and the Linux Foundations' software development governance on Hyperledger

Fabric. The support of the enrolled developer community, in turn, gave an IT firm outside the development community “confidence” in the successful translation of Hyperledger Fabric. It decided to use Hyperledger Fabric to build a blockchain network because it had observed the efforts of the community and the subsequent development of the software. Thus, trust in Hyperledger Fabric was built in a reflexive and routine-based process with multiple actors. On the one hand, experiences with Hyperledger Fabric familiarized and built knowledge and subsequently created trust of IT firms. On the other hand, IT firms within and outside the developer community built trust in the software through their positive experiences with other actors that influenced the software.

With regard to the enrolment of potential blockchain network participants, reflexive trust building also played a role. Besides the above-mentioned leaps of faith based on brands and the observation of others, potential blockchain network participants also engaged in direct interactions with the Hyperledger Fabric system. They visited meetups, fairs, and conferences, received information from blogs and studies, and engaged with Hyperledger Fabric in blockchain workshops and projects. These occasions were intentionally created by the Linux Foundation and IT and consulting firms so they could familiarize themselves with the technology. In doing so, they involved the blockchain network participants in a reflexive trust building process (Möllering, 2006a). On the other hand, the reluctance to go live with blockchain networks (due to regulatory uncertainties) rendered visible a need for additional trust building mechanisms. The potential blockchain network participants and the consultancies that advised them felt that they could not mobilize networks if they were risking violation of regulation, i.e. a routine trust base (Möllering, 2006a). Uncertainties about the interference of existing trust building rules with the new technology hampered potential blockchain network participants from trusting the technology in business processes.

Lastly, Hyperledger Fabric’s role as a trust facilitator was tested by potential blockchain network participants. While the narrative under interestment proposed that Hyperledger-Fabric-based networks would facilitate trust between blockchain network participants, and that knowledge about partners’ identities was key for the network to facilitate trust, cautious enrolments rendered additional mechanisms visible. Although Hyperledger Fabric was permissioned and private, blockchain network participants were still wary of relying on the system to handle their data and determining their mutual relations. As a reaction to this, IBM recommended that potential blockchain network participants start establishing networks with business partners whom they already trusted. Thus, in order to enroll potential blockchain network participants in blockchain networks, Hyperledger Fabric depended on existing

relations among blockchain network participants. Moreover, the firm suggested entering in a gradual trust building process among partners and the technology, where the parties initially share non-sensitive information. This reflects very well Zand's (1972) spiral of trust, an element of reflexive trust building (Möllering, 2006a) where human actors gradually build mutual trust by sharing information and giving control. In this case, the spiral was expanded by a technical actor – the blockchain, which processed data and was itself a trustee. Moreover, blockchain network participants that started to enroll in blockchain networks accompanied Hyperledger-Fabric transactions with legal contracts between the parties. Thus, the established rule-based, trust building mechanisms accompanied new blockchain-based interactions during their enrolment. Similarly, actors with broadly accepted roles, such as money, officially approved digital money, and regular banks were drawn in to stabilize new blockchain networks.

In summary, Hyperledger Fabric's enrollment displayed an interactive and reflexive trust building process, which was supported by reflexivity-based trust spill-overs and routine-based trust mechanisms. In the following sub-chapter, I describe how this began to translate into a mobilized actor-network.

6.4 Mobilization: Preliminary reliance on Hyperledger Fabric

6.4.1 Translation

My observation of the Hyperledger Fabric network ended in April 2018. At that time, I saw the first signs of mobilization. At the same time, the four moments of translation were still happening in parallel. This becomes evident from the dates of the sources quoted in the respective sub-chapters (6.1.1, 6.2.1, 6.3.1, 6.4.1). Nevertheless, Hyperledger Fabric had already assembled a growing and relatively stable network of blockchain code, which was sustained and used by the developer community, the Linux Foundation, information technology and consulting firms, and actual blockchain network participants.

In April 2018, the Hyperledger Fabric release manager (who was at the same time a manager at IBM (Hyperledger, n.d.c)), published the third quarterly project update on Hyperledger Fabric (Hyperledger, 2018e). The report stated that the developer community was diversifying with blockchain developers from other information technology and consulting firms, potential blockchain network participants, and developers without company affiliation. These developers continued to change and improve the Hyperledger Fabric software, and the majority of proposed changes still came from IBM. According to the report, developers, for example from information technology and consulting firms and from potential

blockchain network participants, were mobilized. This was also noticeable in the questions they asked:

Fabric continues to grow and mature. In March, we published our version 1.1 release. We have a growing mix of contributors with IBM comprising only 36% of the contributors over the past quarter (-4%) though 80% of the commits [proposed code changes] since the start of 2018. There have been 96 developers (+9) representing 18 companies contributing 1087 commits and changing nearly 700k LOC [lines of code].

There seems to be a good mix of questions [...] The questions themselves continue to be increasingly sophisticated, which is also a good sign. (Hyperledger, 2018e)

Later in the text newly mobilized information technology and consulting firms and potential blockchain network participants were mentioned: “We have seen some new contributors over the past quarter from Accenture, BBVA, Oracle, Blocledger [information technology and consulting companies, bank] and some individual contributors” (Hyperledger, 2018e).

More and more blockchain network participants were mobilized with the actor-network. A blog post on the Hyperledger blog claimed that “the most renowned leaders in finance, healthcare and supply chain across the globe trust Hyperledger to build their business blockchain technologies” (Hyperledger, 2017k). A scientific paper on Hyperledger Fabric, written by IBM members, stated that Hyperledger Fabric was used in over 400 projects across various industries:

Fabric is used in more than 400 prototypes, proofs-of-concept, and in production distributed ledger systems, across different industries and use cases. These use cases include but are not limited to areas such as dispute resolution, trade logistics, FX netting, food safety, contract management, diamond provenance, rewards point management, low liquidity securities trading and settlement, identity management, and settlement through digital currency. (Androulaki et al., 2018, p. 2)

A *The Wall Street Journal* article illustrated how the Hyperledger Fabric network became part of food, logistics, and luxury good organizations by tracing an increasing numbers of goods:

Already, 1.1 million items sold or on sale at Walmart are on a blockchain – including chicken and almond milk – helping the company trace their journey from manufacturer to store shelf. Global shipping company Maersk uses the same technology from International Business Machines [IBM] to track shipping containers [...]

Everledger, a company started in April 2014 with the intention of creating a blockchain-based registry of every certified diamond in the world, already has 2.2 million diamonds in its registry. It's adding about 100,000 diamonds a month, says [...] [the] chief executive and founder. (Mims, 2018)

The case of “the first enterprise grade blockchain into production for everyday use by multiple financial services organizations” (Chenard, 2018) illustrated the mobilization of Hyperledger Fabric with an information technology and consulting company, blockchain network participants from the financial services industry, and their customers. A Hyperledger-Fabric-based system connected several local and foreign financial services organizations within a network, which aimed to provide receivables financing to Indian small and medium-sized enterprises (SMEs). Through the platform, SMEs received financing for trades against the security of the respective open invoices (Chenard, 2018). The main function of the system was to prevent fraud by the SMEs by reviewing the financing of SME’s invoices among the participating financial institutions. Such fraud could consist in SMEs attempting to secure several financings at different banks with the same invoice (Chenard, 2018). In a case study published by the Hyperledger project, the CTO of the information technology company described this functionality and explained the degree to which the financial institutions shared information with each other: “Every exchange [financial services organizations] can check whether any invoice has been financed elsewhere, without actually knowing anyone else’s business. It’s an efficient way to keep information private, while sharing at the same time” (Hyperledger, 2018a). Competing financial services organizations, which could not “provide any of their client information to a shared registry controlled by any one entity” (Chenard, 2018) were now connected as participants in the permissioned and private Hyperledger-Fabric-based network. The system, which none of them controlled alone, did not reveal secret information, but created new connections among the financial institutions that solved their trust problem. The CTO of the technology company generalized this characteristic of Hyperledger Fabric: “Hyperledger Fabric is a true blockchain and distributed ledger. When you require a global broadcast to share common information among multiple participants, Hyperledger Fabric is perfect” (Hyperledger, 2018a). However, the network’s reliance on Hyperledger Fabric was only temporarily stable. The case study described that the information technology firm enrolled with other blockchain technologies as well (Hyperledger, 2018a). According to its CTO, the involvement of Hyperledger Fabric depended on the platform’s technological advantages and its mobilization: “As long as Hyperledger Fabric is the leader – and we see it as the leader – we continue to contribute to it and use it” (Hyperledger, 2018a). In Callon’s (1986b) words, “this consensus and the alliances which it implies can be contested at any moment” (Callon, 1986b, pp. 218–219). The publicity on the enrolment and mobilization of blockchain network participants into an actor-network with Hyperledger Fabric, in turn mobilized additional information and

technology and consulting firms, and potential blockchain network participants into a broader, platform-agnostic blockchain movement. For example, *The Times* quoted the founder of a blockchain startup which offered a platform for tracing assets. According to him, the effects of Walmart's blockchain-related activities were apparent:

Mr Kelly says momentum has picked up since Walmart announced it would use IBM's blockchain technology to track its food. "Now I think there's a new blockchain company that appears every month for some sort of traceability or transparency or logistics," he says. (Moulds, 2018)

On the other hand, as of the beginning of 2018, I cannot say that blockchain, "had become an accepted part of the rhythm of everyday life" (Jeacle, 2017, p. 107). It was supposedly accepted by a growing developer community, by information technology and consulting companies, and by the Linux Foundation. In 2017, the Hyperledger project as a whole was Linux Foundation's fastest growing project in the foundation's history (Behlendorf, 2017c). At IBM in 2017, there were 650 people working on blockchain technology (Popper & Lohr, 2017b); blockchain was one of IBM's major strategic activities (T. Greenwald, 2018) and the firm's blockchain products and services relied on Hyperledger Fabric (Lowry, 2017c). However, blockchain network participants were only partially mobilized. According to *The Wall Street Journal*, Hyperledger-Fabric-based systems at Walmart and Maersk were mobilizing an increasing number of assets and organizations, but processed "still a fraction of the overall tracking that goes on at these companies" (Mims, 2018).

For several blockchain projects, the Linux Foundation and the Hyperledger brand attracted information technology and consulting firms, potential blockchain network participants, as well as an increasing number of developer community members. Hyperledger Fabric stood for permissioned and private blockchain networks on which blockchain network participants started to rely. IBM mobilized hundreds of customers and employees in blockchain projects. Blockchain network participants, such as the retailer Walmart, began to mobilize other firms to embrace blockchain-based tracking and tracing. To list several spokesmen is not the classic end of translation studies: Following Callon (1986b), mobilization results in a single spokesman who speaks for the actor-network. This might be an indication of the still incomplete mobilization of Hyperledger Fabric's actor-network.

6.4.2 Trust

Thus – as with Ethereum – this case study of Hyperledger Fabric has not opened a black box, but analyzed a network in the making. It was only at the end of my empirical analysis that it began to mobilize. Therefore, I cannot simply assert that a mobilized system – a black box –

is trusted and relied upon by a large crowd in the sense of system trust (Giddens, 1990; Luhmann, 1979; Möllering, 2006a). Nevertheless, mobilization showed two relational arrangements, which resulted from the translation of Hyperledger Fabric. One was a set of blockchain-enabled relations within new business blockchain networks. The other one was implicit routine-based trust in Hyperledger Fabric's entire actor-network.

What I call blockchain-enabled relations has been exemplified by the case of the Indian financial institutions, which started to jointly rely on a private and permissioned Hyperledger-Fabric-based network. They entrusted their sensitive data to the Hyperledger-Fabric-based blockchain. Moreover, they used the answers given by the system as foundations for granting of credit to SME clients who they implicitly assumed to be fraudulent. The ways in which such arrangements and resulting practices change the relation among blockchain network participants and relations among participants and third parties (e.g. customers) could not be investigated in this study. Such relations were just emerging, but remain an interesting topic for further research.

Reliance on Hyperledger Fabric's entire actor-network is the essence of mobilization. The actors that constituted the actor-network were relied upon by blockchain network participants. Organizations from the food, logistics and luxury goods industry, which had worked with IBM in blockchain projects, relied on Hyperledger-Fabric-based systems. The financial services organizations from India, which had worked with an information technology firm, entrusted their confidential information to algorithms. They expected that the network would keep them confidential and answer their requests with correct information. Their reliance incorporated not only the Hyperledger Fabric software itself, but all the other actors which sustained it. An information technology firm perceived Hyperledger Fabric as a "leader" as long as it was sustained by the other actors in the network. If the network of Linux Foundation, developer community, IBM, other information technology and consulting firms and blockchain network participants broke down, the trustee Hyperledger Fabric was no longer reliable. This network was drawn together by a translation, which incorporated trust and trust building mechanisms throughout problematization, interessement, and enrolment. Through joint blockchain projects, information technology and consulting firms had enrolled network participants up to the point that they started to operate some of their processes with Hyperledger-Fabric-based systems. Information technology and consulting firms themselves were enrolled through the open source character of the Hyperledger project. The preliminary status of mobilization is characterized by several spokesmen, which can be seen as access points (Giddens, 1990) to this actor-network: for example the Linux Foundation, Hyperledger

Fabric, IBM, and network participants such as Walmart. Human access points create users' trust in blackboxed systems by facilitating human-system interactions (Giddens, 1991). In the case of Hyperledger Fabric these access points were human and non-human. Moreover, this mobilization illustrated trust in the actor-networks' "reliable functioning" (Möllering, 2006a, p. 74), which was based on considerations and experiences from the entire translation. This means that trust was not solely based on the system representation through a single spokesmen or access point, but involved the construction of trust problems, interessement through trust narratives, reflexive trust building, routines, and leaps of faith from enrolment. Thus, mobilization implicitly incorporated various trust ontologies in translation, including trust as a problem, as an interessement device, and as an input to and process of enrolment. Although these ontologies resemble the ones explored in the Ethereum case, the two cases diverge with regard to the actors involved. As a result, they also differ with regard to the ways in which ontologies were configured and succeeded or not. In the next chapter, I provide a summary and comparison of these aspects, before discussing theoretical contributions, implications, and outlooks.

7 Discussion, implications, and outlook

In chapters 5 and 6 I explored the role of trust in two case studies of blockchain technology translations. In the following, I briefly summarize and compare the findings of the two cases, pointing out the multifaceted role of trust in both translations (7.1). Bringing together a theory of translation and trust to explore the role of trust in the creation of blockchain technology has allowed me to shed light on the processual character of trust in blockchain technology. Moreover, drawing upon these literatures has rendered multiple ontologies of trust visible. In sub-chapter 7.2 and 7.3, I discuss my contributions to organizational trust research and to studying translation in organization and accounting studies. I conclude by outlining the implications of my research for trust research and providing an outlook for further research on blockchain-enabled relations and ANT-inspired trust work.

7.1 Summary and case study comparison

The case studies of Ethereum and Hyperledger Fabric both describe translations of blockchain technologies, following Callon's (1986b) four moments of translation (3.2.1). Both cases render multiple ontologies of trust visible, including trust and the absence of trust as problems, trust as interessement devices, trust as inputs for enrollments, and trust building as actions of enrolment as well as resources for mobilization. However, the attempts to enact these ontologies differed among the cases. Throughout translation the platforms' actor-networks supported and sustained their own respective technological actors. Actors in Ethereum's actor-network included the Ethereum platform (connected with smart contracts, DAOs, DApps, Ether and other tokens), the Ethereum team, the Ethereum community, the business community, IT evangelists, and investors. Hyperledger Fabric assembled IBM, the Linux Foundation, the developer community, information technology and consulting firms, and blockchain network participants. In both cases, the respective blockchain platforms served as obligatory passage points in Callon's (1986b) sense and were meant to solve for various trust problems. While Ethereum's problematization drew on a crisis of trust in established organizations and infrastructures, such as technology corporations, financial services firms, and governments, a similar problem did not suit the Hyperledger Fabric platform. This was due to the platforms' differing technological characteristics and the varying interests of the actors involved. The Ethereum team and the Ethereum community, who initiated the Ethereum platform, proposed an alternative infrastructure to substitute internet platforms which had been dominated by established organizations. This expressed the radical dream put forth by blockchain enthusiasts (Swartz, 2017).

Hyperledger Fabric, on the other hand, was initiated by the information technology corporation IBM and geared towards corporate network participants, including the financial services industry and technology firms. As such, it constituted an incorporative vision of blockchain technology (Swartz, 2017). Although IBM first proposed a problematization inspired by the Ethereum actor-network, the problematization which eventually became central to Hyperledger Fabric's actor-network differed from what could be observed in the Ethereum case. While the Ethereum platform was initially public and permissionless, the Hyperledger Fabric platform was intended as a software for building private and permissioned blockchain networks. In line with this, Hyperledger Fabric's predominant problematizations illustrated a lack of trust among business partners as a problem – one which could be solved with Hyperledger Fabric. This pointed toward the destabilizing and untrustworthy aspects of the Ethereum actor-network, and drew upon reason, routine, and reflexivity. Ethereum's problematization in turn drew on the technical, organizational, and reputational struggles of Bitcoin. This is notable from a theoretical standpoint, given how translation studies suggests that problematization builds upon crises of trust in formerly stable systems or institutions (3.2.2). Although this was also the case in the Ethereum translation, problematization in the Ethereum case also drew on the trust crisis surrounding the relatively new and unstable Bitcoin network. In turn, in the translation of Hyperledger Fabric, Ethereum's trustworthiness was discredited through references to the team's abilities and to miscarried reflexive trust building on behalf of the platform and The DAO. The latter negative experiences led to reputational damages for the Ethereum platform and the Ethereum team, which was then turned into a problem that could be addressed by Hyperledger Fabric. To the theoretical construct of problematization this adds the notion of reason and reflexivity-based crises of trust in unstable actors. Overall, the problematizations of Ethereum and Hyperledger Fabric drew upon a narrative where trust was absent or in doubt, where the solution revolved around blockchain technology. Hyperledger Fabric's translation started after Ethereum, which allowed Ethereum to become both a reference for inspiration and a negative example of an actor-network that could not be trusted. IBM's turn from a problem that was somewhat similar to Ethereum's problem shows how a trust problem and the nature of a non-human OPP are interrelated. The public and permissionless Ethereum platform and the private and permissioned Hyperledger Fabric platform suited different trust problems. This is the first indication of agency in the blockchain platforms. While the Ethereum platform was proposed as an alternative to shaken confidence and unwanted reliance on powerful organizations and

centralized infrastructures, Hyperledger Fabric was proposed as a solution for a lack of trust within and between these actors.

Interessement translated blockchain platforms into trustless technologies, into trust facilitators and into trustees. Although, only the last two aspects pertained to Hyperledger Fabric, which also required “partial trust” as an input. Trust was an interessement device that suggested relations between several actors and – in the case of Hyperledger Fabric – delineated blockchain technology from other technologies. This happened with the aid of sometimes intertwined but also contradictory narratives. One of the main differences between the Ethereum and the Hyperledger Fabric case is the supposed trustlessness of Ethereum. While Ethereum and its smart contracts were related actors that – purportedly – had no necessity to trust either the platform or each other, Hyperledger Fabric was built on the assumption that network participants would have mutual relationships with “partial trust”.

Building on arguments from rationalist trust theory, the narrative that the Ethereum platform was trustless suggested that the Ethereum community, the business community, and investors would not have to trust the platform or each other. It argued that the platform was able to eliminate uncertainties and vulnerabilities of its users. Ethereum’s proof-of-work consensus algorithm was an algorithmic validation of transactions, which allowed for transactions to be processed through a decentralized and permissionless network. The nodes continuously verified the shared transaction ledger and incentives were supposed to assure that the platform could not be manipulated. The underlying assumption was that self-interested users would take rational decisions to avoid negative economic outcomes (Möllering, 2006a, p. 24). Moreover, interactions on the platforms through smart contracts were supposedly trustless, since they were all digitally signed and their executions were guaranteed. Once a smart contract was submitted it could not be reversed. Uncertainty was said to be erased. What differentiates this empirical concept of trustlessness from Möllering’s (2006a) reason category lies in the argument. According to the integrative trust framework, reason is a base for trust whereas trustlessness is an ideal of not trusting at all. It assumes that algorithms work flawlessly and are controllable. In the Ethereum case, a member of the business community confronted the Ethereum community and the team, claiming that trustlessness was not an interessement device and that it would not attract decision makers in the business community. Ethereum’s and Hyperledger Fabric’s enrolment of corporate actors confirmed this. On the other hand, Ethereum’s enrolment also showed how the ideal of trustlessness attracted other actors, such as the Ethereum community and team.

For Hyperledger Fabric, some trust based on reason and routine among potential blockchain network participants was a requirement for running a blockchain network. Unlike Ethereum, its consensus mechanisms were not intended to secure the network from every possible malicious behavior conducted by network nodes. With its restricted permissions, the Hyperledger Fabric platform was designed in a way that unrelated participants were not supposed to run a node. Instead, it presumed routine-based trust mechanisms between network participants like legal agreements and governance mechanisms specified within the Hyperledger-Fabric-based network. Moreover, Hyperledger Fabric was built on the rationalist assumption that only known and identified trustworthy participants that were aligned with a shared goal would be permitted to join permissioned Hyperledger-Fabric-based networks.

On the other hand, both cases had a narrative, which depicted blockchain platforms' technological capabilities as trust facilitators. In the case of Hyperledger Fabric, this role combined a reason and a routine perspective. Arguing with reason, blockchain technology's consensus mechanism and immutable transaction record would enable network participants to mutually control each other and thus avoid opportunistic behavior. This control consisted of assuring correct transaction processing and storage as well as leveraging the data to ensure that business partners would act as promised. Arguing from a routine perspective, blockchains' algorithmic rules for transaction processing and data storage could serve as institutional trust bases, which could create shared expectations among network participants. These rules would produce a shared ledger that would act as a trust facilitator – a “single source of truth”.

Ethereum's narrative directed towards the Ethereum community, investors, and business community was even more trustlessness in the guise of trust. The proof-of-work consensus mechanism and guaranteed execution should have facilitated trust between users in a trustless environment. The rationalist perspective on trust became visible in the argument about guaranteed execution. Smart contracts that were executed on the Ethereum platform were a “third party-guarantor and enforcer” (Möllering, 2006, p. 60) of agreements, which restricted the ability of platform users to act against the code. As smart contracts and thus the code of DAOs were transparent to the public, it was thought fraud could be prevented and that smart contract and DAO issuers would signal trustworthiness towards investors and other stakeholders of business organizations. The signaling aspect of Ethereum differed from Hyperledger Fabric as the latter was conceived for transparency and processes within a network, where Ethereum's signaling meant attracting and informing a broader audience such as investors, customers, or employees. However, similar to Hyperledger Fabric, Ethereum's

smart contract execution produced supposedly immutable data, which was traceable and auditable and thus enabled reconciliation of past events. The difference was that the data was accessible to the public and not restricted to predetermined network participants, as in the case of Hyperledger Fabric. As in the case of Hyperledger Fabric, this technical characteristic was promoted as trust-facilitating. However, the mechanism was a technical control mechanism for reducing uncertainty between parties interacting through smart contracts. With regard to reputation systems envisioned by Vitalik Buterin and members of the Ethereum community, this control was supposed to be based on Ethereum's transaction data and adjacent reviews and internalized by users. For example, investors would be enabled to gather experience and knowledge about economic exchange partners without having to draw upon own prior exchange history with them, but by referring to data-based reputation. This would imply process-based (Zucker, 1986) trust production without own prior exchanges. The recurrence on the Ethereum platform and its data, however, would imply that involved parties shared expectations about Ethereum's role as a provider of immutable and reliable information. It would also require these actors to accept the practice of "open execution". In that sense, the Ethereum platform would act as a transparent institutional (Zucker, 1986) trust facilitator.

Another narrative and goal that appears in both cases was the establishment of blockchain platforms and related technical actors as trustees for other involved actors. Narratives in both cases drew on reason, routine, and reflexivity, but in different ways. The Ethereum team and IT evangelists envisioned the Ethereum platform as a blackboxed, trusted technological infrastructure, which people would not necessarily understand or even notice. The Ethereum platform, the Ethereum team, Ethereum community, investors, and business community would then be mobilized so that others would rely on this network as users of its specific services and applications. Thus, their vision was of a mobilized and trusted technology in the sense of system trust (Giddens, 1991; Luhmann, 1979), whose inner workings would not be apparent for society. On the other hand, interessement outlined trusting relations between the actors within the network as well. It suggested leaps of faith (Möllering, 2006a) toward blockchain technology's algorithms by the Ethereum team, the Ethereum community, and the business community. Complementary to this suggestion, the Ethereum team also hinted at Ethereum's trustworthiness (Mayer et al., 1995; McKnight et al., 2011) as the result of the platform's open source code and its decentralized operations. Lastly, Buterin suggested that the Ethereum community and investors could build reflexive trust (Möllering, 2006a) with the Ethereum platform through experimenting and reviewing a pre-released version of the software.

The narrative on Hyperledger Fabric not only framed the software, but also the fabricated data as trustees. It did not make explicit references to faith in technology, as did Ethereum. However, like Ethereum, it was proposed that blockchain network participants would trust the data produced by Hyperledger-Fabric-based systems based on routine. Jointly determined and executed algorithmic rules would become institutional rules and allow Hyperledger-Fabric-based networks to produce immutable data. Based on these algorithmic rules, which were executed on network nodes of several network participants, the latter could trust the data.

Similar to Ethereum, Hyperledger Fabric's continuity was claimed as sign of trustworthiness – a sign of ability (Mayer et al., 1995) and functionality (McKnight et al., 2011). Data privacy options, as well as the flexibility of Hyperledger-Fabric-based networks, were taken as rational signs of the ability or functionality of the software that were unique of Hyperledger Fabric. Two more trust bases were installed, which were different from Ethereum. IBM's consideration of regulatory requirements was a routine basis directed towards potential blockchain network participants who aimed to comply with regulatory provisions. Lastly, an expected trust spill-over (Stewart, 2003) from reputable actors, such IBM and the Linux Foundation to Hyperledger Fabric occurred as these actors communicated with information technology and consulting firms, potential new members of the developer community, and potential blockchain network participants. This reflexive trust base was characterized by the intention to build these actors' trust in the software through reflexive interactions. This last point reflects yet another similarity to Ethereum's approach.

Overall, interessement outlines relations between actors. In the presented blockchain cases, trust is a relational element. For both blockchain platforms, narratives involving trust functioned as interessement devices insofar as they associated the technology with trust in many ways. These narratives pull in notions of reason, routine, and reflexivity, and in the case of Ethereum, a leap of faith, to outline potential trust relations among actors. However, as they were interessement devices, these narratives did not yet present trust, only proposals. The enrolments in both cases were enabled by leaps of faith taken by several actors; they showed trust building actions and further trust relations that resulted from interessement and enrolment.

In both case studies, leaps of faith by human actors and organizations sparked the beginnings of enrolment. Members of the Ethereum team, early community members, and early investors took leaps of faith by investing their time in the Ethereum platform and buying Ether. They expressed a will to believe that the technical ideas from the Ethereum whitepaper and the idea of a trustless platform had the potential to translate into a successful technical

actor. With small and affordable leaps of faith, they invested in Ether as if uncertainties about it would be favorably resolved (Möllering, 2006a, p. 111). This belief was sustained by personal interactions with Ethereum team members, debates with team and community members in internet forums, and a rising price of the Ether cryptocurrency. The Hyperledger Fabric enrolment was determined by a powerful actor's (IBM's) early leap of faith, i.e. when the firm decided to invest in the development of an alternative blockchain technology for established organizations. IBM took a leap of faith in the sense that it maintained a will to believe in an actor that was yet to be determined. IBM's and Linux Foundation's brands and reputation led other actors in the Hyperledger Fabric case to take leaps of faith to enroll with the software. Thus, trust spilled over (Stewart, 2003) from the initiating brands to the technology itself. Information technology and consulting firms and potential network participants decided to start working with the technical actor, despite not knowing about or having a clear purpose for the software. A spill-over of reflexive trust led to just-do-it leaps of faith, which then enabled further reflexive trust building and enrolment.

Throughout their enrolments, both cases illustrate further reflexive trust building (Möllering, 2006a) with some similarities and differences. Online and offline communication through example blogs, forums, websites, videos, books, conferences, hackathons, and meetups helped actors build knowledge about and familiarize themselves with the blockchain platforms. In the case of Ethereum, smart contracts, the DAO, and tokens served a similar function. The reflexive trust building processes conducted through these formats were accessible to all actors. Investors experimented with buying and selling cryptocurrencies, pulling in additional informative resources, such as forums and white papers. The Ethereum team and community could signal their trustworthiness during personal encounters. The Ethereum community and Hyperledger Fabric's developer community could furthermore support the technical development processes of open source platforms. In Hyperledger Fabric's community, an increasing number of programmers from other firms joined IBM employees to further develop the software. The Ethereum team collected feedback on the Ethereum platform from its community, which experimented, tested, and reported bugs on the platform. Some Ethereum community members even joined the Ethereum team. Thus, the platforms were not built by a single provider, but through a trusted collaborative process with different open source communities. In both cases, the Ethereum community, Ethereum's business community, Hyperledger Fabric's potential network participants, and information technology and consulting firms engaged in projects to develop smart contracts and more complex applications, experiment with the platforms, and use the platform for business

transactions. For several actors, interactions with the platforms, (including smart contracts and the cryptocurrencies) as well as interactions with other actors, such as the Ethereum team, community or IBM, generated positive experiences and enhanced trust in the respective actor-networks. This trust, however, was not solely a question of using the platforms, but of changing them through reflexive trust building processes. IBM's projects with potential network participants generated new requirements for the Hyperledger Fabric software, as did comments and questions from the Hyperledger Fabric community. The Ethereum team perceived data privacy as a subject central to the Ethereum community's negotiation of trust and began improving privacy features of the Ethereum mainnet. Negotiations and changes to the platforms showed how these technical actors were not stable throughout enrolment or the overall translation process, but subject to interpretations and adaptations.

Corporate actors such as Ethereum's business community and Hyperledger Fabric's potential network participants were reluctant entrusting their business data and operations to permissionless and public blockchain networks like Ethereum. Although they were attracted to the concepts of smart contracts and blockchain technology, they did not trust a platform with publicly available transactional data maintained by anonymous miners. The Hyperledger Fabric case in particular shows how businesses had no interest in conflicting with existing routine-based trust structures, such as regulation. That being said, these reluctances did not inhibit the enrolment of enterprises with blockchain technology. Rather, they led to modifications of the technical actor. In the case of Hyperledger Fabric, IBM initiated the translation of blockchain software for permissioned and private networks. Ethereum was translated into a permissioned and private version of itself when the business community enrolled with it.

Furthermore, Hyperledger Fabric's rejection of permissionless and public blockchain technology built on vulnerabilities of the Ethereum actor-network, which emerged after the unintended exploit of The DAO. Before the exploit, investors, the community, and the team bracketed out uncertainties about The DAO's code and generally expected no major issues. Retrospectively, this behavior of dealing with uncertainty was perceived by actors as both risky and trusting. Besides this trust in The DAO and the underlying Ethereum platform, human actors also appeared to trust each other. Conflicts which resulted in the separation of the Ethereum community and platform into two communities and two platforms had been inconceivable beforehand. Reflecting on this experience, team members described a general overconfidence about the cohesion of team, community, and investors – something which was tested through the DAO incident. This mutual trust had been built and expressed through

these actors' enrolment with cryptocurrencies, but also through other reflexive trust building interactions. However, after the DAO exploit, Vitalik Buterin negotiated with the community about how to proceed. Eventually, the team and the majority of the community jointly manipulated the Ethereum platform, and thus broke the ideology of trustlessness in order to rescue funds. Their intention was to limit the damage by interfering with the agency of the Ethereum platform. While the majority of the Ethereum community was aligned with this goal, a smaller group adhered to the trustlessness ideology of the Ethereum platform. This smaller group continued the platform version with the exploited DAO as a separate blockchain, which had a separate cryptocurrency and a separate community. Although the manipulation was positively acknowledged by some members of the business community, the whole story nurtured Hyperledger Fabric's problematization of permissionless networks, which were ran by anonymous miners and provided by teams and communities with less widespread reputation.

However, Hyperledger Fabric also faced some trust deficits throughout its enrolment. One of them stemmed from regulatory uncertainty. When implementing trials in their every-day business, potential network participants did not assume an as-if or just-do-it attitude in the absence of regulatory clarity, but stopped projects altogether. Other network participants that started to use Hyperledger Fabric for their usual businesses complemented the platform with established rule and role-based trust arrangements. Nevertheless, potential network participants hesitated to enter permissioned Hyperledger-Fabric-based blockchain networks with other companies. IBM recommended building on existing trust relations between companies and entering in a gradual trust building process among the partners and the technology in which parties initially share non-sensitive information.

Overall, the enrolment in both cases resembled processes of reflexive trust building between various human and non-human actors. These were enabled by human actors' leaps of faith toward technical actors. Trust in Hyperledger Fabric was built upon reflexive trust in the technology and brands as well as experiences with providers. It was also supported by routine-based trust. By contrast, trust in Ethereum relied less on routines and brands, and more on mutual experiences, knowledge building, and influence over joint problem solving among a network of technical and human actors.

Besides some troubles and adjustments throughout the trust building processes mobilizations of Ethereum and Hyperledger Fabric actor-networks rendered visible temporary trust in various contexts. Möllering's understanding of Luhmann's (1979) and Giddens' (1990) system trust describes several of these trust constellations. Investors and issuers of

ICOs, and users of the game CryptoKitties confided in the reliability of the Ethereum platform, which was supported and maintained by the Ethereum team, the community, Ether, and smart contracts. In doing so they did not count on knowledge of the network's inner operations and relations, but implicitly assumed that it supported their investment, funding, and gaming activities. Several human and non-human access points (Giddens, 1991; Möllering, 2006a, p. 74), such as marketing campaigns, celebrities, cryptocurrency millionaires, and familiar gaming practices attracted these actors to the actor-network. Uncertainties covered by system trust became visible when the actor-network acted unexpectedly. In the case of CryptoKitties, the Ethereum platform had difficulties coping with the high amount of transactions created by CryptoKitties gamers. In the case of ICOs, disappointing profits and stories about scams led to the conclusion that the actor-network was an instable system that lacked control mechanisms (Luhmann, 1979; Möllering, 2006a, 72). The hope among actors with regard to ICOs was that regulatory intervention could create rules, which would align expectations of all actors towards ICOs. In order to further mobilize the business community with the platform, the Enterprise Ethereum Alliance aimed to become a provider of technical rules for the Ethereum platform. Whether this attempt would be successful remained an open-ended question at the time of analysis. Nevertheless, the coming together of the business community under the roof of the EEA represented an initial sign of mobilization, which included statements about enterprises' trust in the Ethereum actor-network. This trust built on interessement and enrolment; it reflected the narrative that Ethereum was a trusted platform, and built on the positive experiences gathered through enrolment. In this sense, the Ethereum and Hyperledger Fabric cases are similar in yet another way: Trust in the mobilized Hyperledger Fabric actor-network also drew upon interessement and enrolment. The mobilization of Hyperledger Fabric in actual blockchain networks points to network participants' confidence in the reliable working of a software backed by the Linux Foundation, developer community and information technology and consulting firms. The coming together of competing financial services firms, which were connected through a single source of truth, reflected one of the trust narratives from interessement. It also built on reflexive trust building among actors during enrolment. Finally, the mobilization of Hyperledger Fabric has also exemplified what I call blockchain-enabled relations. Financial services firms and their respective customer data were connected through a Hyperledger-Fabric-based computational network. However, I cannot tell how this shaped the organizations' mutual trust, their trust in presumably fraudulent clients, or their trust in data over time. A macro perspective on the Hyperledger Fabric actor-network and the early stage

of its development during my research has prevented me from investigating such aspects further. They remain interesting topics for further research.

In sum, the cases of Ethereum and Hyperledger Fabric have shown multiple ontologies of trust which unfold along Callon's (1986b) four moments of translation. In the following, I argue how this contributes to organizational trust research and studies of translation.

7.2 Contributions to trust research

Concepts from ANT – especially translation – have not yet been considered in organizational trust research. By exploring ontologies of trust in the cases of blockchain platforms through the lens of translation I exemplify how ANT may enrich trust research. In reflecting on the phenomenon blockchain technology from a translation perspective, and referring to the examples of Ethereum and Hyperledger Fabric, I contribute to organizational trust research the notion of multiple ontologies of trust. Trust appears, for example, as a problem, an interessement devices, and as a reflexive process. I enrich the current literature by exploring a multifaceted nature of trust and shedding light on the processual character of trust in an information technology.

By drawing on the notion of translation, I pull an assumption from Actor-Network Theory into trust research, namely that technical actors are attributed with agency. Blockchain platforms and other computational devices are viewed as technical actors. From this perspective, I understand blockchain platforms, their smart contracts, DAOs, Ether and other tokens as “more or less specific others” (Möllering, 2006a, p. 111) – trustees with agency. This constitutes a contrast to the assumption that information technologies and specific IT artifacts do not have agency (McKnight et al., 2011; Söllner et al., 2013; van der Werff et al., 2018). I argue that interessement devices in both empirical cases illustrate attributions of agency. The ideologies of trust and trustlessness were built on attributions of agency to blockchain platforms. Despite the instability of the blockchain platforms, they were viewed as avoiding or facilitating trust, or becoming trusted based on various characteristics. These potential trustless and trustful relations through and towards blockchain platforms were constitutive of the interessement of human actors, regardless of whether actual experiences with the platforms confirmed or dismissed the narratives. Moreover, the ANT perspective has helped shed light on how software may act in unintended ways, which influence trusting relations with human actors. This was exemplified well with the DAO incident and subsequent flaws in smart contracts in the Ethereum case.

I have also explored the role of trust or a lack of trust as problems. In this way, my work shares something with the discourse on trust repair in organizational trust research from the aftermath of the financial crisis (Bachmann et al., 2015; Gillespie & Hurley, 2013), i.e. that trust crises constitute problems. However, the actions and narratives described in my case studies do not aim to repair trust, but to establish alternatives or to enable trust where it was lacking.

Overall, translation captures the relation between blockchain platforms and human actors as a reflexive social process. Trust building influences human actors, blockchain platforms and their mutual relations throughout translation. The two cases of emerging blockchain technology bring this understanding from ANT to organizational trust research. In both cases, human actors engaged in trust building processes with blockchain platforms – through interactions with other human actors and with the platforms themselves. Trust spill-overs played a role in the interessement and enrolment of Hyperledger Fabric. These were based on routine, as theorized by Stewart (2003), but also on reputable brands and former experiences, i.e. on reflexivity. In addition, my work contributes to research on trust in information technologies by explicitly describing reflexive trust building attempts. During enrolment, the above mentioned trustors gained knowledge and mutual understanding through communication with one another and other supporters of the technology. This communication was conducted in person as well as through various online media. Möllering (2006a) explains how communication and mutual openness are practices of reflexive trust building between human actors. In this respect, both empirical cases reflect established theory on interpersonal and inter-organizational trust. However, another aspect of reflexive trust building lies in actors' familiarization with blockchain platforms. In both cases, there were repeated interactions among human actors and unstable blockchain platforms, contributions and tests on the platform, experiments with smart contracts, and in the case of Ethereum, buying and selling cryptocurrencies. Human actors' reflexive trust building with blockchain technology consisted of gaining knowledge about how this technology works. In other words, reflexive trust building was enacted through familiarization. With reference to Luhmann (1979), Möllering (2006a) treats familiarization as a reflexive trust building mechanism between human actors. Gefen (2000) and Möhlmann (2016) extend the notion of familiarity to frame it as a basis for user trust in IT artifacts such as online vendors and sharing economy platforms. My research supports the idea of technical actors as trustees, and adds to it that trustors are not only lay people, as suggested by Luhmann (1979). Trustors in both cases were also professionals and early adopters with programming skills. They joined the actor-networks not

as users, but as supporters or even providers. This included, for example, people who joined the Ethereum team or the Hyperledger Fabric developer community. Also the knowledge one acquires through familiarization (Luhmann, 1979), which builds a base for trust in technology (McKnight et al., 2011) was not as stable as it appears in existing theoretical constructs. I show that throughout the observation period, blockchain platforms remained emerging technologies, which attracted people based on ideas, but whose capabilities were in flux and subject to change. Thus, non-human trustees and the knowledge gained by trustors can be unstable, but still engage in trust building. Moreover, my analysis pays attention to truly reflexive interactions, which have not been described in the literature so far. Instead of deciding whether or not to adopt the Ethereum platform, the Ethereum business community influenced the platform according to their requirements and interests. So much so that it eventually led to separate permissioned and private Ethereum networks. This form of mutual influence and change points to the social aspects of trust building between human actors and information technologies like blockchain.

Möllering (2006a) discusses how reflexive trust building processes between human actors leads to leaps of faith. This was also the case for human actors and their trust in blockchain platforms. IBM and the Ethereum team believed in their respective platform concepts. In the case of Ethereum, open communication towards other actors led to initial leaps of faith toward the blockchain platform and its tokens. By contrast, in the case of Hyperledger Fabric, the reputation of enrolled brands spilled over onto the Hyperledger Fabric platform, leading to leaps of faith by other human actors. In both cases, leaps of faith appeared as both inputs and outputs of enrolment.

The mobilization of blockchain platforms in actor-networks consisting of human actors and information technologies speaks to the suggestion that user trust in IT artifacts is one of many relations in a trust network (Söllner et al., 2016). Such relational network could include, for example, providers of the IT artifact. I support the general analytical distinction between the technology and the provider organization or brand, though these are often mingled together. Instead of a singular artifact, my research sketches two trust networks that surround an emerging information technology. This exemplifies that instead of a singular provider, there can be multiple supporters of technological systems who become connected through trust relations.

Overall, these various contributions on actors' reflexive trust building in each other and in blockchain platforms translate the ontological shift towards trust as a process from general organizational trust research into research on trust in information technologies. With this I

move from trust in information technology as an attitude towards trust as a process, which also embraces the leap of faith (Li, 2017). This is even more important considering how research on trust in information technologies still occupies a niche in organizational trust research, but flourishes in other scientific discourses, i.e. information systems research. Moreover, my work extends trust research's attention to people, organizations, and IT artifacts as trustees by suggesting that emerging information technologies can act as trustees too.

Due to the macro perspective of my approach and the early stage of blockchain projects during the observation period, it is difficult to say how blockchain technology influences relations between blockchain network participants. For example, I cannot say how trust between financial institutions that use shared ledgers for receivables financing interferes with the platform. Similarly, I have no information about the CryptoKitties gamers, future EEA platform users, or the character of their mutual relations. However, based on the interestment device of trust, I offer some speculations on how blockchain technology might modify our understanding of institutional-based trust. With reference to studies on the online marketplace eBay, Bachmann and Inkpen (2011) describe online user community norms, structures, and procedures as mechanisms for institutional trust building. I suggest viewing the information technology itself as an actor when researching platform-enabled trust. As we know from critical accounting research, eBay's algorithm provides a calculative infrastructure that inscribes structures, enables control by users, and facilitates trust between them (Kornberger et al., 2017). The user community contributes to the calculative infrastructure through their provision of feedback on sellers and buyers. The algorithm itself, however, is a business secret of the platform provider, eBay. As an organization, eBay has power over the algorithm which facilitates trust between users. Quite differently, blockchain platforms promise shared power over the algorithms. Ethereum and Hyperledger Fabric were both open source platforms where the communities were supposed to influence platforms' underlying code. Smart contracts on the public Ethereum platforms were executed in a transparent way. Moreover, they were processed and verified by multiple network nodes instead of a singular entity like eBay. Although permissioned and private networks reduced this shared power to selected network participants, power in permissioned blockchain networks could still be shared among participants. Reading and writing rights for smart contracts, for example, were said to be customizable to required network setups. Thus, if we assume further mobilization of blockchain platforms, it is worth considering algorithms within the construct of routine-based or institutional-based trust. In addition, this perspective might differentiate secret

algorithms provided by singular organizations from shared power over trust-facilitating algorithms.

Considering the role of blockchains' shared ledgers in facilitating trust through immutable and transparent data, I also see this actor blurring the conceptual line between Zucker's (1986) institutional and process-based trust in a digital platform context. On trust-facilitating digital platforms, such as Ethereum and Hyperledger Fabric, interessement devices suggest that a shared ledger facilitates trust through immutability and transparency. This was supposedly the case on private blockchains with restricted transparency as well. On the one hand, the jointly executed (and therefore transparent) computational code and data might assume the role of a commonly accepted, institutional trust facilitator between users as described above. On the other hand, Ethereum's public historic transaction data was proposed to be used in reputation systems. Such data, however, can also be interpreted as an equivalent to one's own or a third party's experience and thus can potentially act as a data-based or impersonal base of process-based trust. Research on digital trust cues in the sharing economy (Möhlmann & Geissinger, 2018) considers peer reputation as a reason-based mechanism for trust between users. Blockchain data is different from reviews on online market places (Bachmann & Inkpen, 2011) or sharing economy platforms (Möhlmann & Geissinger, 2018) in that it documents interactions, which have occurred directly on the platform (as opposed to interactions mediated by the platform). I argue that this data might evolve into a trust cue for public blockchain platforms – a data-based hybrid of process and institutional bases for trust.

Lastly, Ethereum's interessement constructs an ideology of trustlessness. Although enrolment and mobilization showed that investments in The DAO and ICOs were not trustless, the ideal still appeared as an interessement device. The case of Ethereum was not singular, as Bitcoin had previously established the ideal of trustlessness. In the case of Bitcoin, trustlessness was also central to establishing an identity. The positive connotation of trustlessness supports those voices in organizational trust research, who are wary of the mostly positive perception of trust (Skinner et al., 2013).

Overall, analyzing blockchain technology through the lens of translation has enabled the discovery of trust's multiple roles – trust appears as a problem, an interessement device, an input for enrolment, and as a process and relational element. These different ontologies have led me to complement several constructs in organizational trust research as well as research on trust in information systems. The underlying contribution is that the exploration of multiple ontologies of trust is made possible through a social process perspective on trust in blockchain technology, and information technologies more generally.

7.3 Contributions to the study of translation

In a review of translation studies from organization and accounting research, I've made a conjecture that translation and trust theory are implicitly connected (3.2.2). The case analyses provided in chapters 5 and 6 support this claim. They are similar to other translation studies in so far as they trace mutual relations and modifications of actors – human as well as non-human – throughout translations. My reflections on several relations and devices through the lens of Möllering's (2006a) integrative trust framework has allowed me to identify several ontologies of trust in translation. Trust and the absence of trust can constitute a problem or act as interessement devices. Moreover, leaps of faith enable enrolments and enrolment implies reflexive trust building. Finally, trusting relationships connect actors, can hold actor-networks together, and mobilize them. When studying translations in organizational and accounting contexts, a multitude of trust ontologies can sharpen our view and our language regarding trust.

My review has suggested that the construction of a trust crisis is a common element in translation. I have identified how the destabilization of actors implies that other actors reduce their routinized trust in them. In both blockchain cases, problematization also meant questioning and destabilizing other actor-networks. This was done by problematizing either the need to rely on untrusted established organizations, as in the case of Ethereum; or problematizing absence of trust as in the case of Hyperledger Fabric. Translation theory says that an OPP usually solves for the constructed problem (Callon, 1986b): In the case of blockchain, trust crises. Ethereum and Hyperledger Fabric were both presented as solutions to different trust crises. Remarkably, the case of Hyperledger Fabric shows how a problem was constructed specifically as something which could be solved by Hyperledger Fabric platform. The initial problem presented by IBM drew on the company's early enrolment with Ethereum. However, Hyperledger Fabric had different characteristics from Ethereum and was intended to serve mostly established organizations. This distinction required the framing of a distinct trust crises. Hyperledger Fabric's trust crisis did not question institutions, and thus routine-based trust. Instead it showed how trust crises in translation draw upon reason and reflexive processes, much as Ethereum's questioning of the Bitcoin actor-network.

Moreover, Mouritsen and Thrane (2006) identify trust as a problematizing device within an actor-network where trust is absent despite an organizational ideology of trust. The case of Ethereum turns this construct upside down, as it posits trustlessness as both an ideology, and a solution to reliance on untrusted institutions. This brings me to the point that both blockchain

cases exemplify how trust can serve as an interessement device. The narratives connect blockchain technology to trust, describing it as a trustless system, a facilitator of trust, and a trustee. These narratives incorporate concepts of trust that are based on reason, routine, and reflexivity. These interessement devices envision specific relations between actors in the network and distinguish blockchain technology from other technologies. Its technical characteristics, which are supposedly able to reduce uncertainties among the platforms' users, support arguments for how the platforms either eliminate or enhance trust in business relationships. My theorization of trust's role as an interessement device is different from former translation studies insofar as it sticks to the vocabulary provided by Callon (1986b). However, it resonates with what Mouritsen and Thrane (2006) describe as an ideology of trusting. In their translation case, this idealized trust in network enterprise relationships does not hold true in the network's practice or negotiations, as trust turns out to be absent. Inversely, permissionless blockchain platforms like Ethereum or Bitcoin exhibit trustlessness as an interessement device or ideology; although, Ethereum's enrolment shows that trust in the network is not absent and research on Bitcoin exposes the idea of trustless money as a fantasy. These contrary constellations corroborate translations' distinctions between interessement and enrolment or proposition and negotiation. The explicit ideal of a trustless network extends the repertoire of trust meanings and interessement devices in translation studies.

With regard to enrolment, my research confirms that routine- and reflexivity-based trust can be an input to enrolment. Trust in rules, roles, and brands became visible in the case of Hyperledger Fabric. I also agree with Chua (1995) that the translation of software requires believers who have faith in the immature non-human actor and enroll with it. I have shown in both cases that these believers took a leap of faith (Möllering, 2006a). By doing so, they supported the enrolment of blockchain platforms. On the other hand, I disagree with Chua (1995) with regard to the agency of software. Here, I argue with ANT's common assumption that non-human actors and thus information technologies display unintentional agency. The Ethereum platform performed better than expected after its launch and gave rise to trust in the The DAO. The DAO, in turn, then unintentionally disappointed the trust of investors, the Ethereum team, and the community.

Moreover, I want to stress the spectrum of reflexive trust building activities which belong almost by definition to the moment of enrolment. Callon (1986b) describes enrolment as a set of negotiations and trials – things which reflexive trust building draws upon. All of the joint testing and experimenting, working together to progress blockchain platforms, applications

and networks; discussing and learning online and offline, sharing of information and emotions were practices of inter-personal and inter-organizational reflexive trust building. At the same time, they were negotiations and trials of mutual relationships and roles in actor-networks. They led to leaps of faith – to mutual trusting relationships between human and non-human actors, which again mobilized broader actor-networks. It appears that one of the mechanisms that holds actor-networks together is trust. Where trust is in doubt and uncertainty cannot be dealt with, for example in the case of Ethereum’s ICOs, actor-networks become unstable as actors demand additional trust mechanisms. However, the cases show that trust relations, which constitute mobilization are not solely based on routine, but also reflexive bases. This observation might be due to the timing of my observations, as I have not opened a black box but traced blockchain technology in the making.

Overall, my research explicates – along Callon’s (1986b) moments of translation and Möllering’s (2006a) trust categories – how translation and trust theory are interwoven. The cases point to the richness of trust bases, which the integrative trust framework addresses in qualitative trust studies; at the same this illustrates the richness of relations and ontologies, which translation aims to discover. Now that I have discussed my research’s contributions to organizational trust research and to the study of translations, the following section will reflect on the implications of my research and provide an outlook.

7.4 Implications and outlook

This dissertation has resulted in a journey, which followed various ontologies of trust in the emerging socio-technical world of blockchain technology. Nobody can tell whether and for how long blockchain platforms are going to mobilize and be mobilized. Translations of blockchain technology exemplify that the technology has its supporters, including individuals and business organizations, who sometimes dare to trust it and who make efforts to build actor-networks of trustors around the information technology. Trust in blockchain technology is manifold, it is a social process and it cannot (yet) be taken for granted. At the same time, blockchain technology is expected to interfere with inter-personal, inter-organizational and socio-technical trust structures as it becomes mobilized. This is why blockchain technology is a phenomenon of high relevance for organizational trust research. My work, however, can only be a starting point for investigating socio-technical worlds of blockchain technology within organizational trust research. In the following, I outline ideas for further research on blockchain-enabled relations. Moreover, I point at the implications of trust narratives for trust

research. Finally, I reflect on how translation and more broadly ANT can inspire trust research.

Blockchain-enabled relations supposedly connect users in permissioned and permissionless networks, which have different degrees of shared power and control over data and algorithms. Besides the speculations offered in sub-chapter 7.2, organizational trust research has still little empirical understanding of such blockchain-enabled relations, or the trust and absence of trust they imply. Further research can therefore investigate how network participants within permissioned blockchain networks relate to each other. Given their possibilities to participate in blockchain network operations, what is the role of blockchain network participants? Do they act as users or providers or both? In which ways and on which bases do they trust each other? To what extent is this different in permissioned and private networks compared to relations between users of permissionless and public networks? How are these relations influenced by participants' trust in the blockchain infrastructure and in specific applications? How does the sharing of data points among participants within permissioned blockchain networks change their relations toward end customers and vice versa? Such questions can lead us to an advanced understanding of what theory has begun to call digital trust cues (Möhlmann & Geissinger, 2018) and protocol (Kornberger et al., 2017), and may modify our understanding of process versus institutional-based trust.

Moreover, blockchain technology is a phenomenon that is intertwined with narratives on trust and trustlessness as interessement devices. Thus, it would not be surprising if further qualitative research about this phenomenon also finds these narratives. Research on specific blockchain-based applications or permissioned networks might also encounter the narratives described here, as the respective actors are part of larger macro networks that I have described in chapter 5 and 6. These actors most likely do not only act within their specific network, but are connected to macro networks through implementation and consulting projects, conferences, media, books and experiments. As researchers, we have to continue being wary of simply reproducing such narratives while also further investigating their effects and how they come into practice. In this regard, the example of blockchain technology can also make organizational research attentive to trust narratives with regard to other socio-technical worlds.

Lastly, my introduction of the translation concept into trust research has theoretical implications for organizational trust research beyond the specific phenomenon of blockchain technology. With regard to research on trust in information technologies, it suggests an ontological shift towards a process perspective of trust. Translation's attitude of a becoming

of things can help explore the fragility, temporality, and development of trust in information technologies. The transfer of translation from ANT to organizational trust research also implies that we should no longer consider the technical and the non-human as a context, but as actors on equal footing with humans and organizations. Actors – human and non-human – act. ANT thus has the potential to support efforts in trust research to explore trusting actions that are distinguished from trusting attitudes and intentions, and trace how they come into being. ANT's rendering of trust as a relation, but also its other ontologies, such as problems, ideologies and devices, may finally scrutinize trust research's own ideology of trust as a mainly positive and desirable concept.

References

- Abbott, C. (1929). Better fitting garments decrease alterations. In *Proceedings of the Controllers Congress, of the National Retail Dry Goods Association*, Chicago, IL.
- Alcadipani, R., & Hassard, J. (2010). Actor-network theory, organizations and critique: Towards a politics of organizing. *Organization*, 17(4), 419–435. <https://doi.org/10.1177/1350508410364441>
- Alisie, M. (2014a, July 14). The Ethereum project: Learning to dream with open minds. Retrieved from <https://blog.ethereum.org/2014/07/14/the-ethereum-project/>
- Alisie, M. (2014b, September 2). Crypto renaissance. Retrieved from <https://blog.ethereum.org/2014/09/02/crypto-renaissance/>
- Alisie, M. (2015, March 14). Mihai's Ethereum project update. The first year. Retrieved from <https://blog.ethereum.org/2015/03/14/ethereum-the-first-year/>
- Alvesson, M., & Kärreman, D. (2007). Constructing mystery: Empirical matters in theory development. *Academy of Management Review*, 32(4), 1265–1281. <https://doi.org/10.5465/amr.2007.26586822>
- Alvesson, M., & Sköldbberg, K. (2012). *Reflexive methodology: New vistas for qualitative research* (2nd ed.). London, United Kingdom: Sage.
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., . . . Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference* (pp. 1–15). New York, NY: ACM. <https://doi.org/10.1145/3190508.3190538>
- Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital cryptocurrencies*. Sebastopol, CA: O'Reilly Media.
- Axelrod, R. M. (2006). *The evolution of cooperation*. New York, NY: Basic Books.
- Bacharach, M., & Gambetta, D. (2001). Trust in signs. In K. S. Cook (Ed.), *Trust in society* (pp. 148–184). New York, NY: Russell Sage Foundation.
- Bachmann, R. (2001). Trust, power and control in trans-organizational relations. *Organization Studies*, 22(2), 337–365. <https://doi.org/10.1177/0170840601222007>
- Bachmann, R., Gillespie, N., & Priem, R. (2015). Repairing trust in organizations and institutions: Toward a conceptual framework. *Organization Studies*, 36(9), 1123–1142. <https://doi.org/10.1177/0170840615599334>
- Bachmann, R., & Inkpen, A. C. (2011). Understanding institutional-based trust building processes in inter-organizational relationships. *Organization Studies*, 32(2), 281–301. <https://doi.org/10.1177/0170840610397477>
- Bachmann, R., & Zaheer, A. (Eds.). (2006a). *Handbook of trust research*. Cheltenham, United Kingdom: Edward Elgar.
- Bachmann, R., & Zaheer, A. (2006b). Introduction. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research* (pp. 1–12). Cheltenham, United Kingdom: Edward Elgar.

- Bachmann, R., & Zaheer, A. (2013). Introduction. In R. Bachmann & A. Zaheer (Eds.), *Handbook of advances in trust research* (pp. 1–6). Cheltenham, United Kingdom: Edward Elgar.
- Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications*, 4(1), 1–10. <https://doi.org/10.1057/s41599-018-0065-0>
- Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, 19(10), 1020–1034. Retrieved from <https://aisel.aisnet.org/jais/vol19/iss10/1/>
- Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain – the gateway to trust-free cryptographic transactions. In *24th European Conference on Information Systems*, Istanbul, Turkey. Retrieved from https://aisel.aisnet.org/ecis2016_rp/153
- Behlendorf, B. (2016, September 13). Meet Hyperledger: An “umbrella” for open source blockchain & smart contract technologies. Retrieved from <https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies>
- Behlendorf, B. (2017a, February 14). Happy birthday, Hyperledger! Retrieved from <https://www.hyperledger.org/blog/2017/02/14/happy-birthday-hyperledger>
- Behlendorf, B. (2017b, March 3). Our incubator’s first graduate: Hyperledger Fabric. Retrieved from <https://www.hyperledger.org/blog/2017/03/03/our-incubators-first-graduate-hyperledger-fabric>
- Behlendorf, B. (2017c, December 21). Onward and upward for Hyperledger in 2018. Retrieved from <https://www.hyperledger.org/blog/2017/12/21/onward-and-upward-in-2018-for-hyperledger>
- Belliger, A., & Krieger, D. J. (2006). Einführung in die Akteur-Netzwerk-Theorie. In A. Belliger & D. J. Krieger (Eds.), *ANThology: Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie* (pp. 13–50). Bielefeld, Germany: transcript Verlag.
- Bernstein, M., Potvin, D., & Martin, D. K. (2004). A qualitative study of attitudes toward error in patients facing brain tumour surgery. *Canadian Journal of Neurological Sciences*, 31(2), 208–212. <https://doi.org/10.1017/S0317167100053841>
- Bijker, W. E., & Law, J. (Eds.). (1992). *Shaping technology, building society: Studies in sociotechnical change*. Cambridge, MA: MIT Press.
- Bijlsma-Frankema, K., & Costa, A. C. (2005). Understanding the trust-control nexus. *International Sociology*, 20(3), 259–282. <https://doi.org/10.1177/0268580905055477>
- Bijlsma-Frankema, K., Sitkin, S. B., & Weibel, A. (2015). Distrust in the balance: The emergence and development of intergroup distrust in a court of law. *Organization Science*, 26(4), 1018–1039. <https://doi.org/10.1287/orsc.2015.0977>
- Blau, P. M. (1964). *Exchange and power in social life*. New York, NY: John Wiley & Sons.
- Blockchain manager 1 at information technology company (2017, November 24). Interview by A. D. Palt [Audio file]. Germany.
- Blockchain manager 1 at information technology company (2018, January 18). Interview by A. D. Palt [Audio file]. Germany.
- Blockchain manager 2 at information technology company (2018, January 18). Interview by A. D. Palt [Audio file]. Germany.

- Blockchain manager at consulting company (2018a, March 23). Interview by A. D. Palt [Audio file]. Ireland.
- Blockchain manager at consulting company (2018b, March 27). Interview by A. D. Palt [Audio file]. Ireland (Skype).
- Blockchain manager at information technology and consulting company (2017, November 13). Interview by A. D. Palt [Audio file]. Germany (Skype).
- Blockchain reporter (2018, March 16). Interview by A. D. Palt [Audio file]. Ireland.
- Blue Horizon (n.d.a). Retrieved from <https://bluehorizon.network>
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238. <https://doi.org/10.1257/jep.29.2.213>
- Bowles, N. (2017, December 28). CryptoKitties, explained ... mostly. *The New York Times (NYTimes.com Feed)*. Retrieved from <https://www.nytimes.com/2017/12/28/style/cryptokitties-want-a-blockchain-snuggle.html>
- Brakeville, S. (2017a, March 2). Blockchain comes to SXSW with Hyperledger Fabric and IBM. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/03/blockchain-comes-sxsw-hyperledger-fabric-ibm/>
- Brakeville, S. (2017b, March 20). Highlights of the first blockchain hack at SXSW. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/03/highlights-of-the-first-blockchain-hack-at-sxsw/>
- Brill, J., Cuomo, J., Gopinath, R., Korsten, P., McDermott, B., McLean, J., . . . Wallis, J. (June 2016). *Fast forward: Rethinking enterprises, ecosystems and economies with blockchains*. Somers, NY. Retrieved from <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03757USEN>
- Brody, P., & Pureswaran, V. (September 2014). *Device democracy: Saving the future of the internet of things*. Somers, NY. Retrieved from https://www-03.ibm.com/press/de/de/attachment/45893.wss?fileId=ATTACH_FILE2&fileName=Device%20democracy-%20Saving%20the%20future%20of%20the%20Internet%20of%20Things.pdf
- Burning Billions: Tokens cents on the dollar against raised capital (2018, September 24). *Diar*. Retrieved from <https://diar.co/volume-2-issue-38/>
- Buterin, V. (2013a, September 20). Bootstrapping a decentralized autonomous corporation: Part I. *Bitcoin Magazine*. Retrieved from <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/>
- Buterin, V. (2013b, September 22). Bootstrapping an autonomous decentralized corporation, Part 2: Interacting with the world. *Bitcoin Magazine*. Retrieved from <https://bitcoinmagazine.com/articles/bootstrapping-an-autonomous-decentralized-corporation-part-2-interacting-with-the-world-1379808279/>
- Buterin, V. (2013c, September 25). Bootstrapping a decentralized autonomous corporation, Part 3: Identity corp. *Bitcoin Magazine*. Retrieved from <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-3-identity-corp-1380073003/>

- Buterin, V. (2014a, January 23). Ethereum: Now going public. Retrieved from <https://blog.ethereum.org/2014/01/23/ethereum-now-going-public/>
- Buterin, V. (2014b, January 29). Conference, alpha testnet and Ether pre-sale updates. Retrieved from <https://blog.ethereum.org/2014/01/29/conference-alpha-testnet-and-ether-pre-sale-updates/>
- Buterin, V. (2014c, February 24). DAOs are not scary, part 1: Self-enforcing contracts and factum law. Retrieved from <https://blog.ethereum.org/2014/02/24/daos-are-not-scary-part-1-self-enforcing-contracts-and-factum-law/>
- Buterin, V. (2014d, March 1). DAOs are not scary, part 2: Reducing barriers. Retrieved from <https://blog.ethereum.org/2014/03/01/daos-are-not-scary-part-2-reducing-barriers/>
- Buterin, V. (2014e, March 20). The latest EVM: “Ethereum is a trust-free closure system”. Retrieved from <https://blog.ethereum.org/2014/03/20/the-latest-evm-ethereum-is-a-trust-free-closure-system/>
- Buterin, V. (2014f, April 30). Decentralized protocol monetization and forks. Retrieved from <https://blog.ethereum.org/2014/04/30/decentralized-protocol-monetization-and-forks/>
- Buterin, V. (2014g, May 6). DAOs, DACs, DAs and more: An incomplete terminology guide. Retrieved from <https://blog.ethereum.org/2014/02/24/daos-are-not-scary-part-1-self-enforcing-contracts-and-factum-law/>
- Buterin, V. (2014h, July 22). Launching the Ether sale. Retrieved from <https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/>
- Buterin, V. (2014i, December 10). *White paper*. Retrieved from <https://github.com/ethereum/wiki/wiki/White-Paper/08e9d07781f50dac264314a551b5ba060a07c06a>
- Buterin, V. (2014j, December 26). Secret sharing DAOs: The other crypto 2.0. Retrieved from <https://blog.ethereum.org/2014/12/26/secret-sharing-daos-crypto-2-0/>
- Buterin, V. (2015a, January 23). Superrationality and DAOs. Retrieved from <https://blog.ethereum.org/2015/01/23/superrationality-daos/>
- Buterin, V. (2015b, April 13). Visions, part 1: The value of blockchain technology. Retrieved from <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>
- Buterin, V. (2015c, April 27). Visions, part 2: The problem of trust. Retrieved from <https://blog.ethereum.org/2015/04/27/visions-part-2-the-problem-of-trust/>
- Buterin, V. (2015d, May 9). Olympic: Frontier pre-release. Retrieved from <https://blog.ethereum.org/2015/05/09/olympic-frontier-pre-release/>
- Buterin, V. (2015e, July 5). On abstraction. Retrieved from <https://blog.ethereum.org/2015/07/05/on-abstraction/>
- Buterin, V. (2015f, August 7). On public and private blockchains. Retrieved from <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- Buterin, V. (2015g, October 18). Vitalik’s research and ecosystem update. Retrieved from <https://blog.ethereum.org/2015/10/18/vitaliks-research-and-ecosystem-update/>
- Buterin, V. (2016a, January 15). Privacy on the blockchain. Retrieved from <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/>

- Buterin, V. (2016b, May 9). On settlement finality. Retrieved from <https://blog.ethereum.org/2016/05/09/on-settlement-finality/>
- Buterin, V. (2016c, July 19). Consortium chain development. Retrieved from <https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development/59f07aa73a250dc7acb5a584ee24e4e3c29bc110>
- Buterin, V. (2016d, July 20). Hard fork completed. Retrieved from <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>
- Buterin, V. (2016e, December 4). Ethereum research update. Retrieved from <https://blog.ethereum.org/2016/12/04/ethereum-research-update/>
- Buterin, V. (2017, September 14). A prehistory of the Ethereum protocol. Retrieved from <https://vitalik.ca/general/2017/09/14/prehistory.html>
- Cachin, C. (July 2016). *Architecture of the Hyperledger blockchain fabric*. Rüschlikon, Switzerland. Retrieved from https://www.zurich.ibm.com/dclcl/papers/cachin_dccl.pdf
- Callon, M. (1986a). The sociology of an actor-network: The case of the electric vehicle. In M. Callon, J. Law, & A. Rip (Eds.), *Mapping the dynamics of science and technology: Sociology of science in the real world* (pp. 19–34). London, United Kingdom: Palgrave Macmillan. https://doi.org/10.1007/978-1-349-07408-2_2
- Callon, M. (1986b). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. In J. Law (Ed.), *Power, action and belief: A new sociology of knowledge?* (pp. 196–233). London, United Kingdom: Routledge & Kegan Paul.
- Callon, M., Law, J., & Rip, A. (Eds.). (1986). *Mapping the dynamics of science and technology: Sociology of science in the real world*. London, United Kingdom: Palgrave Macmillan.
- Campbell-Verduyn, M. (Ed.). (2018a). *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance*. New York, NY: Routledge.
- Campbell-Verduyn, M. (2018b). Introduction: What are blockchains and how are they relevant to governance in the contemporary global political economy? In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (pp. 1–24). New York, NY: Routledge.
- Campbell-Verduyn, M., & Goguen, M. (2018). Blockchains, trust and action nets: Extending the pathologies of financial globalization. *Global Networks*, 308–328. <https://doi.org/10.1111/glob.12214>
- Cassell, C., & Lee, B. (2017). Understanding translation work: The evolving interpretation of a trade union idea. *Organization Studies*, 38(8), 1085–1106. <https://doi.org/10.1177/0170840616670435>
- Chan, M. (2017, November 16). Devcon3!!! Retrieved from <https://blog.ethereum.org/2017/11/16/devcon3/>
- Chenard, J. (2018, April 3). Hyperledger Fabric now used in day to day operations. Retrieved from <https://www.hyperledger.org/blog/2018/04/03/hyperledger-fabric-now-used-in-day-to-day-operations>

- Child, J., & Möllering, G. (2003). Contextual confidence and active trust development in the Chinese business environment. *Organization Science*, 14(1), 69–80. <https://doi.org/10.1287/orsc.14.1.69.12813>
- Chua, W. F. (1995). Experts, networks and inscriptions in the fabrication of accounting images: A story of the representation of three public hospitals. *Accounting, Organizations and Society*, 20(2-3), 111–145. [https://doi.org/10.1016/0361-3682\(95\)95744-H](https://doi.org/10.1016/0361-3682(95)95744-H)
- Coindesk (n.d.a). Bitcoin price index. Retrieved from <https://www.coindesk.com/price/bitcoin>
- Coindesk (n.d.b). Ethereum price. Retrieved from <https://www.coindesk.com/price/ethereum>
- Coindesk (2018, July 11). *State of blockchain Q2 2018*. Retrieved from <https://www.coindesk.com/research/state-of-blockchain-q2-2018>
- Consensus Systems (n.d.). ConsenSys. Retrieved from <https://consensys.net/>
- Cook, K. S., & Kramer, R. M. (Eds.). (2004). *Trust and distrust in organizations: Dilemmas and approaches*. New York, NY: Russell Sage Foundation.
- Cornish, C. (2018, April 21). ‘I’m basically just floating everywhere’. *Financial Times*.
- Costa, A. C., & Bijlsma-Frankema, K. (2007). Trust and control interrelations: New perspectives on the trust-control nexus. *Group & Organization Management*, 32(4), 392–406. <https://doi.org/10.1177/1059601106293871>
- Crypto-investing: The DAO of accrue (2016, May 19). *The Economist*. Retrieved from <https://www.economist.com/finance-and-economics/2016/05/19/the-dao-of-accrue>
- CryptoKitties (n.d.a). *CryptoKitties: Collectible and breedable cats empowered by blockchain technology* (No. 2.0). Retrieved from https://drive.google.com/file/d/1soo-eAaJHzhw_XhFGMJp3VncQoM43byS/view
- CryptoKitties (n.d.b). CryptoKitties team. Retrieved from <https://www.cryptokitties.co/press>
- Cuomo, J. (2015a, September 21). Back on the chain gang. Retrieved from <https://developer.ibm.com/blockchain/2015/09/21/back-on-the-chain-gang/>
- Cuomo, J. (2015b, December 15). The force (of blockchain) awakens. Retrieved from <https://developer.ibm.com/blockchain/2015/12/15/the-force-awakens/>
- Cuomo, J. (2016, April 29). A case for permissioned access. Retrieved from <https://developer.ibm.com/blockchain/2016/04/29/a-case-for-permissioned-access/>
- Currall, S. C., & Inkpen, A. C. (2006). On the complexity of organizational trust: A multi-level co-evolutionary perspective and guideline for future research. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research* (235-246). Cheltenham, United Kingdom: Edward Elgar.
- Czarniawska, B. (2009). Emerging institutions: Pyramids or anthills? *Organization Studies*, 30(4), 423–441. <https://doi.org/10.1177/0170840609102282>
- Czarniawska, B., & Hernes, T. (Eds.). (2005). *Actor-network theory and organizing*. Malmö, Sweden: Liber.
- Czarniawska, B., & Sevón, G. (Eds.). (1996). *Translating organizational change*. Berlin, Germany: Walter de Gruyter.

- Czarniawska, B., & Sevón, G. (Eds.). (2005a). *Global ideas: How ideas, objects and practices travel in the global economy*. Malmö, Sweden: Liber.
- Czarniawska, B., & Sevón, G. (2005b). Translation is a vehicle, imitation its motor, and fashion sits at the wheel. In B. Czarniawska & G. Sevón (Eds.), *Global ideas: How ideas, objects and practices travel in the global economy* (pp. 7–12). Malmö, Sweden: Liber.
- Dallyn, S. (2017). Cryptocurrencies as market singularities: The strange case of Bitcoin. *Journal of Cultural Economy*, 10(5), 462–473. <https://doi.org/10.1080/17530350.2017.1315541>
- Dameron, M. (2018, April 3). *Beigepaper: An Ethereum technical specification*. Retrieved from <https://github.com/chronaeon/beigepaper/tree/ad4b1887191fc173151e670d8a0f0eacc833ae6>
- Das, T. K., & Teng, B.-S. (2001). Trust, control, and risk in strategic alliances: An integrated framework. *Organization Studies*, 22(2), 251–283. <https://doi.org/10.1177/0170840601222004>
- De Filippi, P. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production*. (9). Retrieved from <http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/>
- Del Castillo, M. (2016, May 19). Apache foundation founder named Hyperledger executive director. *Coindesk*. Retrieved from <https://www.coindesk.com/hyperledger-appoints-first-executive-director-apache>
- Deloitte Ireland (n.d.). Blockchain lab. Retrieved from <https://www2.deloitte.com/ie/en/pages/technology/topics/blockchain-lab.html>
- Demos, T. (2016, October 3). J.P. Morgan has a new twist on blockchain: The bank’s project is being built off the publicly accessible Ethereum network code. *The Wall Street Journal Online*. Retrieved from <https://www.wsj.com/articles/j-p-morgan-has-a-new-twist-on-blockchain-1475537138>
- Deutsch, M. (1973). *The resolution of conflict: Constructive and destructive processes*. New Haven, CT: Yale University Press.
- Diedrich, H. (2016). *Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations*: Wildfire Publishing.
- Dirks, K. T., Lewicki, R. J., & Zaheer, A. (2009). Repairing relationships within and between organizations: Building a conceptual foundation. *Academy of Management Review*, 34(1), 68–84. <https://doi.org/10.5465/AMR.2009.35713285>
- Dodd, N. (2018). The social life of Bitcoin. *Theory, Culture & Society*, 35(3), 35–56. <https://doi.org/10.1177/0263276417746464>
- Dudley, S. (2016, October 20). Blockchain @ Money20/20: Everything you need to know. Retrieved from <https://www.ibm.com/blogs/blockchain/2016/10/blockchain-money2020-everything-need-know/>
- Dudley, S. (2017a, January 16). FinTech Ideas Festival kicks off blockchain momentum in 2017. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/01/fintech-ideas-festival-kicks-off-blockchain-momentum-2017/>

- Dudley, S. (2017b, January 24). Why all the top blockchain developers will be in San Francisco next week. Retrieved from <https://developer.ibm.com/blockchain/2017/01/24/top-blockchain-developers-will-san-francisco-next-week/>
- DuPont, Q. (2014). The politics of cryptography: Bitcoin and the ordering machines. *Journal of Peer Production*. (4). Retrieved from <http://peer-production.net/is-sues/is-sue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bit-coin-and-the-ordering-machines>
- DuPont, Q. (2018). Experiments in algorithmic governance: A history and ethnography of “The DAO,” a failed decentralized autonomous organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (157-177). New York, NY: Routledge.
- DuPont, Q. (2019). *Cryptocurrencies and blockchains*. Cambridge: Polity.
- DuPont, Q., & Maurer, B. (2015, June 23). Ledgers and law in the blockchain. *King's Review*. Retrieved from <http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/>
- Dyer, J. H., & Chu, W. (2003). The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan, and Korea. *Organization Science*, 14(1), 57–68. <https://doi.org/10.1287/orsc.14.1.57.12806>
- Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, 14(1), 57–74. <https://doi.org/10.2307/258191>
- Enterprise Ethereum Alliance (n.d.b). Retrieved from <https://entethalliance.org/>
- Enterprise Ethereum Alliance (2017, February 28). *Newly formed enterprise collaboration drives Ethereum blockchain technology best practices focusing on security, privacy, scalability, and interoperability* [Press release]. New York, NY. Retrieved from <http://entethalliance.org/wp-content/uploads/2017/02/EEA.pdf>
- Ethereum (n.d.a). Ethereum: Blockchain app platform. Retrieved from <https://ethereum.org/>
- Ethereum (n.d.b). Ethereum: Playlists. Retrieved from <https://www.youtube.com/user/ethereumproject/playlists>
- Ethereum (2014a, May 11). *Ethereum London meetup: The Ethereum experience* [Video file]. London. Retrieved from <https://www.youtube.com/watch?v=GJGIeSCgskc>
- Ethereum (2014b, December 8). *Ethereum Devcon-0 - Gavin: Welcome! Our mission: Dapps* [Video file]. Berlin. Retrieved from https://www.youtube.com/watch?v=_BvvUIKDqp0
- Ethereum (2015a, November 25). *Devcon1: Microsoft announcing Ethereum blockchain as a service (ETH BaaS) on Azure cloud* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=ExsTb0iglcs&index=4&list=PLJqWcTqh_zKHQUFX4IaVjWjft2tbS4NVk
- Ethereum (2015b, December 14). *Devcon1: IBM MTN project - Henning Diedrich* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=_kTajbcAd9E&index=30&list=PLJqWcTqh_zKHQUFX4IaVjWjft2tbS4NVk

- Ethereum (2015c, December 21). *Devcon1: Smart bonds - UBS* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=5kKsouPSr1k&index=46&list=PLJqWcTqh_zKHQUFX4IaVjWjfT2tbS4NVk
- Ethereum (2016a, January 4). *Devcon1: Understanding the Ethereum blockchain protocol - Vitalik Buterin* [Video file]. London. Retrieved from <https://www.youtube.com/watch?v=gjwr-7PgpN8>
- Ethereum (2016b, January 8). *Devcon1: Rebuilding enterprise processes with blockchains and smart contracts - Deloitte* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=abyyK2-gtWQ&index=63&list=PLJqWcTqh_zKHQUFX4IaVjWjfT2tbS4NVk
- Ethereum (2016c, January 19). *Devcon1 panel: Banking with smart contracts* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=_4CACAZOoPI
- Ethereum community member (2018, March 19). Interview by A. D. Palt [Audio file]. Ireland.
- Ethereum Foundation (n.d.). Ethereum Foundation: Playlists. Retrieved from https://www.youtube.com/channel/UCNOFzGXD_C9YMYmnefmPH0g/playlists
- Ethereum Foundation (2015, December 11). *Devcon1: Ethereum for dummies - Dr. Gavin Wood* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=U_LK0t_qaPo&list=PLJqWcTqh_zKHQUFX4IaVjWjfT2tbS4NVk&index=27
- Ethereum Foundation (2016a, January 6). *Devcon1: Balance3 - triple entry accounting* [Video file]. London. Retrieved from https://www.youtube.com/watch?v=NEYTypMoQv0&list=PLJqWcTqh_zKHQUFX4IaVjWjfT2tbS4NVk&index=59
- Ethereum Foundation (2016b, October 10). *Devcon2: Ethereum in 25 Minutes* [Video file]. Shanghai. Retrieved from <https://www.youtube.com/watch?v=66SaEDzImP4>
- Ethereum team member 1 (2018, January 17). Interview by A. D. Palt [Audio file]. Brazil (Skype).
- Ethereum team member 2 (2018, January 24). Interview by A. D. Palt [Audio file]. United States (Skype).
- Faems, D., Janssens, M., Madhok, A., & van Looy, B. (2008). Toward an integrative perspective on alliance governance: Connecting contract design, trust dynamics, and contract application. *Academy of Management Journal*, 51(6), 1053–1078. <https://doi.org/10.5465/AMJ.2008.35732527>
- Ferris, C. (2017a, February 16). Recap: Dutch blockchain hackathon. Retrieved from <https://www.hyperledger.org/blog/2017/02/16/dutch-blockchain-hackathon>
- Ferris, C. (2017b, April 13). Blockchain at MIT: You don't learn with your mouth open. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/04/blockchain-mit-dont-learn-mouth-open/>
- Flick, U. (2004). Triangulation in qualitative research. In U. Flick, E. v. Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 178–183). London, United Kingdom: Sage.
- Flick, U., Kardorff, E. v., & Steinke, I. (2004). What is qualitative research? An introduction to the field. In U. Flick, E. v. Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 3–11). London, United Kingdom: Sage.

- Friedman, B., Kahn Jr., P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, 43(12), 34–40. <https://doi.org/10.1145/355112.355120>
- Fulmer, C. A., & Gelfand, M. J. (2012). At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management*, 38(4), 1167–1230. <https://doi.org/10.1177/0149206312439327>
- Gambetta, D. (1988). Can we trust trust? In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213–237). New York, NY: Basil Blackwell.
- Garfinkel, H. (2004). *Studies in ethnomethodology*. Cambridge, United Kingdom: Polity Press.
- Gargolinski, L. (2017, May 26). Going big and going global: IBM blockchain at Consensus. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/05/going-big-and-going-global-ibm-blockchain-at-consensus/>
- Gaur, N. (2017a, January 1). 7 principles for designing a blockchain network to power and sustain your business. Retrieved from <https://developer.ibm.com/blockchain/2017/01/01/7-principles-for-designing-a-blockchain-network-to-power-and-sustain-your-business/>
- Gaur, N. (2017b, May 11). Guidelines for blockchain adoption in the enterprise: How to compare frameworks. Retrieved from <https://developer.ibm.com/blockchain/2017/05/11/guidelines-blockchain-adoption-enterprise-compare-frameworks/>
- Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega*, 28(6), 725–737. [https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9)
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *Management Information Systems Quarterly*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- Gerring, T. (2014, August 18). Building the decentralized web 3.0. Retrieved from <https://blog.ethereum.org/2014/08/18/building-decentralized-web/>
- Gerring, T. (2016, February 9). Cut and try: Building a dream. Retrieved from <https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/>
- Ghaneei, K. (2016, April 27). Developerworks open tech talks. Retrieved from <https://developer.ibm.com/open/wp-content/uploads/sites/50/2016/06/Open-Blockchain-Transcript.pdf>
- Giddens, A. (1990). *The consequences of modernity*. Cambridge, United Kingdom: Polity Press.
- Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Stanford, CA: Stanford University Press.
- Giddens, A. (1994). Risk, trust, reflexivity. In U. Beck, A. Giddens, & S. Lash (Eds.), *Reflexive Modernization: Politics, tradition and aesthetics in the modern social order* (pp. 184–197). Cambridge, United Kingdom: Polity Press.
- Gillespie, N. (2015). Survey measures of trust in organizational contexts: An overview. In F. Lyon, G. Möllering, & M. N. K. Saunders (Eds.), *Handbook of research methods on trust* (2nd ed., pp. 225–239). Cheltenham, United Kingdom: Edward Elgar.

- Gillespie, N., & Dietz, G. (2009). Trust repair after an organization-level failure. *Academy of Management Review*, 34(1), 127–145. <https://doi.org/10.5465/AMR.2009.35713319>
- Gillespie, N., & Hurley, R. (2013). Trust and the global financial crisis. In R. Bachmann & A. Zaheer (Eds.), *Handbook of advances in trust research* (pp. 177–203). Cheltenham, United Kingdom: Edward Elgar.
- Gillespie, N., & Mann, L. (2004). Transformational leadership and shared values: The building blocks of trust. *Journal of Managerial Psychology*, 19(6), 588–607. <https://doi.org/10.1108/02683940410551507>
- Gillespie, N., & Siebert, S. (2018). Organizational trust repair. In R. Searle, A.-M. I. Nienaber, & S. B. Sitkin (Eds.), *The Routledge companion to trust* (pp. 284–301). New York, NY: Routledge.
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research. *Organizational Research Methods*, 16(1), 15–31. <https://doi.org/10.1177/1094428112452151>
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New York, NY: Aldine.
- Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 1543–1552). AISEL. Retrieved from https://aisel.aisnet.org/hicss-50/da/open_digital_services/4/
- Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin – asset or currency? Revealing users’ hidden intentions. In *22nd European Conference on Information Systems*, Tel Aviv, Israel. Retrieved from <https://aisel.aisnet.org/ecis2014/proceedings/track10/15/>
- Gray, M. (2015, November 9). Ethereum blockchain as a service now on Azure. Retrieved from <https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/>
- Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>
- Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). Edward Snowden: The whistleblower behind the NSA surveillance revelations. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>
- Greenwald, T. (2017, October 18). IBM says profit and sales drop. *The Wall Street Journal (U.S. Edition)*. Retrieved from <https://www.marketscreener.com/INTERNATIONAL-BUSINESS-MA-4828/news/IBM-Says-Profit-And-Sales-Drop-WSJ-25305174/>
- Greenwald, T. (2018, April 18). IBM logs more revenue, less profit. *The Wall Street Journal (U.S. Edition)*.
- Gunther, A. (2018, April 4). Collaboration: Unlocking decentralized, digital identity management through blockchain. Retrieved from <https://www.ibm.com/blogs/blockchain/2018/04/collaboration-unlocking-decentralized-digital-identity-management-through-blockchain/>
- Gupta, M. (2017). *Blockchain for dummies: IBM limited edition*. Hoboken, NJ: John Wiley & Sons.
- Hallam, G. (2014, December 5). DEVcon-0 recap. Retrieved from <https://blog.ethereum.org/2014/12/05/d%ce%bevcon-0-recap/>

- Hallam, G. (2016, June 14). The Ethereum foundation welcomes Microsoft as the premiere sponsor of Devcon2, Shanghai 19-21 September, 2016. Retrieved from <https://blog.ethereum.org/2016/06/14/ethereum-welcomes-microsoft-devcon/>
- Hamm, S. (2015, December 17). How blockchain will transform business and society. Retrieved from <https://www.ibm.com/blogs/think/2015/12/how-blockchain-will-transform-business-and-society/>
- Hardin, R. (2013). Government without trust. *Journal of Trust Research*, 3(1), 32–52. <https://doi.org/10.1080/21515581.2013.771502>
- Harris, J. D., Keevil, A. A. C., & Wicks, A. C. (2013). Public trust in the institution of business. In R. Bachmann & A. Zaheer (Eds.), *Handbook of advances in trust research* (pp. 204–223). Cheltenham, United Kingdom: Edward Elgar.
- Harris, J. D., Moriarty, B. T., & Wicks, A. C. (Eds.). (2014). *Public trust in business*. Cambridge, United Kingdom: Cambridge University Press.
- Harrison, K. (2017, July 17). Are you ready to take the topcoder challenge for blockchain? Retrieved from <https://developer.ibm.com/blockchain/2017/07/17/ready-take-topcoder-challenge-blockchain/>
- Harrison, K. (2018, March 2). Blockchain explained: Why it's not just about Bitcoin. Retrieved from <https://www.ibm.com/blogs/blockchain/2018/03/blockchain-explained-why-its-not-just-about-bitcoin/>
- Hart, P., & Saunders, C. (1997). Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization Science*, 8(1), 23–42. <https://doi.org/10.1287/orsc.8.1.23>
- Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, 29, 50–63. <https://doi.org/10.1016/j.elerap.2018.03.005>
- Haynes, M. (2017, April 11). The platform of the future: Blockchain at Payments 2017. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/04/platform-future-blockchain-payments-2017/>
- Haziot, L. (2018, February 7). Leveraging blockchain from transactions to returns. Retrieved from <https://www.ibm.com/blogs/blockchain/2018/02/leveraging-blockchain-from-transactions-to-returns/>
- Hedera Hashgraph (n.d.). Hedera Hashgraph platform. Retrieved from <https://www.hedera.com/platform>
- Hernes, T. (2005). The organization as a nexus of institutional macro actors: The story of a lopsided recruitment case. In B. Czarniawska & T. Hernes (Eds.), *Actor-network theory and organizing* (pp. 112–128). Malmö, Sweden: Liber.
- Hernes, T. (2010). Actor-network theory, Callon's scallops, and process-based organization studies. In S. Maitlis & T. Hernes (Eds.), *Process, sensemaking, and organizing* (pp. 161–184). Oxford, United Kingdom: Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199594566.003.0009>
- Higgins, S. (2015, January 17). IBM reveals proof of concept for blockchain-powered internet of things. *Coindesk*. Retrieved from <https://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/>

- Higgins, S. (2016, October 3). JP Morgan is quietly developing a private Ethereum blockchain. *Coindesk*. Retrieved from <https://www.coindesk.com/jpmorgan-ethereum-blockchain-quorum/>
- Hine, C. (1995). Representations of information technology in disciplinary development: Disappearing plants and invisible networks. *Science, Technology, & Human Values*, 20(1), 65–85. <https://doi.org/10.1177/016224399502000104>
- Hoffmann, H., & Söllner, M. (2014). Incorporating behavioral trust theory into system development for ubiquitous applications. *Personal and Ubiquitous Computing*, 18(1), 117–128. <https://doi.org/10.1007/s00779-012-0631-1>
- Höhmman, H.-H., & Welter, F. (Eds.). (2005). *Trust and entrepreneurship: A West-East perspective*. Cheltenham, United Kingdom: Edward Elgar.
- Holmström, J., & Robey, D. (2005). Inscribing organizational change with information technology. In B. Czarniawska & T. Hernes (Eds.), *Actor-network theory and organizing* (pp. 165–187). Malmö, Sweden: Liber.
- Homestead Documentation Initiative (n.d.a). Account management. Retrieved from <http://ethdocs.org/en/latest/account-management.html>
- Homestead Documentation Initiative (n.d.b). Ethereum Homestead documentation. Retrieved from <http://ethdocs.org/en/latest/index.html>
- Homestead Documentation Initiative (n.d.c). History of Ethereum. Retrieved from <http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>
- Homestead Documentation Initiative (n.d.d). The Homestead release. Retrieved from <http://ethdocs.org/en/latest/introduction/the-homestead-release.html>
- Homestead Documentation Initiative (n.d.e). Introduction. Retrieved from <http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>
- Homestead Documentation Initiative (n.d.f). Mining. Retrieved from <http://ethdocs.org/en/latest/mining.html>
- Homestead Documentation Initiative (n.d.g). Web 3: A platform for decentralized apps. Retrieved from <http://www.ethdocs.org/en/latest/introduction/web3.html>
- Homestead Documentation Initiative (n.d.h). What is Ethereum? Retrieved from <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>
- Hsieh, Y.-Y., Vergne, J.-P., & Wang, S. (2018). The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (48-68). New York, NY: Routledge.
- Huff, L., & Kelley, L. (2003). Levels of organizational trust in individualist versus collectivist societies: A seven-nation study. *Organization Science*, 14(1), 81–90. <https://doi.org/10.1287/orsc.14.1.81.12807>
- Hütten, M., & Thiemann, M. (2018). Moneys at the margins: From political experiment to cashless societies. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (pp. 25–47). New York, NY: Routledge.

- Hwang, H., & Suárez, D. (2005). Lost and found in the translation of strategic plans and websites. In B. Czarniawska & G. Sevón (Eds.), *Global ideas: How ideas, objects and practices travel in the global economy* (pp. 71–93). Malmö, Sweden: Liber.
- Hyperledger (n.d.a). Hyperledger Fabric: Contributions welcome! Retrieved from <https://hyperledger-fabric.readthedocs.io/en/release-1.2/CONTRIBUTING.html>
- Hyperledger (n.d.b). Hyperledger Fabric: Introduction. Retrieved from <https://hyperledger-fabric.readthedocs.io/en/release-1.2/whatis.html>
- Hyperledger (n.d.c). Hyperledger Fabric: Maintainers. Retrieved from <https://hyperledger-fabric.readthedocs.io/en/release-1.2/MAINTAINERS.html>
- Hyperledger (2017a, February 16). Hyperledger meetups – get involved in 2017! Retrieved from <https://www.hyperledger.org/blog/2017/02/16/hyperledger-meetups-get-involved-in-2017>
- Hyperledger (2017b, March 24). Recap: First Hyperledger Tokyo meetup sells out! Retrieved from <https://www.hyperledger.org/blog/2017/03/24/recap-first-hyperledger-tokyo-meetup-sells-out>
- Hyperledger (2017c, April 5). Developer showcase series: Hart Montgomery, research scientist in cryptography, Fujitsu. Retrieved from <https://www.hyperledger.org/blog/2017/04/05/developer-showcase-hart-montgomery-fujitsu>
- Hyperledger (2017d, April 11). Meet Hyperledger’s new security maven! Retrieved from <https://www.hyperledger.org/blog/2017/04/11/meet-hyperledgers-new-security-maven>
- Hyperledger (2017e, May 24). [Video] Hyperledger interviews Digital Asset’s CMO, Dan O’Prey. Retrieved from <https://www.hyperledger.org/blog/2017/05/24/video-hyperledger-interviews-digital-asset-holdings-cmo-dan-oprey>
- Hyperledger (2017f, July 11). Hyperledger announces production-ready Hyperledger Fabric 1.0. Retrieved from <https://www.hyperledger.org/announcements/2017/07/11/hyperledger-announces-production-ready-hyperledger-fabric-1-0>
- Hyperledger (August 2017g). *Hyperledger architecture, volume 1: Introduction to Hyperledger business blockchain design philosophy and consensus*. Retrieved from https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf
- Hyperledger (2017h, September 6). ABCs of open governance. Retrieved from <https://www.hyperledger.org/blog/2017/09/06/abcs-of-open-governance>
- Hyperledger (2017i, September 12). Meet the TSC: Arnaud Le Hors, IBM. Retrieved from <https://www.hyperledger.org/blog/2017/09/12/3431>
- Hyperledger (2017j, October 18). Hyperledger project update. Retrieved from <https://wiki.hyperledger.org/groups/tsc/project-updates/fabric-2017-oct>
- Hyperledger (2017k, November 6). Video: Hyperledger, a greenhouse for blockchain projects. Retrieved from <https://www.hyperledger.org/blog/2017/11/06/video-hyperledger-a-greenhouse-incubator-for-blockchain-projects>
- Hyperledger (2018a). Case Study: MonetaGo builds world’s first blockchain production network with Hyperledger Fabric. Retrieved from <https://www.hyperledger.org/resources/publications/monetago-case->

study?utm_source=hlsite&utm_medium=banner&utm_campaign=hlcasestudy&utm_content=mone
tago

Hyperledger (2018b, February 15). Developer showcase series: Todd Cooper & James Sloan, NuArca. Retrieved from <https://www.hyperledger.org/blog/2018/02/15/developer-showcase-series-todd-cooper-james-sloan-nuarca>

Hyperledger (March 2018c). *The Hyperledger vision: Blockchain 101, introducing Hyperledger, industry sse cases*. Retrieved from <https://www.hyperledger.org/wp-content/uploads/2018/03/The-Hyperledger-Vision-11-1.pdf>

Hyperledger (2018d, March 20). Hyperledger Fabric v1.1 released! Retrieved from <https://www.hyperledger.org/blog/2018/03/20/hyperledger-fabric-v1-1-released>

Hyperledger (2018e, April 5). Hyperledger project update. Retrieved from <https://wiki.hyperledger.org/groups/tsc/project-updates/fabric-2018-apr>

Hyperledger (2018f, April 18). Hyperledger meetup organizer's guide. Retrieved from <https://wiki.hyperledger.org/community/meetups?rev=1524083197>

Hyperledger (August 2018g). *An introduction to Hyperledger*. Retrieved from https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

IBM (n.d.). IBM blockchain. Retrieved from https://www.ibm.com/blockchain/services?cm_mmc=OSocial_Blog--Blockchain+and+Watson+Financial+Services_Blockchain--WW_WW--The+top+10+blockchain+skills+you+need+to+develop+In+Text+Services&cm_mmca1=000020YK&cm_mmca2=10005803&

IBM FinTech (2017, January 9). *Ginni Rometty's keynote at the FinTech Ideas Festival 2017* [Video file]. Retrieved from <https://www.youtube.com/watch?v=29PTBCpNND8&feature=youtu.be>

ICO advisor 1 (2018, March 22). Interview by A. D. Palt [Audio file]. Ireland.

ICO advisor 2 (2018, March 22). Interview by A. D. Palt [Audio file]. Ireland.

Iota Foundation (n.d.). What is IOTA? Retrieved from <https://www.iota.org/get-started/what-is-iota>

Isaeva, N., Bachmann, R., Bristow, A., & Saunders, M. N. K. (2015). Why the epistemologies of trust researchers matter. *Journal of Trust Research*, 5(2), 153–169. <https://doi.org/10.1080/21515581.2015.1074585>

James, W. (1948). *Essays in pragmatism*. New York, NY: Hafner Press.

James Jr., H. S. (2002). The trust paradox: A survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization*, 47(3), 291–307. [https://doi.org/10.1016/S0167-2681\(01\)00214-1](https://doi.org/10.1016/S0167-2681(01)00214-1)

Jeacle, I. (2003). Accounting and the construction of the standard body. *Accounting, Organizations and Society*, 28(4), 357–377. [https://doi.org/10.1016/S0361-3682\(02\)00021-1](https://doi.org/10.1016/S0361-3682(02)00021-1)

Jeacle, I. (2017). The popular pursuit of DIY: Exploring the role of calculative technologies in an actor network. *Management Accounting Research*, 35, 99–109. <https://doi.org/10.1016/j.mar.2016.01.004>

- Jeffries, F. L., & Reed, R. (2000). Trust and adaptation in relational contracting. *Academy of Management Review*, 25(4), 873–882. <https://doi.org/10.5465/AMR.2000.3707747>
- Jentsch, C. (2016, August 24). The history of the DAO and lessons learned. Retrieved from <https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5>
- Jones, C. T., & Dugdale, D. (2002). The ABC bandwagon and the juggernaut of modernity. *Accounting, Organizations and Society*, 27(1-2), 121–163. [https://doi.org/10.1016/S0361-3682\(01\)00035-6](https://doi.org/10.1016/S0361-3682(01)00035-6)
- Justesen, L., & Mouritsen, J. (2011). Effects of actor-network theory in accounting research. *Accounting, Auditing & Accountability Journal*, 24(2), 161–193. <https://doi.org/10.1108/09513571111100672>
- Kavanagh, D., Miscione, G., & Ennis, P. J. (2019). The Bitcoin game: Ethno-resonance as method. *Organization*, 26(4), 517–536. <https://doi.org/10.1177/1350508419828567>
- Kelley, J. (2018, March 29). How IBM is helping establish, evolve and extend blockchain networks. Retrieved from <https://www.ibm.com/blogs/blockchain/2018/03/how-ibm-is-helping-establish-evolve-and-extend-blockchain-networks/>
- Kiran, S. T. (2017a, March 17). Recap: Hyperledger’s first Hyderabad meetup. Retrieved from <https://www.hyperledger.org/blog/2017/03/17/recap-hyperledgers-first-hyderabad-meetup>
- Kiran, S. T. (2017b, May 30). Hyperledger Hyderabad meetup explores blockchain’s applicability to healthcare. Retrieved from <https://www.hyperledger.org/blog/2017/05/30/hyperledger-hyderabad-meetup-explores-blockchains-applicability-to-healthcare>
- Klein Woolthuis, R., Hillebrand, B., & Nooteboom, B. (2005). Trust, contract and relationship development. *Organization Studies*, 26(6), 813–840. <https://doi.org/10.1177/0170840605054594>
- Knights, D., Noble, F., Vurdubakis, T., & Willmott, H. (2001). Chasing shadows: Control, virtuality and the production of trust. *Organization Studies*, 22(2), 311–336. <https://doi.org/10.1177/0170840601222006>
- Knorr-Cetina, K. D. (1981). *The manufacture of knowledge: An essay on the constructivist and contextual nature of science*. Oxford, United Kingdom: Pergamon Press.
- Komiak, S. Y. X., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly*, 30(4), 941–960. <https://doi.org/10.2307/25148760>
- Kornberger, M., Pflueger, D., & Mouritsen, J. (2017). Evaluative infrastructures: Accounting for platform organization. *Accounting, Organizations and Society*, 60, 79–95. <https://doi.org/10.1016/j.aos.2017.05.002>
- Kozinets, R. V. (2015). *Netnography: Redefined* (2nd ed.). Los Angeles, CA: Sage.
- Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, 50, 569–98. <https://doi.org/10.1146/annurev.psych.50.1.569>
- Kramer, R. M. (2010). Trust barriers in cross-cultural negotiations: A social psychological analysis. In M. N. K. Saunders, D. Skinner, G. Dietz, N. Gillespie, & R. J. Lewicki (Eds.), *Organizational trust: A cultural perspective* (pp. 182–204). Cambridge, United Kingdom: Cambridge University Press.

- Kramer, R. M., & Lewicki, R. J. (2010). Repairing and enhancing trust: Approaches to reducing organizational trust deficits. *Academy of Management Annals*, 4(1), 245–277. <https://doi.org/10.1080/19416520.2010.487403>
- Krieger, D. J., & Belliger, A. (2014). *Interpreting networks: Hermeneutics, actor-network theory & new media*. Bielefeld, Germany: transcript Verlag.
- Lane, C. (1997). The social regulation of inter-firm relations in Britain and Germany: Market rules, legal norms and technical standards. *Cambridge Journal of Economics*, 21(2), 197–215. <https://doi.org/10.1093/oxfordjournals.cje.a013666>
- Lane, C. (1998). Introduction: Theories and issues in the study of trust. In C. Lane & R. Bachmann (Eds.), *Trust within and between organizations: Conceptual issues and empirical applications* (pp. 1–30). Oxford, United Kingdom: Oxford University Press.
- Lane, C., & Bachmann, R. (1996). The social constitution of trust: Supplier relations in Britain and Germany. *Organization Studies*, 17(3), 365–395. <https://doi.org/10.1177/017084069601700302>
- Lang, J. (2017, October 23). Three uses for blockchain in banking. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/10/three-uses-for-blockchain-in-banking/>
- Langfred, C. W. (2004). Too much of a good thing?: Negative effects of high trust and individual autonomy in self-managing teams. *Academy of Management Journal*, 47(3), 385–399. <https://doi.org/10.2307/20159588>
- Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust facebook?: Examining technology and interpersonal trust beliefs. *ACM SIGMIS Database*, 42(2), 32–54. <https://doi.org/10.1145/1989098.1989101>
- Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Milton Keynes, United Kingdom: Open University Press.
- Latour, B. (2002). *Aramis, or the love of technology* (4th ed.). Cambridge, MA: Harvard University Press.
- Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford, United Kingdom: Oxford University Press.
- Latour, B., & Woolgar, S. (1979). *Laboratory life: The social construction of scientific facts*. Beverly Hills, CA: Sage.
- Law, J., & Callon, M. (1992). The life and death of an aircraft: A network analysis of technical change. In W. E. Bijker & J. Law (Eds.), *Shaping technology, building society: Studies in sociotechnical change* (pp. 21–52). Cambridge, MA: MIT Press.
- Lee, J. D., & Moray, N. (1992). Trust, control strategies and allocation of function in human-machine systems. *Ergonomics*, 35(10), 1243–1270. <https://doi.org/10.1080/00140139208967392>
- Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, 46(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392
- Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 114–139). Thousand Oaks, CA: Sage.

- Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review*, 23(3), 438–458. <https://doi.org/10.5465/amr.1998.926620>
- Li, P. P. (2013). Inter-cultural trust and trust-building: The contexts and strategies of adaptive learning in acculturation. In R. Bachmann & A. Zaheer (Eds.), *Handbook of advances in trust research* (pp. 146–173). Cheltenham, United Kingdom: Edward Elgar.
- Li, P. P. (2017). The time for transition: Future trust research. *Journal of Trust Research*, 7(1), 1–14. <https://doi.org/10.1080/21515581.2017.1293772>
- Lieber, A. (2017, March 9). Trust in trade: Announcing a new blockchain partner. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/03/trust-trade-announcing-new-blockchain-partner/>
- The Linux Foundation (2015, December 17). *Linux foundation unites industry leaders to advance blockchain technology: New open ledger project to transform the way business transactions are conducted around the world* [Press release]. San Francisco, CA. Retrieved from <https://www.linuxfoundation.org/press-release/2015/12/linux-foundation-unites-industry-leaders-to-advance-blockchain-technology/#.WZ8FmCiG>
- The Linux Foundation (2017, July 11). Hyperledger announces production-ready Hyperledger Fabric 1.0. Retrieved from <https://www.hyperledger.org/announcements/2017/07/11/hyperledger-announces-production-ready-hyperledger-fabric-1-0>
- Locke, J., & Lowe, A. (2007). A biography: Fabrications in the life of an ERP package. *Organization*, 14(6), 793–814. <https://doi.org/10.1177/1350508407082263>
- Lowry, E. (2017a, July 24). Rethink financial services with IBM blockchain at Distributed: Trade. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/07/rethink-financial-services-with-blockchain-at-distributed-trade/>
- Lowry, E. (2017b, August 7). Top learnings about blockchain for supply chain at Distributed: Trade. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/08/top-learnings-about-blockchain-for-supply-chain-at-distributed-trade/>
- Lowry, E. (2017c, August 14). Business value of blockchain: Webcast preview. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/08/business-value-of-blockchain-webcast-preview/>
- Lowry, E. (2017d, October 31). Trick or treat? Use blockchain to purge your business of horrors. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/10/trick-or-treat-use-blockchain-to-purge-your-business-of-horrors/>
- Lucas, M. (2016, September 13). What do Pokémon Go and blockchain have in common? Retrieved from <https://developer.ibm.com/blockchain/2016/09/13/pokemon-go-blockchain-common/>
- Luce, R. D., & Raiffa, H. (1967). *Games and decisions* (7th ed.). New York, NY: Wiley.
- Luhmann, N. (1979). *Trust and power*. Chichester, United Kingdom: John Wiley & Sons.
- Lustig, C., & Nardi, B. (2015). Algorithmic authority: The case of Bitcoin. In *Proceedings of the 48th Hawaii International Conference on System Sciences* (pp. 743–752). Kauai, HI: IEEE. <https://doi.org/10.1109/HICSS.2015.95>

- Lynn, T., van der Werff, L., Hunt, G., & Healy, P. (2016). Development of a cloud trust label: A delphi approach. *Journal of Computer Information Systems*, 56(3), 185–193. <https://doi.org/10.1080/08874417.2016.1153887>
- Lyon, F., Möllering, G., & Saunders, M. N. K. (2015). Introduction. Researching trust: The ongoing challenge of matching objectives and methods. In F. Lyon, G. Möllering, & M. N. K. Saunders (Eds.), *Handbook of research methods on trust* (2nd ed., pp. 1–22). Cheltenham, United Kingdom: Edward Elgar.
- Lyon, F., & Porter, G. (2010). Evolving institutions of trust: Personalized and institutional bases of trust in Nigerian and Ghanaian food trading. In M. N. K. Saunders, D. Skinner, G. Dietz, N. Gillespie, & R. J. Lewicki (Eds.), *Organizational trust: A cultural perspective* (pp. 255–278). Cambridge, United Kingdom: Cambridge University Press.
- Macdonald, M., Liu-Thorrold, L., & Julien, R. (2017, February 3). *The blockchain: A comparison of platforms and their uses beyond Bitcoin*. Queensland, Australia. Retrieved from COMS4507 - Advances Computer and Network Security website: <https://www.researchgate.net/publication/313249614> <https://doi.org/10.13140/RG.2.2.23274.52164>
- Malhotra, D., & Murnighan, J. K. (2002). The effects of contracts on interpersonal trust. *Administrative Science Quarterly*, 47(3), 534–559. <https://doi.org/10.2307/3094850>
- Mallard, A., Méadel, C., & Musiani, F. (2014). The paradoxes of distributed trust: Peer-to-peer architecture and user confidence in Bitcoin. *Journal of Peer Production*. (4), 1–10. Retrieved from <https://hal-mines-paristech.archives-ouvertes.fr/hal-00985707>
- Maurer, B., Nelms, T. C., & Swartz, L. (2013). “When perhaps the real problem is money itself!”: The practical materiality of Bitcoin. *Social Semiotics*, 23(2), 261–277. <https://doi.org/10.1080/10350330.2013.777594>
- Mauri, R. (2017, September 19). Three features of blockchain that help prevent fraud. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/09/three-features-of-blockchain-that-help-prevent-fraud/>
- Mayer, R. C. (2013). Trust. In E. H. Kessler (Ed.), *Encyclopedia of management theory* (pp. 904–907). Los Angeles, CA: Sage.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management*, 20(3), 709–734. <https://doi.org/10.2307/258792>
- McEvily, B., Perrone, V., & Zaheer, A. (2003). Trust as an organizing principle. *Organization Science*, 14(1), 91–103. <https://doi.org/10.1287/orsc.14.1.91.12814>
- McKneally, M. F., Ignagni, E., Martin, D. K., & D’Cruz, J. (2004). The leap to trust: Perspective of cholecystectomy patients on informed decision making and consent. *Journal of the American College of Surgeons*, 199(1), 51–57. <https://doi.org/10.1016/j.jamcollsurg.2004.02.021>
- McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, 2(2), 1–25. <https://doi.org/10.1145/1985347.1985353>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002a). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>

- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002b). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems*, 11(3-4), 297–323. [https://doi.org/10.1016/S0963-8687\(02\)00020-3](https://doi.org/10.1016/S0963-8687(02)00020-3)
- McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, 23(3), 473–490. <https://doi.org/10.2307/259290>
- McWaters, R. J. (June 2015). *The future of financial services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed*. Retrieved from http://www3.weforum.org/docs/WEF_The_future_of_financial_services.pdf
- McWaters, R. J. (August 2016). *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*. Retrieved from http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
- Meyerson, D., Weick, K. E., & Kramer, R. M. (1996). Swift trust and temporary groups. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 166–195). Thousand Oaks, CA: Sage.
- Mims, C. (2018, March 12). Keywords: Blockchain has power to transform. *The Wall Street Journal (U.S. Edition)*.
- Möhlmann, M. (2015). Collaborative consumption: Determinants of satisfaction and the likelihood of using a sharing economy option again. *Journal of Consumer Behaviour*, 14(3), 193–207. <https://doi.org/10.1002/cb.1512>
- Möhlmann, M. (2016, September 2). *Digital trust and peer-to-peer collaborative consumption platforms: A mediation analysis*. <https://doi.org/10.2139/ssrn.2813367>
- Möhlmann, M., & Geissinger, A. (2018). Trust in the sharing economy: Platform-mediated peer trust. In N. M. Davidson, M. Finck, & J. J. Infranca (Eds.), *The Cambridge handbook of the law of the sharing economy* (pp. 27–37). Cambridge, United Kingdom: Cambridge University Press.
- Möllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology*, 35(2), 403–420. <https://doi.org/10.1017/S0038038501000190>
- Möllering, G. (2005). The trust/control duality: An integrative perspective on positive expectations of others. *International Sociology*, 20(3), 283–305. <https://doi.org/10.1177/0268580905055478>
- Möllering, G. (2006a). *Trust: Reason, routine, reflexivity*. Amsterdam, Netherlands: Elsevier.
- Möllering, G. (2006b). Trust, institutions, agency: Towards a neoinstitutional theory of trust. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research* (pp. 355–376). Cheltenham, United Kingdom: Edward Elgar.
- Möllering, G. (2011). Vernebeltes Vertrauen? Cloud Computing aus Sicht der Vertrauensforschung. In A. Picot, U. Hertz, & T. Götz (Eds.), *Trust in IT: Wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?* (pp. 39–47). Berlin, Germany: Springer. https://doi.org/10.1007/978-3-642-18110-8_4
- Möllering, G., Bachmann, R., & Hee Lee, S. (2004). Introduction: Understanding organizational trust – foundations, constellations, and issues of operationalisation. *Journal of Managerial Psychology*, 19(6), 556–570. <https://doi.org/10.1108/02683940410551480>

- Mougayar, W. (2015, May 24). The business imperative behind the Ethereum vision. Retrieved from <https://blog.ethereum.org/2015/05/24/the-business-imperative-behind-the-ethereum-vision/>
- Mougayar, W. (2016). *The business blockchain: Promise, practice, and application of the next internet technology*. Hoboken, NJ: John Wiley & Sons.
- Moulds, J. (2018, January 15). Blockchain tracks food all the way from farm to table. *The Times*. Retrieved from <https://www.thetimes.co.uk/article/blockchain-tracks-food-all-the-way-from-farm-to-table-dz9s2zv32>
- Mouritsen, J., & Thrane, S. (2006). Accounting, network complementarities and the development of inter-organisational relations. *Accounting, Organizations and Society*, 31(3), 241–275. <https://doi.org/10.1016/j.aos.2005.04.002>
- Mulligan, C., Zhu Scott, J., Warren, S., & Rangaswami, J. P. (April 2018). *Blockchain beyond the hype: A practical framework for business leaders*. Retrieved from http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf
- Musiani, F., Mallard, A., & Méadel, C. (2018). Governing what wasn't meant to be governed: A controversy-based approach to the study of Bitcoin governance. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (pp. 133–156). New York, NY: Routledge.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- Nelms, T. C., Maurer, B., Swartz, L., & Mainwaring, S. (2018). Social payments: Innovation, trust, Bitcoin, and the sharing economy. *Theory, Culture & Society*, 35(3), 13–33. <https://doi.org/10.1177/0263276417746466>
- Nooteboom, B. (1996). Trust, opportunism and governance: A process and control model. *Organization Studies*, 17(6), 985–1010. <https://doi.org/10.1177/017084069601700605>
- Nooteboom, B. (2002). *Trust: Forms, foundations, functions, failures and figures*. Cheltenham, United Kingdom: Edward Elgar.
- Nooteboom, B. (2006). [Book review] Trust: Reason, routine, reflexivity, by G. Möllering. *Organization Studies*, 27(12), 1907–1910. <https://doi.org/10.1177/0170840606074945>
- Nooteboom, B. (2013). Trust and innovation. In R. Bachmann & A. Zaheer (Eds.), *Handbook of advances in trust research* (pp. 106–121). Cheltenham, United Kingdom: Edward Elgar.
- Norén, L., & Ranerup, A. (2005). The internet web portal as an enrolment device. In B. Czarniawska & T. Hernes (Eds.), *Actor-network theory and organizing* (pp. 188–207). Malmö, Sweden: Liber.
- Notheisen, B., Cholewa, J. B., & Shanmugam, A. P. (2017). Trading real-world assets on blockchain: An application of trust-free transaction systems in the market for lemons. *Business & Information Systems Engineering*, 59(6), 425–440. <https://doi.org/10.1007/s12599-017-0499-8>
- O'Leary, R. R. (2017, October 11). The Byzantium countdown: What's left before Ethereum's next fork? *Coindesk*. Retrieved from <https://www.coindesk.com/byzantium-countdown-whats-left-ethereums-next-fork>

- O'Mahoney, J., O'Mahoney, H., & Al-Amoudi, I. (2017). How can the loggerhead sea-turtle survive?: Exploring the journeys of the *Caretta caretta* using ANT and critical realism. *Organization*, 24(6), 781–799. <https://doi.org/10.1177/1350508416672738>
- Oregui, J., & Kumar, K. (2017, November 29). Build it on blockchain: A sustainable palm oil industry. Retrieved from <https://www.hyperledger.org/blog/2017/11/29/build-it-on-blockchain-a-sustainable-palm-oil-industry>
- Ortmann, G. (2004). *Als ob: Fiktionen und Organisationen*. Wiesbaden, Germany: VS Verlag für Sozialwissenschaften.
- Palfreyman, J. (2016a, September 3). Lessons from one year on the (block)chain gang! Retrieved from <https://developer.ibm.com/blockchain/2016/10/03/lessons-from-one-year-on-the-blockchain-gang/>
- Palfreyman, J. (2016b, September 20). Privacy services & blockchain. Retrieved from <https://developer.ibm.com/blockchain/2016/09/20/privacy-services-blockchain/>
- Panetta, K. (2017, August 15). Top trends in the Gartner hype cycle for emerging technologies, 2017. Retrieved from <https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/>
- Panetta, K. (2018, August 16). 5 trends emerge in the Gartner hype cycle for emerging technologies, 2018. Retrieved from <https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/>
- Parity Technologies (n.d.). Parity. Retrieved from <https://www.parity.io/>
- Pavlou, P. A., & Dimoka, A. (2006). The Nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation. *Information Systems Research*, 17(4), 392–414. <https://doi.org/10.1287/isre.1060.0106>
- Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37–59. <https://doi.org/10.1287/isre.1040.0015>
- Peirce, C. S. (1998). Volume 1: Principles of philosophy. In C. Hartshorne & P. Weiss (Eds.), *Collected papers of Charles Sanders Peirce*. Bristol, United Kingdom: Thoemmes Press.
- Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking beyond banks and money: A guide to banking services in the twenty-first century* (pp. 239–278). Cham, Switzerland: Springer.
- Plesner, U. (2014). Virtual worlds as emerging cyber-hybrids: Accounting for the travel between research sites with actor-network theory. In U. Plesner & L. Phillips (Eds.), *Researching virtual worlds: Methodologies for studying emergent practices* (pp. 16–33). New York, NY: Routledge.
- Plesner, U., & Phillips, L. (2014a). Introduction: Approaching the study of virtual worlds. In U. Plesner & L. Phillips (Eds.), *Researching virtual worlds: Methodologies for studying emergent practices* (pp. 1–15). New York, NY: Routledge.
- Plesner, U., & Phillips, L. (Eds.). (2014b). *Researching virtual worlds: Methodologies for studying emergent practices*. New York, NY: Routledge.
- Popper, N. (2016, October 14). Liking Bitcoin's technology, if not Bitcoin. *The New York Times*.

- Popper, N. (2017, October 1). Understanding Ethereum, Bitcoin's virtual cousin. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/10/01/technology/what-is-ethereum.html>
- Popper, N., & Lohr, S. (2017a, March 4). Blockchain: A better way to track pork chops, bonds, bad peanut butter? *International New York Times*. Retrieved from <https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html>
- Popper, N., & Lohr, S. (2017b, March 5). IBM bets big on the arcane idea behind Bitcoin. *The New York Times*.
- The promise of the blockchain: The trust machine (2015, October 31). *The Economist*. Retrieved from <https://www.economist.com/leaders/2015/10/31/the-trust-machine>
- Quattrone, P., & Hopper, T. (2005). A 'time-space odyssey': Management control systems in two multinational organisations. *Accounting, Organizations and Society*, 30(7-8), 735–764. <https://doi.org/10.1016/j.aos.2003.10.006>
- Rampen, J. (2016, October 9). Hyperledger hackathon and hackfest recap. Retrieved from <https://www.hyperledger.org/blog/2016/10/09/hyperledger-hackathon-and-hackfest-recap>
- Ratnasingam, P. (2005). Trust in inter-organizational exchanges: A case study in business to business electronic commerce. *Decision Support Systems*, 39(3), 525–544. <https://doi.org/10.1016/j.dss.2003.12.005>
- Reichertz, J. (2004). Abduction, deduction and induction in qualitative research. In U. Flick, E. v. Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 159–164). London, United Kingdom: Sage.
- Reitwiessner, C. (2016, November 9). Analysis of storage corruption bug. Retrieved from <https://blog.ethereum.org/2016/11/09/analysis-storage-corruption-bug/>
- Richer, T. (2017a, February 28). Top 5 blockchain sessions for developers at Interconnect. Retrieved from <https://developer.ibm.com/blockchain/2017/02/28/top-5-blockchain-sessions-developers-interconnect/>
- Richer, T. (2017b, April 21). From concept to production: Getting real with blockchain at Consensus. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/04/blockchain-is-real-at-consensus-2017/>
- Ripple (n.d.). Ripple. Retrieved from <https://ripple.com/>
- Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering*, 59(6), 385–409. <https://doi.org/10.1007/s12599-017-0506-0>
- Robson, K., & Bottausci, C. (2018). The sociology of translation and accounting inscriptions: Reflections on Latour and accounting research. *Critical Perspectives on Accounting*, 54, 60–75. <https://doi.org/10.1016/j.cpa.2017.11.003>
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404. <https://doi.org/10.5465/amr.1998.926617>
- Rückeshäuser, N. (2017). Do we really want blockchain-based accounting?: Decentralized consensus as enabler of management override of internal controls. In J. M. Leimeister & W. Brenner (Eds.),

- Proceedings of the 13th International Conference on Wirtschaftsinformatik* (pp. 16–30). St. Gallen, Switzerland.
- Sahlin-Andersson, K., & Engwall, L. (Eds.). (2002). *The expansion of management knowledge: Carriers, flows, and sources*. Stanford, CA: Stanford Business Books.
- Sahlin-Andersson, K. (2006). Corporate social responsibility: A trend and a movement, but of what and for what? *Corporate Governance*, 6(5), 595–608. <https://doi.org/10.1108/14720700610706081>
- Sako, M. (1998). Does trust improve business performance? In C. Lane & R. Bachmann (Eds.), *Trust within and between organizations: Conceptual issues and empirical applications* (pp. 88–117). Oxford, United Kingdom: Oxford University Press.
- Saunders, M. N. K., Dietz, G., & Thornhill, A. (2014). Trust and distrust: Polar opposites, or independent but co-existing? *Human Relations*, 67(6), 639–665. <https://doi.org/10.1177/0018726713500831>
- Saunders, M. N. K., Skinner, D., Dietz, G., Gillespie, N., & Lewicki, R. J. (Eds.). (2010). *Organizational trust: A cultural perspective*. Cambridge, United Kingdom: Cambridge University Press.
- Schütz, A. (1970). *Reflections on the problem of relevance*. New Haven, CT: Yale University Press.
- Searle, R., Nienaber, A.-M. I., & Sitkin, S. B. (Eds.). (2018). *The Routledge companion to trust*. New York, NY: Routledge.
- Seligman, A. B. (1997). *The problem of trust*. Princeton, NJ: Princeton University Press.
- Sharma, U. (2017, December 8). Blockchain is good for your health, and your business. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-good-health-business/>
- Shaw, G. (2017, September 19). *Nettitude excellence as standard: Security assessment management report* (No. 1.1). Retrieved from Nettitude website: https://wiki.hyperledger.org/_media/security/management_report_linux_foundation_fabric_august_2017_v1.1.pdf
- Sheppard, B. H., & Sherman, D. M. (1998). The grammars of trust: A model and general implications. *Academy of Management Review*, 23(3), 422–437. <https://doi.org/10.2307/259287>
- Shugol, A., & Stamou Fotini (2017, March 20). Recap: Hyperledger London meetup – reviewing success, discussing the future. Retrieved from <https://www.hyperledger.org/blog/2017/03/20/recap-hyperledger-london-meetup-reviewing-success-discussing-the-future>
- SiliconANGLE theCUBE (2017, March 22). *Ramesh Gopinath | IBM Interconnect 2017* [Video file]. Retrieved from <https://www.youtube.com/watch?v=CxSFVJa9uxc&feature=youtu.be&list=PLenh213llmcZTJLJM AurMJkVnYBY4wLhw>
- Simmel, G. (Ed.). (1950). *The sociology of Georg Simmel*. New York, NY: Free Press.
- Simmel, G. (2004). *The philosophy of money* (3rd ed.). London, United Kingdom: Routledge.
- Six, F. (2005). *The trouble with trust*. Cheltenham, United Kingdom: Edward Elgar.
- Skinner, D., Dietz, G., & Weibel, A. (2013). The dark side of trust: When trust becomes a ‘poisoned chalice’. *Organization*, 21(2), 206–224. <https://doi.org/10.1177/1350508412473866>

- Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, 25(3), 274–287. <https://doi.org/10.1057/ejis.2015.17>
- Söllner, M., Pavlou, P. A., & Leimeister, J. M. (2013). Understanding trust in IT artifacts: A new conceptual approach. In *73rd Annual Meeting of the Academy of Management*, Orlando, FL. Retrieved from <https://journals.aom.org/doi/10.5465/ambpp.2013.11412abstract>
- Sridharan, M. (2017, June 5). Hyperledger Frankfurt meetup recap. Retrieved from <https://www.hyperledger.org/blog/2017/06/05/hyperledger-frankfurt-meetup-recap>
- State of the DApps (n.d.). State of the Dapps. Retrieved from <https://www.stateofthedapps.com/>
- Steiner, J. (2014, December 18). A call to all the bug bounty hunters out there... Retrieved from <https://blog.ethereum.org/2014/12/18/call-bug-bounty-hunters/>
- Steiner, J. (2015, March 20). Jutta's update on bug bounty program and security audit. Retrieved from <https://blog.ethereum.org/2015/03/20/juttas-update-bug-bounty-program-security-audit/>
- Stevens, M., MacDuffie, J. P., & Helper, S. (2015). Reorienting and recalibrating inter-organizational relationships: Strategies for achieving optimal trust. *Organization Studies*, 36(9), 1237–1264. <https://doi.org/10.1177/0170840615585337>
- Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization Science*, 14(1), 5–17. <https://doi.org/10.1287/orsc.14.1.5.12810>
- Stowell, P. (2018, January 30). Come for the happy hour, stay for the skills at Index – San Francisco. Retrieved from <https://developer.ibm.com/blockchain/2018/01/30/come-happy-hour-stay-skills-index-san-francisco/>
- Sundararajan, A. (2016). *The sharing economy: The end of employment and the rise of crowd-based capitalism*. Cambridge, MA: The MIT Press.
- Swartz, L. (2017). Blockchain dreams: Imagining techno-economic alternatives after Bitcoin. In M. Castells (Ed.), *Another economy is possible: Culture and economy in a time of crisis* (pp. 82–105). Cambridge, United Kingdom: Polity.
- Swartz, L. (2018). What was Bitcoin, what will it be?: The techno-economic imaginaries of a new money technology. *Cultural Studies*, 32(4), 623–650. <https://doi.org/10.1080/09502386.2017.1416420>
- Sydow, J. (1998). Understanding the constitution of interorganizational trust. In C. Lane & R. Bachmann (Eds.), *Trust within and between organizations: Conceptual issues and empirical applications* (pp. 31–63). Oxford, United Kingdom: Oxford University Press.
- Sydow, J. (2006). How can systems trust systems? A structuration perspective on trust-building in inter-organizational relations. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research* (pp. 377–392). Cheltenham, United Kingdom: Edward Elgar.
- Sydow, J., & Windeler, A. (1998). Organizing and evaluating interfirm networks: A structurationist perspective on network processes and effectiveness. *Organization Science*, 9(3), 265–284. <https://doi.org/10.1287/orsc.9.3.265>

- Szabo, N. (1994). *Smart contracts*. Retrieved from <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- Szabo, N. (1997). *The idea of smart contracts*. Retrieved from <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>
- Tapscott, D., & Tapscott, A. (2016a). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. New York, NY: Penguin.
- Tapscott, D., & Tapscott, A. (2016b, May 10). The impact of the blockchain goes beyond financial services. *Harvard Business Review*. Retrieved from <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services>
- Thatcher, J. B., Loughry, M. L., Lim, J., & McKnight, D. H. (2007). Internet anxiety: An empirical study of the effects of personality, beliefs, and social support. *Information & Management*, 44(4), 353–363. <https://doi.org/10.1016/j.im.2006.11.007>
- Tillmar, M., & Lindkvist, L. (2007). Cooperation against all odds: Finding reasons for trust where formal institutions fail. *International Sociology*, 22(3), 343–366. <https://doi.org/10.1177/0268580907076575>
- Tremayne, M. (2013). Anatomy of protest in the digital era: A network analysis of Twitter and occupy wall street. *Social Movement Studies*, 13(1), 110–126. <https://doi.org/10.1080/14742837.2013.830969>
- Tual, S. (2014, November 3). Ethereum community and adoption update – week 1. Retrieved from <https://blog.ethereum.org/2014/11/03/stephans-ethereum-community-adoption-update-week-1/>
- Tual, S. (2015a, July 22). Frontier is coming – what to expect, and how to prepare. Retrieved from <https://blog.ethereum.org/2015/07/22/frontier-is-coming-what-to-expect-and-how-to-prepare/>
- Tual, S. (2015b, August 4). The thawing Frontier. Retrieved from <https://blog.ethereum.org/2015/08/04/the-thawing-frontier/>
- Tual, S. (2015c, September 3). A message from Stephan Tual. Retrieved from <https://blog.ethereum.org/2015/09/03/a-message-from-stephan-tual/>
- Uslaner, E. M. (2014). The economic crisis of 2008, trust in government, and generalized trust. In J. D. Harris, B. T. Moriarty, & A. C. Wicks (Eds.), *Public trust in business* (pp. 19–50). Cambridge, United Kingdom: Cambridge University Press.
- Valenta, M., & Sandner, P. (June 2017). *Comparison of Ethereum, Hyperledger Fabric and Corda*. Frankfurt am Main. Retrieved from http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf
- Van de Sande, A. (2015, December 3). Ethereum in practice part 1: How to build your own cryptocurrency without touching a line of code. Retrieved from <https://blog.ethereum.org/2015/12/03/how-to-build-your-own-cryptocurrency/>
- Van de Sande, A. (2016, July 12). How to build server less applications for Mist. Retrieved from <https://blog.ethereum.org/2016/07/12/build-server-less-applications-mist/>

- Van der Werff, L., Real, C., & Lynn, T. (2018). Individual trust and the internet. In R. Searle, A.-M. I. Nienaber, & S. B. Sitkin (Eds.), *The Routledge companion to trust* (391-407). New York, NY: Routledge.
- Van Rijmenam, M., Schweitzer, J., & Williams, M.-A. (2017). A distributed future: How blockchain affects strategic management, organisation design & governance. In *77th Annual Meeting of the Academy of Management*, Atlanta, GA. Retrieved from <https://journals.aom.org/doi/10.5465/AMBPP.2017.14807abstract>
- Voß, O. (2016, July 5). Blockchain: Wie Hacker um eine Zukunftstechnologie kämpfen. *WirtschaftsWoche Online*. Retrieved from <http://www.wiwo.de/unternehmen/banken/blockchain/blockchain-wie-hacker-um-eine-zukunftstechnologie-kaempfen/13834276.html>
- Walgenbach, P. (2001). The production of distrust by means of producing trust. *Organization Studies*, 22(4), 693–714. <https://doi.org/10.1177/0170840601224006>
- Wallis, J. (2017, October 26). Beyond proof of concept: Blockchain highlights from Sibos 2017. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/10/beyond-proof-of-concept-blockchain-highlights-from-sibos-2017/>
- Wang, W., & Benbasat, I. (2005). Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems*, 6(3), 72–101. <https://doi.org/10.17705/1jais.00065>
- Wang, W., & Benbasat, I. (2007). Recommendation agents for electronic commerce: Effects of explanation facilities on trusting beliefs. *Journal of Management Information Systems*, 23(4), 217–246. <https://doi.org/10.2753/MIS0742-1222230410>
- Weber, B. (2016). Bitcoin and the legitimacy crisis of money. *Cambridge Journal of Economics*, 40(1), 17–41. <https://doi.org/10.1093/cje/beu067>
- Wedgwood, K. (2017, June 29). Thought leaders reimagine their industries at blockchain summit. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/06/thought-leaders-reimagine-industries-blockchain-summit/>
- Weick, K. E. (1989). Theory construction as disciplined imagination. *Academy of Management Review*, 14(4), 516–531. <https://doi.org/10.2307/258556>
- Welter, F. (2012). All you need is trust?: A critical review of the trust and entrepreneurship literature. *International Small Business Journal*, 30(3), 193–212. <https://doi.org/10.1177/0266242612439588>
- Wendell, D. (2015, April 7). Devgrants: Here to help. Retrieved from <https://blog.ethereum.org/2015/04/07/devgrants-help/>
- Werbach, K. (2018). *The blockchain and the new architecture of trust*. Cambridge, MA: MIT Press.
- Whittle, A., & Spicer, A. (2008). Is actor network theory critique? *Organization Studies*, 29(4), 611–629. <https://doi.org/10.1177/0170840607082223>
- Wilcke, J. (2016, February 29). Homestead release. Retrieved from <https://blog.ethereum.org/2016/02/29/homestead-release/>
- Williamson, O. E. (1983). *Markets and hierarchies: Analysis and antitrust implications: A study in the economics of internal organization*. New York, NY: The Free Press.

- Williamson, O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. *Administrative Science Quarterly*, 36(2), 269. <https://doi.org/10.2307/2393356>
- Winiecki, D. J. (2009). The call centre and its many players. *Organization*, 16(5), 705–731. <https://doi.org/10.1177/1350508409338883>
- Winman, T. (2016, October 24). Blockchain is real and it's now! Retrieved from <https://www.ibm.com/blogs/blockchain/2016/10/blockchain-real-now/>
- Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger* (No. EIP-150 revision). Retrieved from <http://gavwood.com/paper.pdf>
- Wood, G. (2016, January 11). The last blog post. Retrieved from <https://blog.ethereum.org/2016/01/11/last-blog-post/>
- Woolgar, S., & Lezaun, J. (2013). The wrong bin bag: A turn to ontology in science and technology studies? *Social studies of science*, 43(3), 321–340. <https://doi.org/10.1177/0306312713488820>
- Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Los Angeles, CA: Sage.
- Yumang, R. (2017a, March 7). Google Hangout: Preview of IBM blockchain at SXSW. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/03/google-hangout-preview-ibm-blockchain-sxsw/>
- Yumang, R. (2017b, March 22). IBM Interconnect: Reimagine your industry with blockchain. Retrieved from <https://www.ibm.com/blogs/blockchain/2017/03/ibm-interconnect-reimagine-your-industry-with-blockchain/>
- Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter?: Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, 9(2), 141–159. <https://doi.org/10.1287/orsc.9.2.141>
- Zamfir, V. (2016, December 6). The history of Casper — chapter 1. Retrieved from <https://blog.ethereum.org/2016/12/06/history-casper-chapter-1/>
- Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly*, 17(2), 229–239. <https://doi.org/10.2307/2393957>
- Zand, D. E. (2016). Reflections on trust and trust research: Then and now. *Journal of Trust Research*, 6(1), 63–73. <https://doi.org/10.1080/21515581.2015.1134332>
- Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior*, 8, 53–111.