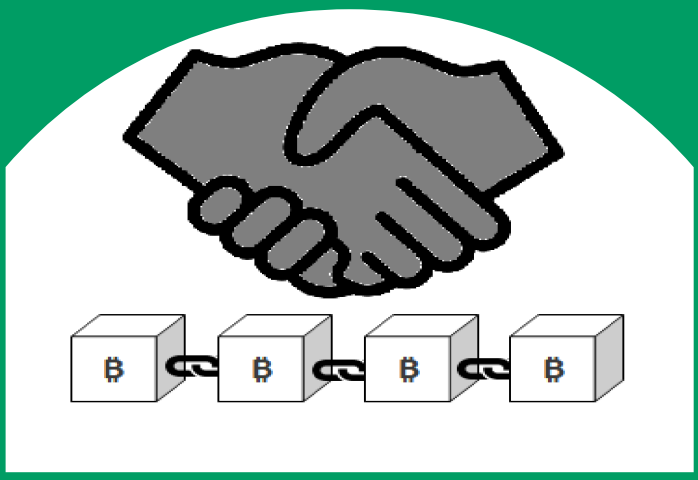
Information Systems Science

Understanding the Aspects of Trust in Blockchain and Cryptocurrencies

Venkata Marella



Aalto University

DOCTORAL DISSERTATIONS

Aalto University publication series
DOCTORAL DISSERTATIONS 119/2021

Understanding the Aspects of Trust in Blockchain and Cryptocurrencies

Venkata Marella

Aalto University
School of Business
Information Systems Science

Supervising professor
Professor Virpi Kristiina Tuunainen, Aalto University School of Business, Finland

Thesis advisor
Professor Matti Rossi, Aalto University School of Business, Finland

Preliminary examiners
Associate Professor Juho Lindman, University of Gothenburg Department of Applied IT, Sweden
Senior Lecturer Claire Ingram Bogusz, Uppsala University Institution for Informatics and Media, Sweden

Opponents
Associate Professor Juho Lindman, University of Gothenburg Department of Applied IT, Sweden
Senior Lecturer Claire Ingram Bogusz, Uppsala University Institution for Informatics and Media, Sweden

Aalto University publication series
DOCTORAL DISSERTATIONS 119/2021

ISBN 978-952-64-0497-4 (printed)
ISBN 978-952-64-0498-1 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-64-0498-1

Unigrafia Oy
Helsinki 2021

Finland

Publication orders (printed book):
Email: venkata.marella@aalto.fi

Completed with the support of Foundation for Economic Education, HSE Foundation, Jenny and Antti Wihuri Foundation, and Marcus Wallenberg Foundation

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

Author
Venkata Marella

Name of the doctoral dissertation
Understanding the Aspects of Trust in Blockchain and Cryptocurrencies

Publisher School of Business

Unit Information Systems Science

Series Aalto University publication series DOCTORAL DISSERTATIONS 119/2021

Field of research

Date of the defence 4 October 2021

Language English

☐ **Monograph** ☐ **Article dissertation** ☒ **Essay dissertation**

Abstract

The advent of cryptocurrencies like Bitcoin has revolutionized the financial industry through a peer-to-peer network that allows the transfer of money without involving a financial intermediary. The underlying blockchain technology of cryptocurrencies provides a platform on which parties without any pre-existing trust among each other can conduct transactions without any involvement or mediation by a trusted third party. Traditional financial organizations are governed by centralized authorities, which are not transparent about their operations, while cryptocurrencies operate on a decentralized system with a distributed ledger, which offers an extremely high degree of transparency. Having a centralized authority incurs several costs that the customers of financial organizations need to pay as transaction fee, which is not required in the case of cryptocurrencies. However, cryptocurrencies do come with a serious drawback. Due to the absence of a centralized authority, fraudulent transactions cannot be reverted. Despite this shortcoming, cryptocurrencies are still able to create trust among users. Hence, it is important to understand what technological attributes of cryptocurrencies create trust among the users.

Our research findings suggest that the openness and immutability of the ledger are the technological attributes that create trust in cryptocurrencies, which are the features of blockchain. Once I identified the technological attributes of blockchain that create trust in cryptocurrencies, I explored how these attributes of blockchain technology can bring trust in a different domain, the hiring process. The process of verifying the documents of job applicants in the hiring process is time-consuming, costly, and inefficient. I built a prototype using blockchain by which the immutable and distributed ledger helps to accurately verify the documents of job applicants immediately and at a low cost. The research provides valuable insights into how blockchain can be implemented in a business process.

Finally, millions of dollars' worth of cryptocurrencies are lost in cyber-attacks on cryptocurrency exchanges every year. Whenever these cyber-attacks happen, customers might lose trust not only in that exchange but also in cryptocurrencies in general. To understand how exchanges rebuild trust, I studied the trust rebuilding measures taken by seven exchanges after cyber-attacks. The research results suggest that compensation is the best technique to rebuild trust while merging with a reputed organization can also be studied as a structural solution to rebuild trust among the customers of the exchange. Overall, this dissertation examines how trust is created, how it is applied, and how it is rebuilt in the domain of blockchain and cryptocurrencies

Keywords

ISBN (printed) 978-952-64-0497-4 **ISBN (pdf)** 978-952-64-0498-1

ISSN (printed) 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2021

Pages 106 **urn** http://urn.fi/URN:ISBN:978-952-64-0498-1

Understanding the Aspects of Trust in Blockchain and Cryptocurrencies

Acknowledgments

During my software career in the United States, I observed that the majority of migrant software professionals are hired by companies on a contract basis through contractors or consulting firms. Though the companies pay decent salaries to these employees, the contractors take a significant portion of their paychecks. In the worst cases, these contractors can skip paying the employees completely, especially if it is the last month of the project. It is very unfair that the person who performs the task gets paid less, while the contractor makes a huge amount of money just by scheduling interviews and running the paychecks of a few contract employees. I have always wondered why the role of intermediaries cannot be automated, not just to save money but also to eradicate unfair practices. Blockchain technology is one such technology that has the potential to show its impact across various industries by eliminating the layer of intermediation in the business process. Satoshi Nakamoto combined cryptography with databases in a distributed network to develop an open and immutable ledger, which can bring trust to the system without intermediaries. This motivated me to research the trust issues in Blockchain technology and cryptocurrencies.

My background in computer science has helped me understand the workings of blockchain and cryptocurrencies. The Dagstuhl workshop on blockchain provided me an opportunity to network with reputed researchers in both information systems and computer science. In the blockchain summer school at the University of Copenhagen, I learned how blockchain can be implemented for various business use cases. The IRIS conference in 2017 helped me network with fellow researchers in my field, and successfully present my research to them. The 32th Bled eConference held at Bled, Slovenia in 2018 was a turning point in my doctoral program My paper received the outstanding paper award at the conference and later the paper was published in the Journal of Electronic Markets. I thank the Conference committee for selecting my paper for the outstanding paper award. It gave me a lot of confidence that I can write good research papers. Later, my papers that were accepted for the AMCIS and HICSS conferences helped me improve my research writing skills. Blockchain events conducted by TietoEVRY cooperations allowed me to learn about various latest technology tools on Blockchain and also provided me an opportunity to network and collaborate with various blockchain practitioners across Finland and other parts of Europe.

I thank the preliminary examiners of my thesis, Associate Professor Juho Lindman from the University of Gothenburg, and Senior Lecturer Claire Ingram Bogusz from Uppsala University, for thoroughly reviewing my dissertation and providing valuable comments, which improved the quality of my work. Moreo-

ver, I am honored to have Juho Lindman and Claire Ingram Bogusz as opponents for my doctoral defense. I look forward to having an interesting debate in the defense. I thank my supervisor, Professor Virpi Tuunainen, for her support in all my research papers and her constructive critiques of my research work. I am very grateful for her mentorship throughout the program. I appreciate her guidance throughout my doctoral program. I thank Professor Matti Rossi for introducing the topic to me and helping me with my research, and Professor of Practice Esko Penttinen for introducing me to companies that are performing pilot studies in blockchain technology. I am very grateful to Professor Roger Bons from FOM University, who helped me to publish my paper in the Journal of Electronic Markets. I thank Professor Liisa Välikangas for providing me several opportunities to participate in various Blockchain hackathon events, which helped me to expand my knowledge on Blockchain. I would also like to express my gratitude to Professor S.V.C. Gupta, who taught me cryptography during my bachelor's program.

I thank my co-authors Anoop Vijayan, Bikesh Upreti, Maryam Roshan, and Jani Merikivi, who have helped and guided my research work. It has been a wonderful experience to work with all of them. I offer a special thanks to Yong Ding, who shared my teaching duties during my doctoral program. I am extremely happy to have become friends Arpine Maghakyan, Anne-Marie Tuikka, Tapani Rinta-Kahila, Darius Pacauskas, Sampsa Suvivuo, Anila Kiran, Yanqing Lin, Wenjie Fan, Sadaat Yawar, Niina Mallat, Sanna Tiilikainen, Elena Mazurova, Kari Koskinen, Hadi Ghanbari, Pradeep Durgam, Heather Bivona, and Nancy Spangler during the program. I enjoyed their wonderful company and discussions on various topics. I thank Merja Mäkinen and Elli Hämäläinen for helping with various travel- and teaching-related issues. I appreciate the help of the HSE Foundation, the Foundation of Economic Education (LSR), the Marcus Wallenberg Foundation, and the Antti-Wihuri Foundation for providing the financial support necessary for me to complete my research. I thank Thomas Taussi for sharing his interesting opinions on cryptocurrencies and Tuula Murremäki for helping me regarding financial matters during my doctoral program. I am extremely lucky to become friends with Petra Ojala, Martti Ojala, Adéla Miklasová, Matu Kormano, and Petri Haapalehto in Helsinki. I appreciate their help during my doctoral program. I thank Keir Finlow-Bates for sharing his knowledge and insights on blockchain technology and cryptocurrencies.

I thank my parents, Sudha Rani Jeedigunta and Prasad Marella, for their love and support throughout my life. I am forever indebted for their sacrifices to make a better future for me. I thank my brother and other relatives who have been very friendly to me and my family for the past few years. Finally, I thank my wife Subha Tushara Ponnada, who has been extremely cooperative and affectionate during my doctoral journey. I would not have been able to finish the doctoral program without her love.

Espoo, 26 August 2021

Venkata Marella

Contents

List of Keywords

Blockchain: Blockchain technology is a decentralized and distributed database in which all transactions are recorded in a ledger (Glaser et al., 2014).

Consensus Mechanism: The process of selecting the next legitimate block to the blockchain is called a consensus mechanism.

Cryptocurrencies: Cryptocurrencies can be defined as digital cash that uses cryptographic algorithms to ensure the safety and security of transactions (Oshodin et al., 2016).

Cryptocurrency Exchange: A cryptocurrency exchange is an online platform on which individuals can buy and sell cryptocurrencies using digital currencies or other cryptocurrencies (Leighton, 2019).

Cryptographic Hash Function: A cryptographic hash function is a mathematical function that takes an input of variable length and generates an output of fixed length that is unique to the given input. It is computationally impossible to find the input of a hash function from the hash output (Narayanan et al., 2016).

Distributed Denial of Service (DDoS) Attack: A DDoS attack involves flooding the victim's computer machines and resources by sending several unwanted packets and depleting the victim's resources for legitimate use (Kotenko & Ulanov, 2014).

Functionality of Technology: Functionality refers to the belief that a specific technology has the capability, functions, and features to do the required task.

Helpfulness of Technology: Helpfulness is described as the belief that technology provides adequate and responsive assistance to users via its help attributes.

Nodes in Blockchain: A node in a blockchain network refers to a computer on which the data are stored.

Proof of Stake (PoS): Miners owning the larger stakes in the system are randomly selected to put the next block onto the blockchain.

Proof of Work (PoW): Miners need to solve a computational puzzle to attach a legitimate block of transactions onto the block-chain.

Reliability of Technology: Reliability can be defined as the property that enables technology to operate consistently over some time.

Social Movement: A social movement can be defined as a set of beliefs and opinions of a certain segment of the population, which represents a change in some elements of the social structure (McCarthy & Zald, 1977).

List of Publications

This doctoral dissertation consists of a summary and of the following publications, which are referred to in the text by their numerals.

This thesis is based on the following research papers:

[1] Marella, V., (2017). Bitcoin: A social movement under attack. *Selected Papers of the IRIS*, *8*(8), 147-163.

[2] Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Journal of Electronic Markets*. 30(2), 259-271

[3] Marella, V., & Vijayan, A. (2020). Document verification using blockchain for trusted CV information. *Americas Conference on Information Systems—2020 Proceedings*, *12*, 1-10.

[4] Marella, V., Roshan, M., Merikivi, J., & Tuunainen, V. K. (2021). Rebuilding trust in cryptocurrency exchanges after cyber-attacks. *Proceedings of the 54th Hawaii International Conference on System Sciences*, *54*, *5636-5646*.

Author's Contribution

Publication I: Marella, V., (2017). Bitcoin: A social movement under attack. *Selected Papers of the IRIS*, *8*(8), 147-163.

Venkata Marella was the sole contributor to this paper.

Publication II: Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Journal of Electronic Markets*, 30(2), 259-271.

Venkata Marella was the lead author of this paper. He contributed the initial idea of the paper and formed the research question. He explored the existing literature and found the appropriate literature to analyze. He was also involved in the data collection process and drawing the results from the research findings.

Publication III: Marella, V., & Vijayan, A. (2020). Document verification using blockchain for trusted CV information. *Americas Conference on Information Systems—2020 Proceedings*, *12*, 1-10.

Venkata Marella was the lead author of this paper. He contributed to the entire paper except the building of the prototype of the solution. He contributed to gathering the survey details of falsified CV information, framed the research question, proposed the research methodology, designed the solution, and explained the advantages of the solution.

Publication IV: Marella, V., Roshan, M., Merikivi, J., & Tuunainen, V. K. (2021). Rebuilding trust in cryptocurrency exchanges after cyber-attacks. *Hawaii International Conference on System Sciences, 54, 5636-5646.*

Venkata Marella was the lead author of this paper. He was involved in framing the research question, the literature review on trust repair mechanisms, data collection, performing the qualitative analysis, and sentimental analysis on the data, as well as drawing the conclusions from the research findings.

PART I: SUMMARY

1. Introduction

In the ancient world, peace treaties between the warring tribes were made in the names of Gods (Thieme, 1960). Each tribe insisted that their opponent tribe promise in the name of their Gods/Goddesses that they would not violate the norms of the peace treaty. Why promise to honor peace agreements in the name of God? The simple answer is trust. To trust or not to trust is the dilemma of human society. There is a trust deficit when parties sign peace agreements without involving the Gods. Ancient civilizations heavily relied on Gods for everything. They performed sacrifices to Gods for rain, fertility, and well-being. They believed that angering the Gods would lead to being cursed with famine, epidemics, and defeat. Hence, they believed that their opponents would not violate the norms of an agreement as it would anger the Gods, for which their civilization would be cursed. The modern world is no longer dependent heavily on Gods and Goddesses. It is dependent rather on technology. Technological changes have replaced the role of God in human well-being. Can technology solve the age-old problem of trust?

Trust is central to everyone's social life. Trust is such an important aspect of human civilization that societies cease to exist without it (Vu, 2010). Societies with high trust outperform societies with low trust (Werbach, 2018). A climate of trust creates the required environment for cooperation between people (Friedman et al., 2000). We as human beings, with limited mental (intellect) and physical (sensing) capabilities, cannot face the complexities of the world without resorting to trust, as it is the only tool to reason sensibly about the possibilities of everyday life (Luhmann, 1979). We make decisions every day by trusting something or someone and making ourselves vulnerable to the actions of others. You may leave your computer unlocked, trusting that your colleague will not spy on your emails; you may use an elevator, trusting that it will take you to the right floor of the building without malfunctions; you may take a vaccine, expecting that it will protect you from a disease, or purchase a product online, trusting that it will be delivered in a timely manner and in good condition. There is an endless list of such examples in our daily lives in which trust is the key component of everything we do. However, if individuals or organizations fail act or behave according to one's expectation, it creates a trust deficit, and people tend to look for alternatives. For example, if your internet service provider does not provide the promised internet speed, you cancel your subscription and look for alternative service providers. Similarly, if traditional financial institutions fail to deliver what they have promised to investors, the latter will look for alternative options.

The 2008 collapse of Lehman Brothers, the third-largest investment banker in the United States, created a trust deficit in traditional financial institutions among investors (Marella, 2017). According to Edelman's (2015) trust barometer, trust in institutions, and corporations especially, fell to its lowest level during the 2008 global financial crisis (Tapscott & Tapscott, 2016). Investors began looking for alternative options. A few months later, a whitepaper was published in the crypto-mailing list entitled "Bitcoin: A peer-to-peer electronic cash system." The first line of the paper states, "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008). The idea of transferring money without involving a financial institution attracted several investors toward Bitcoin. As Bitcoin gained popularity, several other cryptocurrencies emerged, and cryptocurrency exchanges were formed to trade cryptocurrencies with fiat currencies.

After the development of Bitcoin, researchers realized that the underlying technology of Bitcoin is blockchain technology, which provides an immutable ledger that replaces the requirement of having third-party governance for the safety and security of transactions. It is like understanding the importance of the internet after the invention of email (Kaiserman, 2018). Blockchain is a decentralized database that is distributed across a number of nodes (i.e., computers) and in which all transactions recorded on the database are made immutable using cryptographic techniques (Narayanan et al., 2016). Every node in the blockchain network has access to the information on the blockchain. The immutability and openness of blockchain provide the required trust between unknown parties (Venkata et al., 2019).

Blockchain is an emerging technology, and cryptocurrencies (an application of blockchain) are a new phenomenon by which trust provided by technology has replaced the requirement of a trusted third party as an intermediary. It is important to understand how trust is created using blockchain. Blockchain is predicted to disrupt various fields, and studying the trust aspects of this technology is of pivotal importance. Cryptocurrencies are the most popular application of blockchain, representing a 350 billion dollar market as of August 2020 (CoinMarketCap, 2020). None of the transactions using these cryptocurrencies are controlled or protected by any centralized authority. They are rather protected by the cryptographic algorithms used in the blockchain. Hence, studying the attributes of technology that create trust in cryptocurrencies is a topic of interest.

Once the attributes of the technology that create trust in cryptocurrencies are understood, it is extremely important to know how these attributes can create trust in other areas. Because blockchain has the potential to disrupt several domains, including supply chain management, asset management, digital identity, electronic voting systems, and healthcare data management, I want to implement blockchain in an area that is less discussed, the hiring process, to make the recruitment of new employees more reliable and less expensive. The research in this area allows us to understand how the attributes of technology bring trust to the business process. The solution not only helps to elucidate how

to implement blockchain for a business problem, but it also helps us to evaluate the benefits of using blockchain.

Cryptocurrencies do not just rely on blockchain, they also depend on exchanges and wallet technologies for trading and storing cryptocurrencies. A cryptocurrency wallet is a software program that stores the public and private keys of an account and can interact with the blockchain to enable the management of the account. A cryptocurrency wallet can be an online wallet, software wallet, or hardware wallet (Bierer, 2016). A cryptocurrency exchange is an online platform that allows customers to trade cryptocurrencies with fiat currencies or other digital assets (DeVries, 2016). Customers of these exchanges often have online wallets with the exchanges.

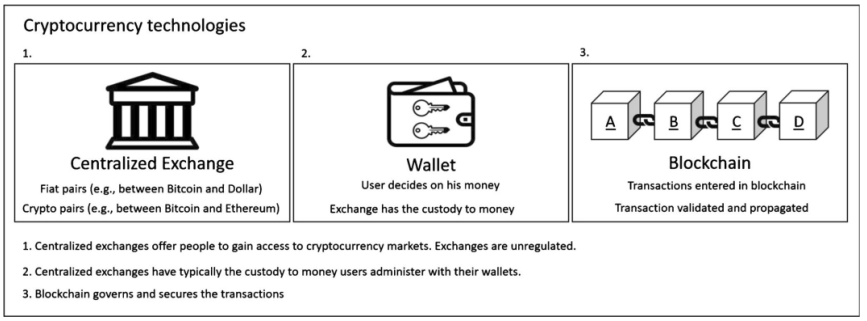


Figure 1. Cryptocurrency technologies (Narayanan et al., 2016)

These exchanges are subjected to several cyber-attacks each year, in which cryptocurrencies worth several millions of dollars are lost. Customers can lose trust in crypto currency when such events occur. Hence, it is extremely important to rebuild trust with customers. Though there is a significant study on trust in technology in the information systems literature, less research is dedicated to rebuilding trust in technology. I have researched the topic of rebuilding trust in cryptocurrency exchanges after cyber-attacks.

My dissertation introduces Bitcoin as a social movement and explains how it differs from traditional financial institutions. Later, I examine the technological attributes of cryptocurrencies that create trust among users. Then, I implement blockchain in a business use case to understand how these attributes of technology create trust in the business process without involving intermediaries. Finally, I examine the trust rebuilding process in cryptocurrency exchanges.

2. Background and Motivation

Cryptocurrencies can be defined as digital currencies (or assets), where the security of the transactions and the generation of new crypto-coins is governed by cryptographic algorithms (Narayanan et al., 2016). Cryptocurrencies are not governed by any central authority, unlike fiat currencies, which are governed by the monetary policies framed by the central banks of their countries (He, 2019). Several governments in various countries have abused their monetary policies for temporary benefits and devalued their currency. Hence, cryptocurrencies are a good alternative to traditional fiat currencies in countries like Iran and Venezuela, which have extremely volatile currencies (Gail, 2018).

Unlike traditional centralized databases, blockchain provides immutability to the transactions, and hence no record can be tampered with or deleted (Politou et al., 2019). Apart from immutability, the digital signature on each of the transactions helps to authenticate the party who initiated the transaction (Agrawal, 2018). The distributed nature of the ledger brings openness to the system, and any node in the system can access the data on the blockchain. These features of blockchain eliminate the requirement of a third party (central authority) in a business transaction.

The role of the intermediaries in a business transaction is to perform the careful verification of the background of the party involved, along with a chain of intermediaries (Nofer et al., 2017). The process of human or institutional intermediation is costly, time-consuming, and lacks transparency in its operations (Quentson, 2016). Cryptocurrencies replace financial intermediaries with blockchain technology. However, cryptocurrencies do have several shortcomings. First, they are not governed by any authority, and fraudulent transactions cannot be reported to anyone to claim reparations or revert the transactions. Second, all the users of cryptocurrencies are pseudo-anonymous meaning that they are not identified by their names or social security numbers; they are rather identified with 32-bit public key addresses linked to their accounts (Narayanan et al., 2016). This kind of pseudo-anonymity means that individuals involved in a cryptocurrency transaction cannot be identified easily. Thus cryptocurrencies can become a tool for illegal activities like drug trafficking, money laundering, tax evasion, illegally weapons buying, terrorism financing, and extortion (Brezo & Bringas, 2012). Third, Cryptocurrencies do not have legal status in several countries, so buying and selling cryptocurrencies can be extremely difficult in these places. Finally, the value of cryptocurrencies is very volatile for several reasons, including competition from other cryptocurrencies, demand and supply, cyber-attacks, cost of mining, and rewards for mining (Bloomenthal, 2020).

Despite these shortcomings, cryptocurrencies can create trust among customers and make them invest. In such a case, it is very interesting to identify the attributes of cryptocurrencies that create trust among users.

Cryptocurrencies are just the tip of the iceberg of all the applications that can be built using blockchain (Cassiopeia Services, 2020). To uncover the potential of blockchain, I applied it in the hiring process to authenticate the documents provided by the job applicants. This research helps to uncover the benefits of using blockchain in the process compared to traditional business processes.

Several exchanges have been subjected to multiple cyber-attacks right from the genesis of cryptocurrencies. When investors lose their money, they lose trust not only in the exchange but also in cryptocurrencies. Hence, the exchanges need to rebuild trust for customers. I explored various trust rebuilding techniques adopted by cryptocurrency exchanges. These trust rebuilding techniques are not particularly framed for cryptocurrency exchanges but are generalizable to any organization that operates virtually. Due to the COVID-19 pandemic, several organizations operate online with less physical interaction, hence the research is extremely relevant in the current situation.

2.1 Research Objectives

The objective of this thesis is to understand the technological attributes of cryptocurrencies that create trust among users and how these technological attributes can apply in a different domain, the hiring process. In this thesis, I have focused on how cryptocurrencies have developed into an alternative to traditional financial institutions. I examine the set of technological attributes that create trust in cryptocurrencies and applied these attributes to the hiring process. Finally, I study how cryptocurrency exchanges rebuild trust among customers after cyber-attacks. Hence, the overall research question for the dissertation is as follows:

How is trust built among the users of cryptocurrencies and blockchain applications?

The sub-questions of the dissertation are as follows:

- What set of technological attributes of cryptocurrencies create trust among users?
- How does blockchain create trust in verifying the documents of job applicants in the hiring process?
- How do cryptocurrency exchanges rebuild trust among users after cyber-attacks?

Several blockchain projects are still in the pilot phase of implementation, and many companies are yet to venture into blockchain projects. My research

helps them understand how blockchain creates trust in a specific business process and highlights the benefits of using blockchain.

2.2 Dissertation Structure

This essay-based dissertation is composed of four individual research papers related to the trust aspects of cryptocurrency and blockchain. The research papers are appended to the second part of the dissertation. The first part of the dissertation explains the relationship between various research papers and how they explore the various trust aspects related to blockchain and cryptocurrencies. I provide the related literature for all the papers and explain their theoretical contribution as well as their practical implications.

The first part of the dissertation is divided into eight sections. The next section provides a literature review on trust in technology, trust in cryptocurrencies and blockchain. In the later sections, I discuss the theoretical background and then talk about the research methodology, followed by detailed discussion on philosophical assumptions. Then, I explain about data collection and analysis; discussion of research findings; the implications of this research in terms of theoretical contributions and practical implications; and the conclusion of the dissertation.

3. Literature Review

Trust is a multifaceted, complex, and evolving phenomenon (Grabner-Kräuter et al., 2015). Trust refers to the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform the actions that are important to the trustor, irrespective of the trustor's ability to monitor or control the other party (Mayer et al., 1995). The party (or the person) who trusts is called a trustor and the party (or the person) who is trusted is called a trustee (Naber et al., 2018).

Trust as a concept has been discussed extensively in various fields, including social science, organization and management science, psychology, sociology, education, political science, economics, history, and anthropology (Gambetta, 1988). Trust can be defined as being vulnerable to the actions of the other party (Mayer et al., 1995). Trust is extremely important due to the existence of uncertainty or the possibility of undesirable outcomes (Luhmann, 1979).

From a sociological perspective, trust is conceived as a property of a collective unit, not isolated individuals. Trust in the social system refers to the members of the system acting accordingly and being secure in the expected futures constituted by the presence of each other (Lewis et al., 1985). Trust in political science refers to citizens' assessments of the core institutions of the polity and a positive evaluation of attributes such as credibility, fairness, competence, and transparency in its policy-making (Zmerli, 2014). Trust in the field of psychology is defined as an emotional state of mind rather than an expectation of a particular behavior from others (Thagard, 2018). In the field of medicine, trust is defined as the patients' reliance on the person and the character of their physicians and also the patients' and physicians' reliance on medical-scientific research and effectiveness of treatment (Imber, 2017). Economists view trust as an institutional phenomenon. Institutional trust can be defined as the belief that future interactions will continue based on rules or norms. The views of social psychologists on trust are defined as one's expectations of the other party in a transaction, considering the risks associated with assuming and acting on such expectations and contextual factors that either contribute to or inhibit the development of the relationship (Coleman & Deutsch, 2014).

Trust has been extensively studied in the field of information systems as well. Most of the literature on trust in information systems is related to consumer online trust, social media platforms, internet banking services, mobile payments, and automation. For example, Lee et al.'s research on e-commerce considers technical competence, reliability, and understanding the medium of purchase as the components of trust (Lee et al., 2014). A study on mobile payments

suggests that the reputation of the mobile service provider plays an important role in mobile payments (Chandra et al., 2010). The research on trust in automation proposes that humans' interactive experiences with automation technology creates trust in automation (Yang et al., 2017). Finally, the research on trust in online banking suggests that secure authentication mechanisms and situational awareness play a major role in the creation of trust in online banking (Nilsson et al., 2005).

Trust literature can be divided into two sub-sections: building trust and rebuilding trust. The literature on building trust is studied across various domains, including technology. Trust in cryptocurrencies and blockchain comes under the category of trust in technology. Figure 2 demonstrates how these concepts are related. The literature review begins by discussing the existing literature on building trust and rebuilding trust. Then, I will explore the literature on building trust in technology and present the various trust dimensions in the literature in the study of trust in technology. Then, I will discuss the existing literature on trust in technology and cryptocurrencies and address the research gap in trust in cryptocurrencies.

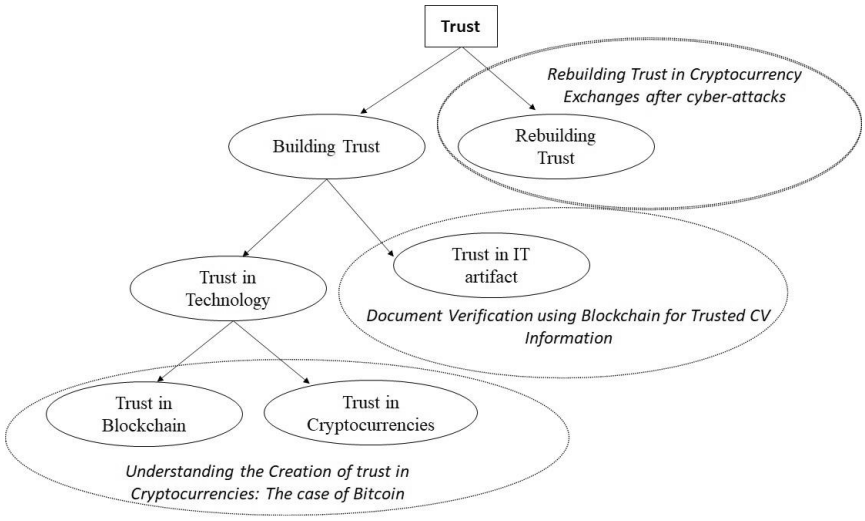


Figure 2. Relationship between the trust concepts of the papers

3.1 Building Trust

Trust can be conceptualized as confidence in relying on another in an uncertain relationship (Ye et al., 2020). Trust is a dynamic emotional relationship that evolves and entails responsibility (Flores & Solomon, 1998). Lewicki and Bunker (1995) propose three stages of trust development in a professional relationship: calculus-based trust (CBT), knowledge-based trust (KBT), and identification-based trust (IBT). CBT is a form of trust that is built on the grounds of fear of punishment for violating trust and desire for the rewards for preserving it.

The relationship in CBT is sustained by comparing the costs and benefits. There is constant monitoring and reporting between the parties in CBT, and controlling the other person's behavior is crucial. In CBT, trust relies heavily on a cognitive assessment of the trustee. Trust is sustained as long as the benefits outweigh the cost of damaging it. Emotional concerns are irrelevant in CBT. Knowledge-based trust occurs when an individual has enough knowledge and understanding about the other person to predict that person's behavior. Parties understand each other through repeated interactions, communication, and relationship building. IBT refers to a transaction in which both of the parties who are involved understand and endorse each other. It requires parties to fully internalize and harmonize with each other's desires. Identification enables the parties to think, feel, and respond like a single party. Trust has to develop over time. A trust relationship should develop and mature from CBT to KBT, and from KBT to IBT (Lewicki & Bunker, 1995).

3.2 Rebuilding Trust

Trust is easier to destroy than to build (Canavera, 2021). Trust violations occur when the behavior or the performance of the trustee does not reach the expectations of the trustor (Tomlinson & Mayer, 2009). Trust violations lead to a reduction in subsequent trust and cooperation (Lewicki & Bunker, 1995). They hamper the mutual support and information sharing between the parties (Bies & Tripp, 2015) and reduce the level of organizational citizenship behavior and job performance (Robinson, 1996). They can also lead to a reduction in the profitability of organizations (Simons & Parks, 2000). Hence, rebuilding trust after a trust violation is a subject of high significance in various fields of study.

Trust rebuilding or repair is a process of reversing the negative attitude accumulated by the trustor due to the trust violation and enabling the trustor to take the risk of being vulnerable to the actions of the trustee again (Kramer & Lewicki, 2010). The majority of trust rebuilding techniques are focused on the efficiency of the actions taken by the violator (trustee) to repair trust after the violation. These trust rebuilding techniques are classified as social accounts, compensation, and structural solutions. Social accounting refers to the verbal techniques, such as apology and explanations, used to rebuild trust. Compensation refers to actions taken to reduce the damage caused by trust violations. Structural solutions refer to the steps taken by an organization to prevent trust violations in the future.

Trust violations in CBT can be repaired when the offender gives a sincere, timely, and complete apology (Lewicki & Tomlinson, 2014). This process can be further accelerated by compensation and structural solutions. If these techniques indicate repentance, these are going to help the trust repair process. In IBT, there is a higher level of emotional investment, and any trust violation can be viewed as a direct challenge to the trustor's most cherished values (Lewicki & Bunker, 1995). It can also represent a conflict with the trustor's psychological orientation (Deutsch, 1985). Both parties should exchange information about the trust violation with each other and clear any kind of misunderstanding. The

trustor should be willing to forgive the actions of the trustee, and his commitment toward the relationship plays an important role in rebuilding trust (Finkel et al., 2002). In the final communication stage, the parties affirm their commitment to a high-IBT relationship. Trust rebuilding strategies differ according to the kind of relationship the parties have. Parties with very few alternatives to their existing relationships or who experience a high degree of interdependence will likely continue the relationship despite repeated trust violations (Rusbult & Martz, 1995). Parties who are emotionally involved in a high-IBT relationship are less sensitive to trust violations (Robinson, 1996).

Rebuilding trust after a trust violation is usually researched in the context of relationships and organizational management (Pratt & Dirks, 2007; Schniter, et al., 2013). In information systems research, rebuilding trust is studied in the areas of eCommerce, and online auctions (Choi & Nazareth, 2005; Seeger et al., 2017; Utz et al., 2009). The existing literature classifies trust violations into two types, integrity-based violations of trust and competence-based violations of trust. The research suggests using apology for competence-based violations of trust and denial for integrity-based violations of trust to rebuild trust (Utz et al., 2009). There is no information systems research on rebuilding trust in cryptocurrencies or cryptocurrency exchanges.

3.3 Trust in Technology

Technology is defined as the use of systematic procedures to produce intended effects. Many researchers acknowledge that people put their trust in technology artifacts themselves, which is commonly referred to as trust in technology, and it represents a human-to-technology trust relationship. This is different from trust in humans, which represents human-to-human trust relationships (Lankton et al., 2015a). The IT artifact itself becomes the trustee, an item on which the trustor has to put his trust. A lot of research has been conducted to understand the trust dimensions in technology. The research on trust in B2B eCommerce suggests confidentiality, integrity, authentication, non-repudiation, access controls, and availability as the dimensions for technology trust (Ratnasingam, 2005). Integrity refers to data being noncorrupt in storage and during transmission. Confidentiality means that unauthorized people should not be able to access data. Availability refers to communication between computers that should happen when requested. Authentication is the process of making sure that the signatory is really who they purport to be. Non-repudiation is giving assurance that completed transactions cannot be denied (Diniz et al., 2005). On the other hand, the trust studies in eCommerce by Corbitt et al. (2003) use reliability, security, and privacy as the trust dimensions (Corbitt et al., 2003). Reliability is the belief that the technology will consistently operate properly (McKnight et al., 2011). Security refers to the safety of the transactions. Privacy refers to the protection of the personal information of the users of the system. A similar study in the area of eCommerce from Lee et al. (2014) suggests that technical competence, reliability, and medium understanding are the trust constructs to evaluate trust in eCommerce. Technical competence refers to the ability of a technology to execute the tasks it is supposed to perform. The

degree to which a consumer understands the workings of the internet shopping website is called medium understanding (Lee et al., 2014). The research performed by Diniz et al. (2005) on Brazilian internet banking uses functionality, reliability, and usability as the trust dimensions. Functionality refers to the set of services offered by the technology. Reliability refers to the security of the transactions, and usability indicates the ease of browsing the services and the ability to complete a transaction (Diniz et al., 2005). For this research in understanding the creation of trust in cryptocurrencies, I have chosen the trust dimensions reliability, functionality, and helpfulness, as used by McKnight et al. (2011) for the adoption of Microsoft Excel, as these trust dimensions are suitable to classify the technological attributes of cryptocurrencies. These trust dimensions are useful in exploring all the features of cryptocurrencies. Table 1 represents the trust dimensions from different research papers.

Table 1. Literature review on trust in information systems

Trust Dimensions	Context	Study
Confidentiality, integrity, authentication, non-repudiation, access controls, and availability	B2B eCommerce	(Ratnasingam, 2005)
Reliability, security, and privacy	eCommerce	(Corbitt et al., 2003)
Technical competence, reliability, and medium understanding	eCommerce	(Lee et al., 2014)
Functionality, reliability, and usability	Internet banking	(Diniz et al., 2005)
Reliability, functionality, and helpfulness	Adoption of Excel	(McKnight et al., 2011)

3.4 Trust in IT Artifacts

Trust does not always involve people; it also includes objects. In the field of information systems, these objects can be IT artifacts. IT artifacts refer to hardware or software that enables a particular task (Vance et al., 2008). IT artifacts take the role of trustee in the relationship with users. Though trust is a dynamic process that evolves, initial trust formation is extremely important in the case of IT artifacts. Initial trust refers to trust in an unfamiliar trustee, in which the trustor does not have any credible information or experience with the trustee (Bigley & Pearce, 1998). When users interact with unknown IT artifacts, their perceptions of uncertainty and risk are significant (McKnight et al., 2002). Trust related to IT artifacts is mostly studied on topics such as recommendation agents, automated systems, and eCommerce websites (Lee &

See, 2009; Benbasat & Wang, 2005). Understanding human behavior as it relates to the usage of IT artifacts and designing IT artifacts accordingly is the core goal of information systems research. The designers of IT artifacts should focus on design elements such as navigability and visual aesthetics (Vance et al., 2008). Söllner et al.'s (2012) trust model evaluates IT artifacts based on three dimensions: the performance, process, and purpose of the IT artifact. The model is based on the trust model proposed by Lee and See (2004) on trust in automation. Paravastu et al.'s (2014) study on trust in software artifacts, particularly antiviral software, uses performance and predictability. Performance of the software refers to the capability of software to accomplish the designated task . Predictability of the software overlaps with integrity in interpersonal relations, both referring to behaving as expected. The predictability of technology is very important if people have to rely on it (Dalton & Choo, 2001).

Vance et al.'s (2008) research suggests that ease of use plays a major role in creating trust in IT artifacts. It also proposes that culture can show an effect on the degree to which users place trust in IT artifacts. Low trusting societies are less inclined to trust IT artifacts while high trusting societies are more likely to trust IT artifacts, implying that IT artifacts are not culturally neutral (Vance et al., 2008). Since system characteristics play a major role in the creation of trust in IT artifacts, in the paper "Document verification for trusted CV information," we built a prototype the accepts documents in various formats to increase the ease of use.

3.5 Trust in Blockchain

Trust in business is defined as the expectation of one party that another party will act with integrity, honesty, consideration, accountability, and transparency (Tapscott & Tapscott, 2016). A Gallup survey conducted in 2015 on American confidence in institutions found that "business" ranked second lowest among the fifteen institutions measured, indicating a lack of trust in corporations. Blockchain technology has emerged in response to the erosion of trust in traditional institutions and online intermediaries as it eliminates the requirement of a trusted third party (De Filippi et al., 2020). *The Economist* (2015) termed blockchain "the trust machine," implying that it is a system in which the issues related to trust do not exist. Blockchain has also been called the "trust protocol" by Tapscott and Tapscott (2016), who also state that blockchain technology is the greatest chain of being sure about things. Blockchain creates a trusted network for business, which can simplify and accelerate the economy. Blockchain became popular in the financial sector, where transparency, trust, and security of transactions are of pivotal importance (*The Economist,* 2015). Carrying out user transactions via a peer-to-peer network in a transparent way would add an additional level of technical trust on top of institutional trust (Lindman et al., 2020). Blockchain technology enables trust-free (no trust on people), frictionless transactions, which reduces transaction fees significantly (Beck et al., 2016).

Blockchain offers an immutable ledger that is distributed among the nodes of the network. Data is stored in the form of blocks. Each block receives a hash

value from the previous block and propagates its hash value to the next block. This chaining of blocks with hash values makes the blockchain ledger immutable (Narayanan et al., 2016). The execution and verification of transactions as well as the maintenance of the ledger are carried out by reliant cooperation and competition between multiple nodes, creating a decentralized trust machine (Bogusz et al., 2020). The key feature of distributed trust architecture is that it is possible to trust the output of the system without necessarily trusting any of its individual components (nodes) (Werbach, 2018). Blockchain promises to drastically reduce the cost of trust, replacing a centralized authority with an open, distributed ledger. The need for trusted middlemen allows technology giants like Google, Facebook, and Amazon to turn economies of scale and network effects into de facto monopolies (Casey & Vigna, 2018). Blockchain offers a unique opportunity for a trusted ecosystem where large-scale data sharing can be enabled among various stakeholders (Roman & Stefano, 2016).

3.6 Trust in Cryptocurrencies

Cryptocurrencies and blockchain are relatively new phenomena, which came into existence with the inception of Bitcoin in 2008 (Nakamoto, 2008). It has been over ten years since the inception of cryptocurrencies, and there have been several research papers written on them. However, there has not been much literature dedicated to the study of trust in cryptocurrencies (Bucko, 2015). The literature review in this dissertation aims to show that there is a lack of literature on trust in the cryptocurrencies domain and to identify the existing research gap in the literature of trust in cryptocurrencies. I performed a literature review via the AIS library using the keywords “trust,” “blockchain,” “Cryptocurrency,” and “Bitcoin.” Bitcoin being the most popular cryptocurrency and synonymous with cryptocurrency, the word “Bitcoin” is used in the literature review.

The existing literature suggests that trust in cryptocurrencies can be generated by confidence in the underlying technology of cryptocurrencies (Bucko et al., 2015). However, the paper does not suggest the attributes of the technology that creates trust in cryptocurrencies. Other research on trust in cryptocurrencies talks about trust from a stakeholder’s perspective (miners, users, exchanges, and merchants) rather than from a technological perspective (Sas & Khairuddin, 2017). Sadhya et al.’s (2018) study on trust in cryptocurrencies uses argument mapping from various technology trust dimensions, including reliability, functionality, and helpfulness. The paper claims that the decentralization feature of blockchain creates reliability. However, these claims are not supported by any data analysis in the paper. Research from Mendoza-Tello et al. (2018) suggests that social networks help to create trust in cryptocurrencies. The study was conducted through surveys that were distributed at universities, business libraries, and shopping centers. The research claims that there is a lot of uncertainty in cryptocurrencies due to price volatility, lack of regulations, and cyber-attacks. Social networks have the ability to communicate thoughts, opinions, and comments on cryptocurrencies, which decrease the perceived risk of cryptocurrencies (Mendoza-Tello et al., 2018). Hence, there is a lack of proper research into understanding trust in cryptocurrencies.

4. Theoretical Background

In this dissertation, framing theory is used to explain how Bitcoin is considered a social movement. The trust dimensions (functionality, reliability, and helpfulness) proposed by Lankton et al. (2015) were used to identify the factors that create trust in cryptocurrencies. Finally, the trust rebuilding techniques suggested by Lewicki and Tomlinson (Lewicki & Tomlinson, 2014) were evaluated in the context of cryptocurrency exchanges.

4.1 Framing Theory

Bitcoin revolutionized the financial industry. To explain how Bitcoin can be considered a social movement in the financial industry, I use framing theory, which is generally used in the communication disciplines. Framing is the process by which people develop an understanding of an issue and realign their thinking on it (Benford & Snow, 2000). Framing theory is derived from the expectancy-value theory of an individual's attitude (Chong & Druckman, 2007). According to expectancy-value theory, an individual's attitude toward an event or an issue is the total sum of their beliefs about that event. Framing allows individuals to realign their attitude toward a subject. Frames affect the attitudes and behaviors of audiences. This process is typically called a framing effect.

I use framing theory to explain how Bitcoin is projected as a social movement in the financial sector. Collective action frames are classified as diagnostic framing, prognostic framing, and motivational framing (Snow & Benford, 1988). Diagnostic framing is referred to as injustice framing, which is related to problem identification and attribution. It frames certain events or issues as problematic. The second category of collective action frames is prognostic framing, which describes the solution for the problem mentioned in the diagnostic framing and proposes a strategy to execute the solution. The third category of collective action frames is motivational framing, which calls for action to make things better by using vocabulary to motivate investors (Chong & Druckman, 2007).

4.2 Trust in Technology

Cryptocurrencies are decentralized systems that operate completely on technology, without any human or institutional mediation. Hence, it is extremely important to identify the attributes of the technology that create trust in cryptocurrencies. I have extensively researched various trust theories in technology.

According to Friedman, Khan, and Howe, "people trust people, not technology" (Friedman et al., 2000, p. 36). However, if technology emulates the qualities of humans, then people trust technology. The qualities of a human being that create a trust are competence/ability, integrity, and benevolence (Lankton et al., 2014). Competence/ability refers to the belief that the trustee has skills that help the trustor achieve the desired function. Integrity is the belief that a trustee associates with a set of principles that are acceptable to the trustor. Benevolence is the belief that the trustee is motivated to do something good for the trustor, besides being profitable. These three qualities in technology would translate to functionality, reliability, and helpfulness (McKnight et al., 2011). I tried to look for the characteristics of cryptocurrencies that are related to the constructs of functionality, reliability, and helpfulness. Functionality is conceptually very similar to ability or competence. Functionality refers to the belief that a specific technology has the capability, functions, and features, to do the required task. Reliability can be defined as a property that enables technology to operate consistently over some time. Helpfulness is like benevolence and is described as the belief that technology provides adequate and responsive assistance to users via its help attributes (McKnight et al., 2011).

4.3 Trust Rebuilding Techniques

Cryptocurrency exchanges are subjected to cyber-attacks, leading to the need to rebuild trust among customers. Trust violations happen when an outcome does not conform to the trustor's expectations of the trustee's behavior (Tomlinson & Mayer, 2009). Trust repair is the process of changing the trustor's negative expectations that were accumulated due to a trust violation; these expectations must be altered to a point at which the trustor is once again willing to put his or her confidence in the trustee (Dirks et al., 2018). A general response to trust violations include social accounting (including explanations and apology), compensation (including reparations and penance), and structural solutions (including regulation and hostage posting) (Lewicki & Tomlinson, 2014).

With regards to social accounting, apology plays a key role in rebuilding trust among the customers. Polin et al. (2012) identify six potential components of an effective apology: expression of regret for the violation, explanation of why the violation occurred, acknowledgement of responsibility for causing the violation, declaration of repentance, offer of repair, and request for forgiveness. The expression of regret represents the trustee's expression of regret for the offense. An explanation of the violation is a statement in which the trustee explains how the violation happened to the trustor. Acknowledgement of responsibility is an admission that the trustee accepts his part in the mistake. A declaration of repentance is a statement in which the trustee expresses his regret for violation and promises not to repeat it. An offer of repair refers to a statement extending a way to work toward trust rebuilding on the part of the trustee. The request for forgiveness is a statement asking for the trustor to pardon the trustee's actions. The study concludes that an apology is more effective if it has all these components. Research on social accounting has concluded that reticence (silence) is a

suboptimal response to trust violation (Weitzl et al., 2017). Reticence appears to show an expression of repentance by showing that the trustee is upset about the violation and is willing to change things to prevent further violations (Lewicki & Tomlinson, 2014). Nevertheless, a recent study concluded that denial of a trust violation is more effective than an apology when the trust violation is due to the low integrity of the trustee (Lewicki & Tomlinson, 2014). Actions taken by the trustee play a major role in rebuilding trust rather than mere words. Offering substantial compensation for the violations can restore trust among the customers. Substantial compensation shows a sign of repentance and is considered an effective way to rebuild trust (Lewicki & Tomlinson, 2014). Overcompensating is more likely to repair the trust of the customers (Bozic & Kuppelwieser, 2019). The final category of the trust repair mechanism is structural solutions. Changing the structure of the organization helps to repair trust among customers. According to Nakayachi and Watabe (2005), hostage posting helps repair trust by allowing the trustor to monitor the actions of the trustee and pay penalties for any violations. Similarly, regulation is a tactic that focuses on altering the situation to make the trustee more accountable for his or her actions (Dirks et al., 2011).

5. Methodology

The empirical part of this thesis comprises four separate but interlinked research papers that deal with the trust aspects of cryptocurrencies and blockchain. Though each paper deals with a different research question, all of them share a certain similarity in the property of the technology that is being researched. For the papers "Bitcoin: a social movement under attack" and "Document Verification using Blockchain for Trusted CV Information", I used qualitative methodology with an interpretive approach. I used quantitative methodology via textual analysis with a positivistic approach for the paper "Understanding the creation of Trust in Cryptocurrencies: The case of Bitcoin". For paper "Rebuilding Trust in Cryptocurrency Exchanges after Cyber-attacks", I used qualitative methodology and sentimental analysis following a positivistic and interpretive approach. I used both quantitative and qualitative research methods for the thesis, and the following section explains the ontological and the epistemological assumptions for each of the papers in the thesis. In a later section, I will discuss the data collection and analysis approach taken for each paper.

5.1 Philosophical Assumptions

Ontology is the fundamental assumption that researchers make about their phenomenon of interest (Guba & Lincoln, 1989). The ontological assumption of my thesis is that there exist multiple subjective interpretations of a single objective reality. From this ontological assumption, I derive the epistemological assumption that I used an interpretive research paradigm for most of the papers. However, I have also used a positivist approach to describe the underlying objective reality. Epistemology refers to the process through which the researcher generates knowledge about the phenomenon of interest (Purao, 2013).

I have used a blended approach of both quantitative and qualitative research methods in this thesis. For the paper "Bitcoin: a social movement under attack," the research question is focused on understanding how Bitcoin is presented as a social movement in digital media and social media. To understand different perspectives, I have chosen the interpretive research approach using the qualitative method. In the second paper, titled "Understanding the creation of trust in cryptocurrencies: The case of Bitcoin," I aimed to explore the factors that create trust in cryptocurrencies. I used an objective approach to uncover the factors. Quantitative textual analysis was used for the research. I analyzed 1.97 million posts to calculate the factors closest to the word "trust." I used semantic

similarity as a measure to identify the factors that create trust in cryptocurrencies. It is impossible to perform qualitative analysis on such a large set of data. For the final paper, titled "Rebuilding trust in cryptocurrency exchanges after cyber-attacks," the research question is designed to understand how cryptocurrency exchanges rebuild trust in cryptocurrencies. To answer the research question, I used a blended approach of both qualitative and quantitative research approaches to answer the research question. I used qualitative analysis to analyze the steps taken by the exchanges and the responses of the customers for the actions taken by the exchange. To evaluate the positive and negative feedback received from customer, I used sentimental analysis. Table 2 represents the methods and the research paradigms for the papers in the dissertation.

Table 2. Choice of methods and research paradigms

Research Paper	Method	Research Paradigm
Bitcoin: A social movement under attack	Qualitative analysis (Open coding)	Interpretivism
Understanding the creation of trust in cryptocurrencies: The case of Bitcoin	Textual analysis (Semantic similarity)	Positivism
Document verification using blockchain for trust CV information	Design science research methodology	Constructivism
Rebuilding trust in cryptocurrency exchanges after cyber-attacks	Qualitative analysis (Inductive and deductive), sentiment analysis	Interpretivism, positivism

Design science researchers do not believe that the truth exists; they rather believe that artifacts are created to change the world (Purao, 2013). IT artifacts consist of constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems) (Hevner et al., 2004). For a better understanding of how blockchain brings trust to the business process without involving intermediaries, I constructed an IT artifact as a prototype using the design science research methodology for the paper titled "Document verification using blockchain for trusted CV information." Though design science research follows the supervisory structure of management science, it is heavily influenced by computer science and engineering (Purao, 2013). Design science follows the principle of "knowing-via-making," by which new ideas are generated in the process of building an IT artifact (Kuechler & Vaishnavi, 2008). Design science research

ontologically recognizes the evolution in the researcher's instance toward the problem and the artifact and epistemologically observes a convergence between the problem and the artifact (Purao, 2013).

5.2 Data Collection and Analysis

This section provides an overview of the datasets used for all the research papers in this thesis and the various analysis methods used to extract meaningful knowledge from these datasets.

For the paper titled "Bitcoin: A social movement under attack," data were collected from reputed websites like BitCoinTalk, CoinDesk, CNBC, and The Register. Data collected from one website were triangulated with information available on other websites. I performed a content analysis on the data collected from these websites. Content analysis is a technique for compressing many words from a text into fewer content categories based on explicit rules of coding (Stemler, 2001). Framing theory was used to establish Bitcoin as a social movement. The trust deficit created among the investors in the traditional financial institutions due to the collapse of Lehmann Brothers during the 2008 global financial crisis was projected as a problem using diagnostic framing. It is framed that there is a lack of transparency in the operations of traditional financial institutions, and investing in them is no longer a safe option (Coy, 2008). Nakamoto's whitepaper projected Bitcoin as an alternative investment option where there is no involvement of a financial institution for the safety and security of the transactions, which can be seen as prognostic framing. Early Bitcoin users and exchanges promoted Bitcoin as a good option for investors. The features of Bitcoin match the requirements of the solution for the perceived problem. Bitcoin users, exchanges, digital media, social media, online discussion forums, and blogs projecting Bitcoin as a solution can be considered motivational framing. Using content analysis, I was able to identify the vulnerabilities in the exchanges that were being exploited by cyber-attackers. I categorized these vulnerabilities based on the similarities of the natures of the cyber-attacks.

To identify the various factors that impact the creation of trust in cryptocurrencies for the paper "Understanding the creation of trust in cryptocurrencies: The case of Bitcoin," data were scraped from the online forum, Bitcointalk.org, which was founded by Satoshi Nakamoto (Nakamoto, 2009). Bitcointalk.org's online forum is the oldest and most reputed online forum related to Bitcoin and other cryptocurrencies. I used the Beautifulsoup package from the Python language to scrape the postings from the online forum. I collected about 1.97 million posts from the General Discussion subsection of the online forum written between March 1, 2012, and September 21, 2018. My data included original posts and replies to these posts, the dates of each post and reply, and the metadata about the users who made the posts.

I used Doc2Vec textual analysis, as proposed by Le and Mikolov's (2014) model, on the forum data, which generates the vector representation of words and documents through paragraph vectors. After the vector representation of the words and documents, I computed the semantic similarity to identify the

closeness of the posts and words to trust. Semantic similarity is a metric defined over a corpus, by which the similarity is based on the likeness of semantic meaning instead of syntactical representation. Like a classification problem, the model learns the network weight to maximize the prediction of the nearest word. But these networks output the learned weight as a vector and semantic representation of the text rather than the final prediction from the model. To train the Doc2Vec model, I relied on the implementation provided by the Python package Gensim (Rehurek & Sojka, 2010). Among the available models, I trained three different variants of the Doc2Vec model: paragraph vector with a distributed bag of words (PV-DBOW) with doc vectors only, PV-DBOW in a skip-gram model with word vectors trained with document vectors, and PV with distributed memory (PVDM) using the sum. Due to the extensive resource requirements involved in the estimation of PV-DM with concatenation, I omitted it from my potential model alternatives. The results showed that PV-DBOW with documents and words trained together performed better in comparison to other models, making it my preferred choice.

In the paper "Document verification using blockchain for trusted CV information," I built a prototype of a blockchain application for trusted CV information using a design science research methodology. Design science research methodology allows us to create information-systems-based solutions that have the quality, utility, and efficacy to solve a problem. Peffers et al. (2017) divide the design science research process into six steps: identifying a problem, defining the objectives, designing and developing a solution, demonstrating the solution, evaluating the solution, and communicating the research to academia.

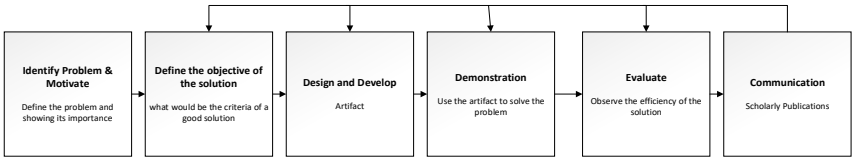


Figure 3. Design science research process (Peffers et al., 2017)

In the paper, I identified the problem as verifying the background information of a job applicant accurately in a short period of time. I defined the objectives of the solution as the reliable verification of the background of a job applicant without any flaws, reduced time consumption so that companies can do background verification immediately during the hiring process, and reduced costs so that small and medium enterprises can do background verification for all their job applicants. I performed several iterations of the design and development phase. I initially designed the solution to save the encrypted document on the blockchain. Later, the solution was redesigned to save just the hash value of the document onto the blockchain as hash value helps to authenticate a given document while keeping the information of the document confidential. As a researcher, it is extremely important to understand how blockchain can create trust in the business process. After designing the solution, I evaluated various platforms, like Ethereum Smart Contracts with Solidity, Corda Framework, and Hyper Ledger Frameworks. After carefully evaluating the pros and cons of each platform, I decided to build my solution on the Hyperledger Fabric framework. I

built the prototype of the design solution using Hyperledger Fabric in the demonstration phase and evaluated my solution in terms of cost, scalability, and accuracy when identifying fake information on a CV. Finally, the paper was published by the 2021 Americas Conference in Information Systems.

Data were collected from multiple online cryptocurrency websites like Coindesk and Cointelegraph for the paper "Rebuilding trust in cryptocurrency exchanges after cyber-attacks" to gather information about major cyber-attacks on cryptocurrency exchanges between 2012 and 2020. I excluded cyber-attacks that were not discussed extensively on the online forum. Finally, I selected seven major cyber-attacks on different cryptocurrency exchanges. Then, I gathered information on how they informed their customers about a given cyber-attack and how they apologized for the violation. I collected the apology information via email, Twitter, website announcements, and press releases. I also gathered information about other trust rebuilding measures that the exchanges took during the months following the cyber-attack. Finally, I extracted the response of the customers and potential customers to the cyber-attacks on the Bitcointalk.org online forum. I used the Beautifulsoup package in Python for web scraping of the posts made by the current and potential customers of the exchange on the apologies made by the exchanges, analyzing a total of over 500 posts.

A cross-case analysis approach was followed in my empirical study. Cross-case analysis facilitates the comparison of commonalities and differences across different cases. I utilized both quantitative and qualitative methods in my study, consisting of three steps. First, I used deductive qualitative analysis for the analysis of apologies made by the exchanges, by using the six components of an effective apology proposed by Polin et al. (2012): an expression of regret, an explanation of the violation, an acknowledgment of responsibility, a declaration of repentance, an offer of repair, and a request for forgiveness.

Second, I used VADER (valence aware dictionary and sentiment reasoner) sentiment analysis to identify the positive and negative sentiments of the user responses to the cyber-attacks. Sentiment analysis is a process through which text is analyzed using natural language processing, and the sentiments of the text are categorized as negative, positive, or neutral (White, 2020). VADER is a lexicon- and rule-based sentiment analysis tool that is specifically attuned to the sentiments expressed in social media. For each statement in the text, VADER provides a fraction of positive, negative, and neutral sentiments.

Finally, I focused more deeply on the users' responses for each exchange and conducted a qualitative analysis using the Atlas.ti software. I aimed to identify the factors that contribute to positive and negative sentiments. For this purpose, I started with open coding of the users' responses for each exchange. Next, I clustered the open codes into larger categories that formed positive and negative themes. This allowed me to identify how exchanges' trust rebuilding measures were received from the customers.

6. Research Findings

My research findings provide deeper insights into various trust aspects of cryptocurrencies and blockchain. They include classifications of vulnerabilities of cryptocurrency exchanges, the impact of cyber-attacks on the value of cryptocurrencies, factors influencing trust in cryptocurrencies, building a prototype of a blockchain use case, and trust rebuilding techniques used by cryptocurrency exchanges. In the following sub-sections, I will discuss the research findings of each paper in detail.

6.1 Bitcoin: A social movement under attack

Cryptocurrency exchanges have been targeted by cyber-attackers with various kinds of cyber-attacks. My research focused on several cyber-attacks and broadly classified the vulnerabilities of the system as code bugs, user errors, and susceptibility to distributed denial of service (DDoS) attacks. The cyber-attacks that occurred due to exploitation of the code written by the exchanges for the security of wallets and transactions are considered code bugs. The cyber-attacks that occurred due to user errors in managing the security of their wallets are termed user errors. In a DDoS attack, the attacker floods the victim's resources with illegitimate requests using multiple compromised computers so that legitimate users cannot access these resources (Yaar et al., 2003).

As the popularity of cryptocurrencies has increased, exchanges have been formed on which investors can buy and sell cryptocurrencies. These exchanges have become targets for cyber-attacks, and cryptocurrencies worth millions of dollars have been lost. The impact of cyber-attacks hampers Bitcoin as a social movement. My research findings show that a cyber-attack on any exchange would not only diminish the value of the exchange but also reduce the overall value of Bitcoin. In 2014, the bankruptcy of Mt.Gox, the biggest Bitcoin exchange, located in Tokyo, Japan, reduced the value of Bitcoin by 36%. Similarly, a cyber-attack on the exchange Bitfinex diminished the value of Bitcoin by 24% (Table 3). Though several other factors constitute the fluctuations in the value of cryptocurrencies, cyber-attacks on cryptocurrency exchanges make their value more volatile.

Table 3. Impact of cyber-attacks on the value of Bitcoin (Marella, 2017)

Event	Reduction (From-To)	Percentage Reduction
Mt.Gox Shut Down	$737 - $472	36%
Bitfinex Attack	$656 - $510	23%
Bitfinex & BTC-e DDoS	$3,000 - $2,571	6%
Mintpal Attack	$634 - $618	2.5%
Flexicon Attack	$661 - $625	5%
Bitstamp Attack	$288 - $265	8%

Some exchanges do not disclose any information about cyber-attacks, while a few exchanges provide vague information about the attacks. When the Mt.Gox exchange lost 450 million dollars in a cyber-attack, the exchange merely posted a note saying that the "decision was taken to close all transactions for the time being." If the cyber-attacks incur huge losses, exchanges do not provide any information to the customers and shut down their services. Exchanges sometimes lose their confidence and make very negative statements in conveying information about the cyber-attack to customers. BitCash informed customers of an attack by saying, "Unfortunately, the nightmare became a reality" (Bradbury, 2013). This kind of irresponsible behavior by exchanges creates more distrust among Bitcoin investors.

The exchanges charged lesser transaction fees during the initial days of Bitcoin. As the volume of the transactions increased in the Bitcoin network, the transaction fees for buying and selling bitcoins increased. The rapid increase in the number of Bitcoin transactions resulted in a two-tier Bitcoin transaction processing system by which the miners gave high priority to transactions with high transaction fees and low priority to transactions with low transaction fees. Cyber-attacks on cryptocurrency exchanges and the high transaction fees hamper the social movement started by cryptocurrencies like Bitcoin.

6.2. Understanding the creation of trust in cryptocurrencies: The case of Bitcoin

In this paper, I explore various attributes of the technology that creates trust among the users of Bitcoin. To search for the constructs, I listed the keywords representing functionality, reliability, and helpfulness in the context of blockchain technology and cryptocurrencies from the literature. For functionality, I searched for keywords such as transfers, decentralization, immutability, and openness. Similarly, to identify reliability-related posts, I searched for posts closest to the keywords stability, regulation, knowledge, and security. Finally, I used keywords such as investments, profits, and alternative currency as words associated with the helpfulness construct. I calculated the semantic closeness of these attributes to the word "trust" in the corpus of 1.97 million postings from Bitcointalk.org. My research shows that openness, immutability, and transfer are three technological attributes that are semantically close to trust (Figure 4).

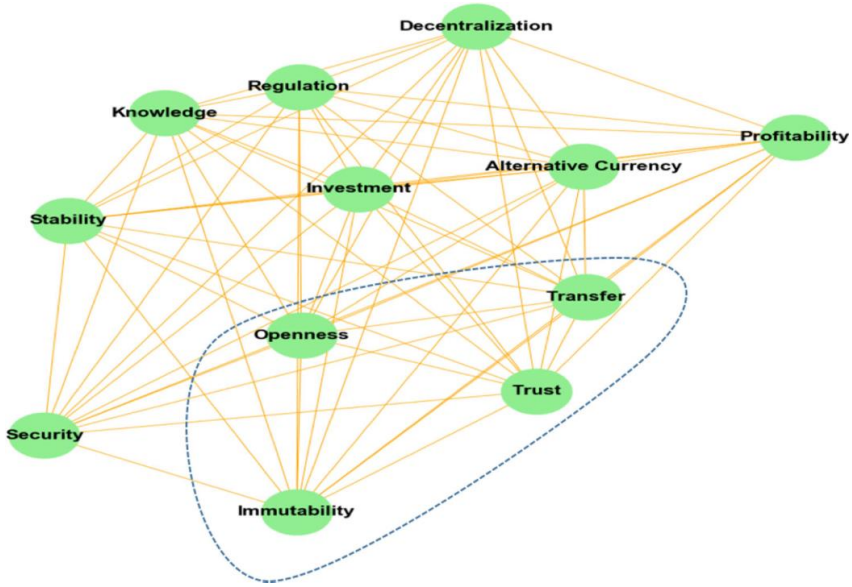


Figure 4. Semantic proximity network representation of trust and its associated attributes (Marella et al., 2020)

6.3. Document verification using blockchain for trusted CV information

I built a blockchain prototype to solve the problem of fake information in the CB submitted by a job applicant in the hiring process. The prototype was built using Hyperledger Fabric, an open-source permissioned DLT that offers high modularity supporting external plugin components, performance scalability, and configurable architecture compared to other blockchain technologies. The organizations that take part in building Hyperledger Fabric network are called members. Universities, companies, doctors, police, and certification authorities are all members. Each of the members in the consortium blockchain would be provided with at least three entities: peer, administrator, and certification authority. The peer is the entity responsible for submitting new documents to the blockchain. The administrator of the organization verifies the authenticity of the documents and approves them. Then, the hash value of the documents, along with the hash of the identification (Social Security Number + Last name), are updated on the blockchain by the orderer, and the transaction is updated by all the orderers in the network. The certification authority is the entity responsible for giving certificates to the administrators and peers. Once all the transactions are saved into blocks, these blocks are distributed to all the other peers in the network (Hyperledger, 2019). A recruiter of an organization will act as the verifier of a job applicant's document and obtains a verifier certificate from the verifier organization. My solution is efficient, time-saving, and less costly than the conventional background verification process practiced across various companies (Figure 5).

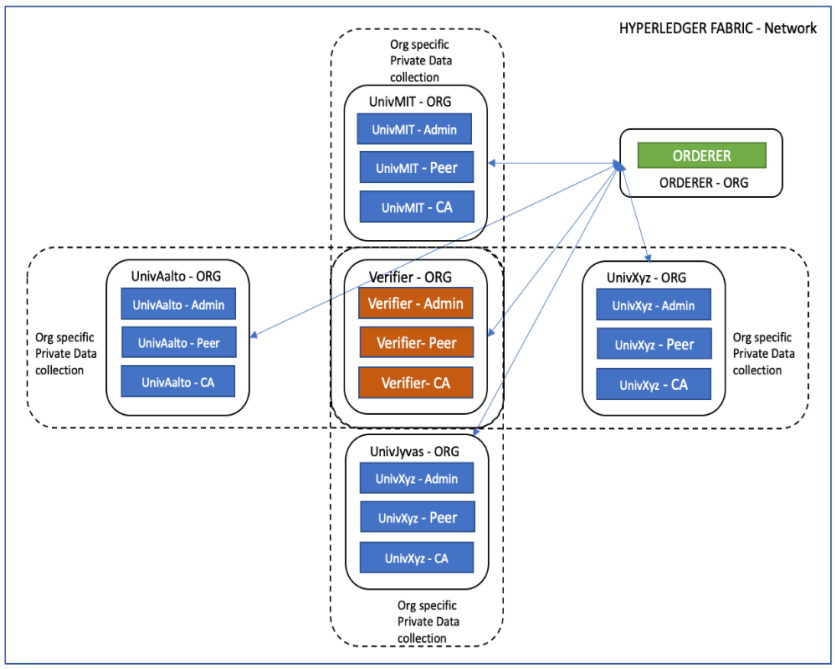


Figure 5. Architecture of the Hyperledger Fabric consortium blockchain (Marella & Vijayan, 2020)

6.4. Rebuilding trust in cryptocurrency exchanges after cyber-attacks

I explored trust rebuilding techniques adopted by seven different cryptocurrency exchanges after a cyber-attack. My findings show that an apology itself is not enough to rebuild trust among customers after a cyber-attack. The BitCash exchange only made an apology without implementing any other trust rebuilding mechanisms and consequently cumulated only 33% positive sentiments.

Compensation plays a crucial role in rebuilding trust. All the exchanges that offered compensation received high positive sentiments from customers. Binance (54%), Coincheck (69%), Bitcoinica (56%), and BitFloor (55%) are examples of such exchanges. However, if there are repeated cyber-attacks, compensation may not be a useful technique to rebuild trust. Bithumb and BitStamp compensated their customers, but they received 35% and 24% positive sentiments, respectively, due to the repetition of cyber-attacks. I also found that the reputation of the exchange plays an important role in rebuilding trust. Binance has a good reputation for protecting customers' wallets against cyber-attacks, and it has a separate fund set aside to compensate customers when necessary. So, the exchange received 54% positive sentiments from the forum users. Similarly, BitFloor received 55% positive sentiments from forum users due to its good reputation. I found that merging with a reputed organization is a structural change that could help in rebuilding trust among customers. Coincheck merged with Monex Group after being hit by its biggest cyber-attack and losing 532 mil-

lion dollars (Wood, 2018). Coincheck compensated its customers before merging with Monex Group. Hence, the exchange received 69% positive sentiment from its users.

The following table represents the motivation and contribution of each paper in the dissertation.

Table 4. Contributions of research papers

Motivation	Research Paper	Contributions
To understand Bitcoin and how it is a social movement.	*Bitcoin: A social movement under attack*	The paper explains how bitcoin differs from traditional financial institutions and how it is framed as a social movement. It also provides literature on cyber-attacks on crypto exchanges and their impact on Bitcoin.
After studying how Bitcoin differs from traditional financial institutions in paper 1, (i.e., absence of central authority), I wanted to explore the factors that create trust in cryptocurrencies.	*Understanding the creation of trust in cryptocurrencies: The case of Bitcoin*	The paper identifies that immutability and openness are the features of blockchain that create trust in cryptocurrencies.
After understanding how blockchain creates trust in cryptocurrencies in paper 2, I wanted to explore how blockchain can be applied in other business scenarios.	*Document verification using blockchain for trust CV information*	The paper produced a working prototype of a blockchain application for a reliable hiring process.
Paper 1 explains the impact of cyber-attacks on cryptocurrencies. This motivated me to understand how exchanges rebuild trust among customers after a cyber-attack.	*Rebuilding trust in cryptocurrency exchanges after cyber-attacks*	The research findings of the paper present the existing trust rebuilding techniques implemented by the exchanges.

7. Discussion

Cryptocurrencies like Bitcoin are a relatively new phenomenon for both academicians and practitioners. Unlike other emerging technologies, which are primarily studied in computer science and information systems, the scope of cryptocurrencies expands over a wide area of research, including computer science, finance, economics, and information systems (Giudici et al., 2020). Blockchain technology, which is the underlying technology of cryptocurrencies, has applications in a wide variety of domains like supply chain management, music and art, land registrations, finance, food traceability, and healthcare (Pilkington, 2016). This dissertation explores these two technologies and uncovers how trust is created in cryptocurrencies and how blockchain technology can bring trust in a business scenario.

I explained how Bitcoin is considered a social movement in the finance industry using framing theory. Unlike any traditional financial institution, Bitcoin operates without a central authority and offers high transparency for its transactions, low transaction fees, and high returns on investment. However, as the popularity of cryptocurrencies has grown, cryptocurrency exchanges have become the potential targets of the cyber-attackers. Cryptocurrencies worth millions of dollars are lost in cyber-attacks, and the exchanges are not always transparent about these attacks with their customers. These attacks have prompted a reduction in the value of cryptocurrencies. Hence, I consider that these cyber-attacks are a threat to the social movement started by cryptocurrencies.

In the paper "Bitcoin: a social movement under attack", I discuss the case of Students for a Democratic Society as an example to explain the situation of Bitcoin. In the 1960s, Students for a Democratic Society emerged in the United States from the liberal ideologies of the young Americans at that time. They advocated nonviolent civil disobedience as a tool to bring participatory democracy to student youth. The rapid growth of the organization led to its collapse. Though SDS advocated non-violence, the organization became violent on the issues like the Vietnam War. The organization broke into several factions and implemented terrorist tactics in its operation. By 1969, Students for a Democratic Society was dissolved due to increased factionalism within its ranks. Similar to Students for a Democratic Society (SDS), Bitcoin might fail to capitalize on its success due to cyber-attacks (Organization, n.d.). Despite the huge demand for Bitcoin today, these cyber-attacks can pose a threat to Bitcoin as a social movement (Freeman, 1999).

After studying how Bitcoin operates without a central authority in paper titled "Bitcoin: a social movement under attack", I delved deeply into the trust aspects

of cryptocurrencies by exploring various attributes of technology that create trust among the users of cryptocurrencies like Bitcoin in the paper "Understanding the creation of trust in cryptocurrencies: The case of Bitcoin". The results produced using the Doc2Vec model showed that trust is semantically close to immutability, openness, and transfers. Bitcoin makes the international transfer of coins faster with a low transactional fee (Bamert et al., 2013). So, traditional banks are now exploring blockchain technology to make international money transfers faster and cheaper for their customers (Shane, 2018). Immutability and openness are attributes of cryptocurrencies that are provided by the underlying technology. Immutability of the ledger brings safety and security to the transactions, while openness refers to the availability of the data in the Bitcoin ledger to everyone. The openness of the ledger creates transparency while immutability offers accountability. Transparency is the key element to creating trust (Grimmelikhuijsen & Welch, 2012). The degree of transparency and accountability offered by cryptocurrencies like Bitcoin is unparallel by any traditional financial institution.

After understanding that the technical attributes of blockchain technology that create trust in cryptocurrencies from the results of paper "Understanding the creation of trust in cryptocurrencies: The case of Bitcoin", I explored the potential of blockchain in a different domain, the recruitment industry, in paper "Document verification using blockchain for trust CV information". I built a prototype of a solution for the problem of verifying the authenticity of the documents provided by a job applicant in the hiring process. My prototype reduces costs, saves time, and is accurate in verifying the authenticity of documents. The prototype is substantial evidence of how blockchain can be disruptive. The prototype built in the paper is very generic, and with a few changes, the solution can be used in various other domains like verification of land record documents and digital notary.

As discussed in "Bitcoin: a social movement under attack", cyber-attacks are detrimental to cryptocurrencies, and cryptocurrency users can lose their trust not only in the exchange but also in cryptocurrencies in general. In paper 4, I examine how cryptocurrency exchanges rebuild trust among their customers after cyber-attacks. My research suggests that an apology from the exchange with full acceptance of responsibility for failing to prevent the cyber-attack is insufficient to rebuild trust. The exchanges need to fulfill the promises made in the apology. This supports Schweitzer et al. (2006), who conclude that a mere apology will not likely lead to trust repair.

Among the various trust rebuilding methods adopted by cryptocurrency exchanges, compensation is the best technique to rebuild trust among customers. It supports the claim of Bottom et al. (2002) that financial compensation would better restore trust among customers compared to just an apology. However, if the exchanges are subjected to repeated cyber-attacks, then compensation does not have much impact on rebuilding trust. The research findings also suggest that the reputation of the exchange plays a key role in rebuilding trust among customers of the exchange. Finally, the research results indicate that a merger

can be a structural solution to rebuild trust among customers. Merger as a potential solution to rebuild trust is never discussed in literature about rebuilding trust. Hence, mergers as a trust rebuilding technique can be explored further.

8. Implications

The papers in this dissertation made a few theoretical contributions and practical implications, which I will discuss in detail in this section. Later, I will discuss the limitations of and suggestions for future research on the papers.

8.1 Theoretical Contributions

All the papers included in this thesis focus on trust aspects related to cryptocurrencies and blockchain. The papers in the dissertation contribute to the literature on vulnerabilities in cryptocurrency exchanges, trust creation in cryptocurrencies, prototyping of a blockchain application to create trust for a business use case, and rebuilding trust in cryptocurrency exchanges.

The paper titled "Bitcoin: A social movement under attack" provides information on various vulnerabilities in cryptocurrency exchanges. The research identified code bugs, users errors, and susceptibility to DDoS attacks as common vulnerabilities of exchanges that cyber-attackers exploit.

The paper on understanding the creation of trust in cryptocurrencies makes contributions to the trust literature in cryptocurrencies. The textual analysis performed on 1.97 million posts from Bitcointalk.org identifies that the immutability and openness of ledgers as the technological attributes that create trust in cryptocurrencies. Second, we identified that these technological attributes replace the human component of trust in the business process as cryptocurrencies operate in the absence of a central authority. These results are not exclusive to cryptocurrencies they can be generalized to other blockchain-based applications.

The paper on rebuilding trust in cryptocurrency exchanges after cyber-attacks contributes to the literature on rebuilding trust in cryptocurrency exchanges. My research findings show that mergers can be an effective trust rebuilding technique. When an organization loses customer trust, it may consider merging with another reputed organization to rebuild trust among its customers. The existing literature only proposes regulation (Dirks et al., 2011) and hostage posting (Nakayachi & Watabe, 2005) as structural solutions to rebuilding trust. My paper proposes mergers as another solution. The research suggests that the compensation and reputation of the exchange (organization) play a major role in rebuilding trust among customers. Reputed exchanges that were subjected to repeated cyber-attacks were unsuccessful in rebuilding trust. My paper contrib-

utes to the literature on rebuilding trust in organizations that operate completely online without a physical presence in general and cryptocurrency exchanges specifically.

8.2 Practical Implications

The practical implication of the research include providing several guidelines for exchanges to protect themselves from cyber-attacks, providing insights into how to build trust in blockchain applications, demonstrating how a blockchain application can create trust in the business process, and suggesting some effective trust rebuilding techniques for exchanges to adopt after cyber-attacks.

Cyber-attacks on cryptocurrency exchanges pose a threat to the social movement started by cryptocurrencies. Cyber-attacks diminish the value of cryptocurrencies and make them very volatile. I recommend that exchanges need to eliminate cyber-attacks by cooperating and sharing knowledge about the nature of cyber-attacks with other exchanges. Furthermore, the proof of work consensus mechanism not only consumes electricity but also consumes a significant amount of time (10 minutes to add each block) (Hertig, 2020), which creates a bottleneck in processing transactions and thereby increases transaction fees. Hence, it is recommended to use proof of stake to overcome the problem of high transaction fees.

From the research on understanding the creation of trust in cryptocurrencies, I identify the openness and immutability of the ledger as the technological attributes that create trust in cryptocurrencies. Openness offers transparency, while immutability creates accountability. Blockchain is not a requirement for every application, and blockchain's value can be realized only when it is applied to a business process where there is a lack of transparency and accountability. My research suggests that organizations should develop blockchain applications to explore the business use cases where there is a lack of transparency and accountability and utilize the value offered by blockchain. Since several blockchain-based applications are still in the early stages of development, the business owners must highlight these attributes of blockchain to create trust among the users of the application.

In the next paper, I develop a prototype for a solution using blockchain to identify the fake information provided by job applicants in the hiring process. The paper demonstrates the step-by-step process of building a blockchain solution to a business problem where there is a lack of transparency in the process. The solution is highly scalable and can be extended to any geographic location easily. The solution satisfies the properties of confidentiality, integrity, and availability, which are fundamental to any security system (Coss & Samonas, 2014). The solution built for the problem is generic and can be used in various other domains.

In the final paper "Rebuilding trust in cryptocurrency exchanges after cyber-attacks", I suggested several guidelines for the exchanges to rebuild trust among customers. Cryptocurrency exchanges operate online without any physical presence. Due to the impact of the COVID-19 pandemic, several organizations have

moved their operations online and have fewer face-to-face interactions with customers. Hence, the research findings from this study apply to several organizations and are not just limited to cryptocurrency exchanges. My research also reveals that the reputation of an exchange plays a crucial role in rebuilding trust. Therefore, exchanges need to provide high-quality services to maintain good reputations among customers. It was also found that offering an effective apology with all the six components suggested by Polin et al. (2012) would help to rebuild trust. Hence, I recommend that cryptocurrency exchanges need to make effective apologies as an initial step to rebuild trust among customers.

8.3 Limitations of Research

My research has certain limitations. Data collected for the paper "Understanding the creation of trust in cryptocurrencies: The case of Bitcoin" are from the online forum Bitcointalk.org. The members of the forum may or may not be Bitcoin users. Hence, the research results are not exclusive to the opinions of actual users. Furthermore, we do not have information about the forum members' technical skills or understanding of blockchain and Bitcoin. Hence, our research findings reflect the opinions of individuals with different levels of knowledge and understanding of cryptocurrencies.

For the paper "Rebuilding trust in cryptocurrency exchanges after cyber-attacks", the secondary data collected consist of the responses to exchanges' apologies to cyber-attacks. These responses are not exclusive to the customers of the exchanges. Hence, we consider them to be the opinions of both the current and potential customers of the exchange.

8.4 Future Research

The paper "Rebuilding trust in cryptocurrency exchanges after cyber-attacks" can be extended by collecting more data on cyber-attacks on cryptocurrency exchanges. The current research considers the opinions of both current customers and potential customers of exchanges. Future research can be conducted by focusing exclusively on the opinions of the current customers of the exchanges. Moreover, the paper has explored only seven cases of cyber-attacks; it can be extended to at least twenty cases of cyber-attacks. The research can also be improved by collecting historical data on the trading volume of the exchanges to assess the impact of trust rebuilding measures taken by the exchanges.

The applicability of the research in the paper "Document verification using blockchain for trusted CV information" can be enhanced further. The trust aspect of the blockchain prototype is not thoroughly investigated in the current version of the paper. The paper can be further extended by study how the prototype brings trust to the business process. The application can also be used by employment offices to verify the work histories of unemployed people. Similarly, the application can be used by funding agencies to verify the transcripts of students for providing funding. I plan to include these two stakeholders in the solution.

9. Conclusion

This doctoral dissertation contributes to the literature on trust in the domain of blockchain and cryptocurrencies by studying the creation, application, and rebuilding of trust. The dissertation identifies and highlights the features of blockchain technology in creating trust among the users of cryptocurrencies. Cryptocurrencies offer a high degree of transparency and accountability through an open and immutable ledger, which are the inherent features of blockchain. The dissertation not only demonstrates the application of blockchain in a business scenario but also explains how blockchain can create trust and improve the efficiency of the process. Blockchain is still an emerging technology, and the productivity of blockchain applications is uncertain. My prototype illustrates the efficiency of blockchain in terms of cost, time, and accuracy.

Cyber-attacks on cryptocurrency exchanges pose a serious threat to cryptocurrencies. Whenever these cyber-attacks happen, customers might lose their trust not only in a specific exchange but also in cryptocurrencies in general. Hence, it is extremely important for the exchanges to rebuild trust among their customers after cyber-attacks. This research is not only applicable in the context of cryptocurrency exchanges but also generalizable to organizations that provide their services virtually. The research results underscore the pivotal role that compensation plays in rebuilding trust among the customers of an exchange and also provide new insight into using mergers as a structural solution to rebuild trust among the customers. Mergers as a structural solution to rebuild trust can be researched further in the context of online service providers.

Blockchain, unlike artificial intelligence, has yet to prove its applicability (Lindman et al., 2020). It has been over a decade since the inception of Bitcoin, yet there are no successful large-scale implementations of blockchain other than cryptocurrencies. This can create doubts among organizations about whether blockchain is practically feasible for their businesses. My dissertation emphasizes the features of blockchain that create trust among the users of cryptocurrencies. It also focuses on how these features of blockchain can transform the business process in a different domain and showcase the advantages of using blockchain. Cryptocurrency is the only exemplary application of blockchain, and the success of cryptocurrencies drives the large-scale implementation of blockchain. However, cyber-attacks on cryptocurrency exchanges hamper trust in cryptocurrencies, which is detrimental to the implementation of blockchain in other domains. Hence, my dissertation proposes some of the best trust rebuilding techniques adopted by various cryptocurrency exchanges to rebuild trust

among their customers. This dissertation outlines various trust aspects of blockchain and cryptocurrencies, which are extremely important for the large-scale adoption of any emerging technology.

10. References

Agrawal, R. (2018). Digital signature from blockchain context. Retrieved from https://ravikantagrawal.medium.com/digital-signature-from-blockchain-context-cedcd563eee5

Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., & Welten, S. (2013). Have a snack, pay with Bitcoins. Proceedings from *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013*. https://doi.org/10.1109/P2P.2013.6688717

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain—The gateway to trust- free cryptographic transactions. Proceedings from *Twenty-Fourth European Conference on Information Systems (ECIS)*, 5-16.

Benbasat, I., & Wang, W. (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

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Academy of Management*, *26*(2000), 611-639. Retrieved from http://www.jstor.org/stable/223459

Bierer, T. (2016). Hashing it out: Problems and solutions concerning cryptocurrency used as article 9 collateral. *Journal of Law, Technology & the Internet*, *7*, 79-96.

Bies, R. J., & Tripp, T. M. (2015). *Beyond Distrust. "Getting even" and the need for revenge*. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 246–260). Sage Publications, Inc.

Bigley, G. A., & Pearce, J. L. (1998). Straining for shared meaning in organization science: Problems of trust and distrust. *Academy of Management Review*, *23*(3), 405-421.

Bloomenthal, A. (2020). *What Determines the Price of 1 Bitcoin?* Investopedia. https://www.investopedia.com/tech/what-determines-value

Bogusz, C. I., Laurell, C., Sandström, C., & Sandström, C. (2020). Tracking the digital evolution of entrepreneurial finance: The interplay between crowdfunding, blockchain technologies, cryptocurrencies, and initial coin offerings. *IEEE Transactions on Engineering Management*, *67*(4), 1099-1108. https://doi.org/10.1109/TEM.2020.2984032

Bozic, B., & Kuppelwieser, V. G. (2019). Customer trust recovery: An alternative explanation. *Journal of Retailing and Consumer Services*, *49*, 208-218.

Bradbury, D. (2013). Czech bitcoin exchange Bitcash.cz hacked and up to 4,000 user wallets emptied. Retrieved from https://www.coindesk.com/czech-bitcoin-exchange-bitcash-cz-hacked-4000-user-wallets-emptied

Brezo, F., & Bringas, P. G. (2012). Issues and risks associated with cryptocurrencies such as Bitcoin. *The Second International Conference on Social Eco-Informatics*, 20-26.

Bucko, J. (2015). *Security and trust in cryptocurrencies*.

Bucko, J., Pal'ová, D., & Vejacka, M. (2015). Security and trust in cryptocurrencies. Proceedings from *Central European Conference in Finance and Economics*, 14-24.
Canavera, K. (2021). Rebuilding trust. *Patient Education and Counseling*, *104*(5), 996-997. https://doi.org/10.1016/j.pec.2021.01.040
Casey, M. J., & Vigna, P. (2018). In blockchain we trust. *MIT Technology Review*, 10-16.
Cassiopeia Services. (2020). Bitcoin is just the tip of the iceberg: Exploring blockchain's full potential. Retrieved from https://fintechweekly.com/magazine/articles/bitcoin-is-just-the-tip-of-the-iceberg-exploring-blockchain-s-full-potential
Chandra, S., Srivastava, S. C., & Theng, Y.-L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems*, *27*(29), 561-588. https://doi.org/10.17705/1cais.02729
Choi, J., & Nazareth, D. L. (2005). Rebuilding consumer trust in e-Commerce relationships. Proceedings from *Association for Information Systems - 11th Americas Conference on Information Systems, AMCIS 2005: A Conference on a Human Scale*, *1*, 390-394.
Chong, D., & Druckman, J. N. (2007). Framing theory. *Annual Review of Political Science*, *10*(1), 103-126. https://doi.org/10.1146/annurev.polisci.10.072805.103054
CoinMarketCap. (2020). Retrieved from www.CoinMarketCap.com
Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, *2*(3), 203-215.
Coss, D., & Samonas, S. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21-45.
Dalton, C., & Choo, T. H. (2001). An operating system approach to securing e-services. *Communications of the ACM*, *44*(2), 58-64.
De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284. https://doi.org/10.1016/j.techsoc.2020.101284
Deutsch, M. (1985). *Distributive justice: A social-psychological perspective*.
DeVries, P. D. (2016). An analysis of cryptocurrency, Bitcoin, and the future. *International Journal of Business Management and Commerce*, *1*(2), 1-9.
Diniz, E., Porto, R. M., & Adachi, T. (2005). Internet banking in Brazil: Evaluation of functionality, reliability and usability. *Evaluation*, *8*(June), 41-50.
Dirks, K. T., Kim, P. H., Ferrin, D. L., & Cooper, C. D. (2011). Understanding the effects of substantive responses on trust following a transgression. *Organizational Behavior and Human Decision Processes*, *114*(2), 87-103.
Dirks, K. T., Lewicki, R. J., Zaheer, A., & Dirks, K. T. (2018). Introduction to special topic forum: Repairing relationships within and between organizations: Building a conceptual foundation. *Academy of Management Review*, *34*(1), 68-84.
The Economist. (2015). Blockchain—The next big thing. Retrieved from http://www.economist.com/news/%0Aspecial-report/21650295-orit-next-big-thing
Finkel, E. J., Rusbult, C. E., Kumashiro, M., & Hannon, P. A. (2002). Dealing with betrayal in close relationships: Does commitment promote forgiveness? *Journal of Personality and Social Psychology*, *82*(6), 956-974. https://doi.org/10.1037/0022-3514.82.6.956
Flores, F., & Solomon, R. C. (1998). Creating trust. *Business Ethics Quarterly*, *2*, 205-232.

Freeman, V. J. J. (1999). *Waves of protest: Social movements since the sixties*. Rowman and Littlefield Publishers.
Friedman, B., Khan, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34-40. https://doi.org/10.1145/355112.355120
Gail, E. (2018). Digital currencies: An Iran, Venezuela saviour amid sanctions and inflation? Retrieved from: https://coincentral.com/digital-currencies-an-iran-venezuela-saviour-amid-sanctions-and-inflation/
Gambetta, D. (1988). *Trust: Making and breaking cooperative relations*. New York: B. Blackwell New York.
Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: Market analysis and perspectives. *Journal of Industrial and Business Economics*, *47*(1), 1-18. https://doi.org/10.1007/s40812-019-00138-6
Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin—Asset or currency? Revealing users' hidden intentions. *Twenty Second European Conference on Information Systems*, 1-14.
Grabner-Kräuter, S., Bitter, S., & Grabner-Kra, S. (2015). *Forum for social economics trust in online social networks: A multifaceted perspective*. In Forum for social economics, 44(1), 48-68 Routledge. https://doi.org/10.1080/07360932.2013.781517
Grimmelikhuijsen, S. G., & Welch, E. W. (2012). Developing and testing a theoretical framework for computer-mediated transparency of local governments. *Public Administration Review*, *72*(4), 562-571. https://doi.org/10.1111/j.1540-6210.2011.02532.x
Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Sage.
He, D. (2018). Monetary Policy In The Digital Age: Crypto assets may one day reduce demand for central bank money. 55(2), 13-16.
Hertig, A. (2020). What is proof-of-work? Retrieved from https://www.coindesk.com/what-is-proof-of-work
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1), 75-105. https://doi.org/10.2307/25148625
Imber, J. B. (2017). How navigating uncertainty motivates trust in medicine. *AMA Journal of Ethics*, *19*(4), 391-398.
Kaiserman, S. (2018). Bitcoin is to blockchain as email was to the internet. Retrieved from https://www.linkedin.com/pulse/bitcoin-blockchain-email-internet-sheri-kaiserman/
Kotenko, I., & Ulanov, A. (2014). Agent-based simulation of DDOS attacks and defense mechanisms. *International Journal of Computing*, *4*(2), 113-123.
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.
Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: Anatomy of a research project. *European Journal of Information Systems*, *17*(5), 489-504.
Lankton, N., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into expectation disconfirmation theory. *The Journal of Strategic Information Systems*, *23*(2), 128-145. https://doi.org/10.1016/J.JSIS.2013.09.001
Lankton, N., McKnight, D. H., & Tripp, J. (2015a). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 880-918. https://doi.org/10.17705/1jais.00411
Le, Q., & Mikolov, T. (2014). Distributed representations of sentences and documents. Proceedings of *International Conference on Machine Learning*, *31*. https://doi.org/10.1145/2740908.2742760
Lee, J. D., & See, K. A. (2009). Trust in automation: Designing for appropriate

reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50-80. https://doi.org/10.1518/hfes.46.1.50_30392
Lee, John 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
Lee, M. K. O., Turban, E., Lee, M. K. O., & Turban, E. (2014). *A trust model for consumer internet shopping*. *4415*(2001). https://doi.org/10.1080/10864415.2001.11044227
Leighton, B. (2019). What is a cryptocurrency exchange and how do they work? Retrieved from https://www.coininsider.com/cryptocurrency-exchanges/
Lewicki, R., & Bunker, B. (1995). *Trust in relationships: A model of development and decline*.
Lewicki, R. J., & Tomlinson, E. C. (2014). Trust, trust development, and trust repair. In *The handbook of conflict resolution: Theory and practice* (pp. 104-137).
Lewis, J. D., Weigert, A., & Dame, U. N. (1985). *Trust as a social reality *. 1*, 967-985.
Lindman, J., Berryhill, J., & Welby, B. (2020). The uncertain promise of blockchain for government. *OECD Working Papers on Public Governance*, *43*.
Luhmann, N. (1979). *1979 Trust and power*. Chichester: Wiley.
Marella, V., & Vijayan, A. (2020). Document Verification using Blockchain for Trusted CV Information. Proceedings from *Americas Conference on Information Systems— 2020, 12*, 1-10. https://aisel.aisnet.org/amcis2020/adv_info_systems_research/adv_info_systems_research/12
Marella, V. (2017). Bitcoin: A social movement under attack. *Selected Papers of the IRIS, 8*(8), 147-163. http://aisel.aisnet.org/iris2017/1
Marella, Venkata, Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Journal of Electronic Markets*. https://doi.org/10.1007/s12525-019-00392-5
McCarthy, J. D., & Zald, M. N. (1977). Resource mobilization and social movements: A partial theory. *American Journal of Sociology*, *82*(6), 1212-1241. https://doi.org/10.1086/226464
McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). 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, H., Carter, M., Thather, J., & Clay, P. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(12), 12-32.
Mendoza-Tello, J. C., Mora, H., Pujol-López, F. A., & Lytras, M. D. (2018). Social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments. *IEEE Access*, *6*, 50737-50751. https://doi.org/10.1109/ACCESS.2018.2869359
Naber, A. M., Payne, S. C., & Webber, S. S. (2018). The relative influence of trustor and trustee individual differences on peer assessments of trust. *Personality and Individual Differences*, *128*(June 2019), 62-68. https://doi.org/10.1016/j.paid.2018.02.022
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin: A Peer-to-Peer Electronic Cash System*.
Nakamoto, S. (2009). Summary-satoshi. Retrieved from https://bitcointalk.org/index.php?action=profile;u=3
Nakayachi, K., & Watabe, M. (2005). Restoring trustworthiness after adverse

events: The signaling effects of voluntary "hostage posting" on trust. *Organizational Behavior and Human Decision Processes*, *97*(1), 1-17. https://doi.org/10.1016/j.obhdp.2005.02.001
Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton University Press.
Nilsson, M., Adams, A., & Herd, S. (2005). Building security and trust in online banking. Proceedings of *Conference on Human Factors in Computing Systems*, 1701-1704. https://doi.org/10.1145/1056808.1057001
Organization, A. (n.d.). *Students for a Democratic Society*. https://www.britannica.com/topic/Students-for-a-Democratic-Society
Oshodin, O., Molla, A., & Ong, C. E. (2016). An information systems perspective on digital currencies: A systematic literature review. Proceedings of *The 27th Australasian Conference on Information Systems, ACIS 2016*.
Paravastu, N., Gefen, D., & Creason, S. (2014). Understanding trust in IT artifacts—An evaluation of the impact of trustworthiness and trust on satisfaction with antiviral software. *Data Base for Advances in Information Systems*, *45*(4), 30-50. https://doi.org/10.1145/2691517.2691520
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2017). *A design science research methodology for information systems research 1222*(August). https://doi.org/10.2753/MIS0742-1222240302
Peter T. Coleman, & Morton Deutsch, E. C. M. (2014). *The handbook of conflict resolution: Theory and practice* (3rd ed.).
Pilkington, M. (2016). Blockchain technology: Principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing.
Polin, B., Lount, R. B., & Lewicki, R. J. (2012). On the importance of a full apology: How to best repair broken trust. *Academy of Management Proceedings*, *2012*(1), 14152.
Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *ArXiv*, 1-13.
Pratt, M. G., & Dirks, K. T. (2007). *Rebuilding trust and restoring positive relationships: A commitment-based view of trust*.
Purao, S. (2013). Truth or dare: The ontology question in design science research. *Journal of Database Management*, *24*(3), 51-66. https://doi.org/10.4018/jdm.2013070104
Quentson, A. (2016). Retrieved from https://bitcoinmagazine.com/%0Aarticles/how-bitcoin-and-blockchain-can-avert-systemic-bank-collapses-1461170796/
Ratnasingam, P. (2005). E-Commerce relationships: The impact of trust on relationship continuity. *International Journal of Commerce and Management* 15(1), 1-16.
Rehurek, R., & Sojka, P. (2010). Software framework for topic modelling with large corpora. *LREC Workshop on New Challenges for NLP Frameworks*, 45-50. Retrieved from http://www.muni.cz/research/publications/884893
Robinson, S. L. (1996). Trust and breach of the psychological contract. *41*(4), 574–599. Retrieved from https://www.jstor.org/stable/2393868 REFEREN.
Roger C. Mayer, Davis, J. H., and Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management*, *20*(3), 709-734.
Roman, D., & Stefano, G. (2016). Towards a reference architecture for trusted data marketplaces: The credit scoring perspective. Proceedings of the *2nd International Conference on Open and Big Data, OBD 2016*, 95-101. https://doi.org/10.1109/OBD.2016.21
Rusbult, C. E., & Martz, J. M. (1995). Remaining in an abusive relationship: An investment model analysis of nonvoluntary dependence. *Personality and Social Psychology Bulletin*, *21*(6), 558-571.

Sadhya, V., Hirschheim, R., & Watson, E. (2018). *Exploring technology trust in Bitcoin: The blockchain exemplar*. Proceedings of ECIS conference.
Sas, C., & Khairuddin, I. (2017). Design for trust an exploration of the challenges and opportunities of Bitcoin users. Proceedings of *The 2017 CHI Conference on Human Factors in Computing Systems*, 6499-6510. https://doi.org/10.1145/3025453.3025886
Schniter, E., Sheremeta, R. M., & Sznycer, D. (2013). Building and rebuilding trust with promises and apologies. *Journal of Economic Behavior & Organization*, *94*, 242-256.
Schweitzer, M. E., Hershey, J. C., & Bradlow, E. T. (2006). Promises and lies: Restoring violated trust. *Organizational Behavior and Human Decision Processes*, *101*(1), 1-19. https://doi.org/10.1016/j.obhdp.2006.05.005
Seeger, A. M., Neben, T., & Heinzl, A. (2017). Information failures, trust violation, and customer feedback in web-enabled transactions: The role of causal transparency as a trust repair mechanism. Proceedings of *The 25th European Conference on Information Systems, ECIS 2017*, *2017*, 2017-2033.
Shane, D. (2018). $530 million cryptocurrency heist may be biggest ever. Retrieved from https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html
Simons, T., & Parks, J. M. (2000). The sequential impact of behavioral integrity on trust, commitment, discretionary service behavior, customer satisfaction, and profitability. Cornell University Center for Hospitality Research.
Snow, D. A., & Benford, R. D. (1988). Ideology, frame resonance, and participant mobilization. *International Social Movement Research*, *1*(1), 197-217.
Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., & Leimeister, J. M. (2012). Understanding the formation of trust in IT Artifacts—Socio-technical design of ubiquitous computing systems. Proceedings of *The International Conference on Information Systems (ICIS)*, *2012*, 39-58. https://doi.org/10.1007/978-3-319-05044-7_3
Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research and Evaluation*, *7*(17), 2000-2001. https://doi.org/10.1362/146934703771910080
Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Penguin.
Thagard, P. (2018). What is trust? Retrieved from https://www.psychologytoday.com/us/blog/hot-thought/201810/what-is-trust
Thieme, P. (1960). The "Aryan" gods of the Mitanni Treaties. *Journal of the American Oriental Society*, 80 (14) 301-317.
Tomlinson, E. C., & Mryer, R. C. (2009). The role of causal attribution dimensions in trust repair. *Academy of Management Review*, *34*(1), 85-104. https://doi.org/10.5465/amr.2009.35713291
Utz, S., Matzat, U., & Snijders, C. (2009). On-line reputation systems: The effects of feedback comments and reactions on building and rebuilding trust in on-line auctions. *International Journal of Electronic Commerce*, *13*(3), 95-118. https://doi.org/10.2753/JEC1086-4415130304
Vance, A., Elie-dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: The effects of system quality and culture. *Journal of Management Information Systems*, *24*(4), 73-100. https://doi.org/10.2753/MIS0742-1222240403
Vu, L.-H. (2010). High quality P2P Service provisioning via decentralized trust management. *Analysis*, *4711*(March) EPFL. http://library.epfl.ch/theses/?nr=4711
Weitzl, W., Weitzl, W., & Berg. (2017). *Measuring electronic word-of-mouth effectiveness*. Springer Gabler.

Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
White, B. (2020). Sentiment analysis: VADER or TextBlob? Retrieved from https://towardsdatascience.com/sentiment-analysis-vader-or-textblob-ff25514ac540
Wood, A. (2018). Confirmed: Monex Group to acquire Coincheck. Retrieved from https://cointelegraph.com/news/confirmed-monex-group-to-acquire-coincheck
Yaar, A., Perrig, A., & Song, D. (2003). Pi: A path identification mechanism to defend against DDoS attacks. Proceedings of *IEEE Symposium on Security and Privacy*, *2003*, 93-107. https://doi.org/10.1109/SECPRI.2003.1199330
Yang, X. J., Unhelkar, V. V., Li, K., & Shah, J. A. (2017). Evaluating effects of user experience and system transparency on trust in automation. Proceedings of *ACM/IEEE International Conference on Human-Robot Interaction*, *Part F1271*, 408–416. https://doi.org/10.1145/2909824.3020230
Ye, C., Hofacker, C. F., Peloza, J., & Allen, A. (2020). *How online trust evolves over time: The role of social perception*. 1539-1553. https://doi.org/10.1002/mar.21400
Zmerli, S. (2014). *Political trust BT—Encyclopedia of quality of life and well-being research*. A. C. Michalos (Ed.) (pp. 4887-4889). Springer Netherlands. https://doi.org/10.1007/978-94-007-0753-5_2202

Cryptocurrencies, an application of Blockchain, is relatively a new phenomenon. Blockchain eliminates the role of a trusted intermediary in the business process through an immutable shared ledger. This dissertation examines how trust is created, implemented, and rebuilt in blockchain and cryptocurrencies.

Aalto-DD 119/2021

ISBN 978-952-64-0497-4 (printed)
ISBN 978-952-64-0498-1 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

Aalto University
School of Business
Information Systems Science
www.aalto.fi

BUSINESS + ECONOMY

ART + DESIGN + ARCHITECTURE

SCIENCE + TECHNOLOGY

CROSSOVER

DOCTORAL DISSERTATIONS