JÖNKÖPING UNIVERSITY
International Business School

Is It as Trustless as They Say?

A Functional Analysis of the Blockchain and Trust.

MASTER
THESIS WITHIN: *Business Administration*
NUMBER OF CREDITS: 30
PROGRAMME OF STUDY: Strategic Entrepreneurship
AUTHOR: Carl-Johan Hallström & Carl Uggla
JÖNKÖPING May 2018

Acknowledgements

We would like to start by saying thank you and expressing our appreciation to everybody that has been part of our journey during this thesis and making it to what it is.

First of all, we would like to thank our supervisor, Annika Hall, who has been tremendous in supporting us in any way possible. Due to the complexity of the topic of this thesis, we understand that it might have been a challenge to supervise. We have shared some deeply philosophical discussions, and she has shown a genuine interest and encouragement, which has helped us do our very best! Finally, we appreciate all the interesting articles you have found and forward to inspire and help us. Thank you, Annika!

Secondly, we would like to present our greatest gratitude to the fellow students in our supervisor group. Jonathan Nyström Lennström & Axel Lundberg; Felix Schmieg & Alia Mostafa; and Subhan Arshad & Loredana Cristea, your feedback from our meetings have been vital for our progression.

Last but not least, we would like to acknowledge all our interviewees who not only provided us with great discussions and insights but also due to their enthusiastic spirit inspired and motivated us on our journey.

May 2018

Carl-Johan Hallström **Carl Uggla**

Master Thesis in Business Administration

Title: Is It as Trustless as They Say?
Authors: Carl-Johan Hallström & Carl Uggla
Tutor: Annika Hall
Date: 2018-05-21

Key terms: Blockchain, Trustless, Trust, Function, Functional equivalence

---

Abstract

Since the introduction of Bitcoin in 2008, the technology behind the digital currency, the blockchain has evolved into the next big thing. In 2017 Bitcoin was on everyone's mind and its value soared from $1,000 in January to $20,000 in December. Now the blockchain is compared to the Internet as the next ground-breaking technology, and many entrepreneurs and established tech companies are experimenting with it. During this frenzy, the blockchain has been dubbed as a trustless system, as it removes the need for trusted intermediaries. This thesis takes a critical stance on the notion of the blockchain being trustless and asks if it is truly trustless today; moreover, if it has the fundamental potential to be trustless. To answer these questions, this thesis reviews previous trust literature and use Luhmann's theory of functional equivalence to see if the blockchain has the same function as trust, and if so if it has the potential to substitute the need for trust. Therefore, this thesis has conducted interviews with experts in the Swedish blockchain community to understand what the function of the blockchain is. This thesis found that the blockchain is not trustless today, as trust is still put in the community's goodwill and competence. Moreover, this thesis concludes that blockchain is functionally equivalent to trust, but as the blockchain and trust are not entirely substitutable, the blockchain does not have the potential to become truly trustless.

Table of Content

Figures

Tables

Appendix

1. Introduction

This first chapter will provide an introduction to the thesis in order to get an understanding of the underlying factors that have generated the need for blockchain. Furthermore, a problematization will be presented in order to understand why this study is important to conduct which will finally reach the purpose of this thesis. Welcome!

In the modern society, individuals put their trust in institutions, where large institutions such as governments and banks have been cornerstones. However, are they trustworthy enough, and are we right to put so much trust in them? An example in modern history where questions like these began to rise was after the great recession of 2008. People had blindly relied on their banks with their money and trusted that they were responsible. This was evidently wrong. Instances like the great recession, breaches of institutional trust, has occurred throughout modern history more often than one might expect. For instance, currently, in Venezuela, the government and banks are in shambles. The Bolivar has defaulted and there is a shortage of food and necessities, which is due to government mismanagement and widespread corruption (Pozzebon, 2018). Moreover, Zimbabwe suffered great food shortages and loss of income from the agriculture industry in the 1990s when President Mugabe forced 4,000 white farmers to give up their lands. To compensate for the difference between expected governmental revenue and actual revenue, the government started to print money (Petroff, 2017). These events snowballed into what culminated into a national financial crisis in 2008 where Zimbabwean currency experienced a hyperinflation of about 80 billion percent per month (McIndoe-Calder, 2018), leading them to give up their currency in 2009 (Petroff, 2017). One commonality of all these cases is centralized power and one point of failure. In this setting, in 2008, a person or group of people under the pseudonym Satoshi Nakamoto introduced the digital currency, Bitcoin (Nakamoto, 2008). One prominent design feature of Bitcoin is that it is a decentralized system, meaning that there is no central power that governs and rules the currency; thereby, eliminating a single point of failure as in the cases mentioned above. Since its creation, the interest in Bitcoin has grown and its valuation peaked at almost $20,000 in December 2017 (Coinmarketcap.com, 2018). Due to Bitcoin's decentralized nature, there is no longer any need for a trusted third party to govern, supervise, or even manage electronic transactions.

Therefore, Bitcoin's underlying technology, the blockchain, has been dubbed by proponents as a 'trust-free' or 'trustless' system (Goldman Sachs, 2018; Glaser, 2017).

One of the most revolutionary parts of the blockchain is that it solves the double spending problem in a decentralized manner. According to Lustig and Nardi (2015): "*The double spending problem refers to spending money in one online purchase, and then quickly making another purchase with the same money*" (Lustig & Nardi, 2015, p.744). Traditionally, this has been prevented through a central trusted third party, such as a bank, that maintain a ledger of all transactions to verify and process payments. Although this system is generally working fairly well, its main flaws are that it is enabling misuse of power and in increased transaction costs; consequently, limiting the smallest size of a transaction between two parties (Nakamoto, 2008). For instance, if the transfer of money from Sweden to China cost $5 and someone wants to send $5, then a transaction requires being at least $10 in order to send the original $5, limiting trade of possible goods and services between the two countries. In short, Bitcoin and other cryptocurrencies solve the double spending issue by securely establishing authenticity through cryptography, validity through a decentralized network with a distributed ledger of transactions, and a traceable and immutable track record through a blockchain (Nakamoto, 2008).

Risius and Sphorer (2017, p. 386) define the blockchain as "...*a fully distributed system for cryptographically capturing and storing a consistent, immutable, linear event log of transactions between networked actors*". Consequently, a blockchain is a string of blocks containing transactions that are mathematically linked together in a chronological order, e.g. a ledger of transactions. These transactions can be moving money or any kind of digital value. A blockchain may be designed in many different ways, but the Bitcoin blockchain is made possible through the following four features: (1) a timestamp server that cryptographically proves that a transaction exists, and when it was made; (2) a decentralized network of mining nodes, or block creators, that together monitors the mutually agreed upon history of transactions; (3) a consensus mechanism that provides the rules of which consensus between the nodes in the network is established; and, (4) an incentive system that promotes activity on the network and align nodes' interests. Since the blockchain ledger is distributed among all the members, the technology guarantees a transparent way of viewing an immutable history of transactions that the entire network has approved upon (Risius & Spohrer, 2017). Due to these technical features, the blockchain has been referred to as a trustless system as it is able to function

despite untrusting parties without the need of a trusted intermediary or safeguards such as contracts (Christidis & Devetsikiotis, 2016).

1.1 Problematization

While there is an abundance of bloggers, journalists, and redditors who frantically argue for and against the notion of the blockchain being a trustless system, there is limited research that critically examine trust in regards to the blockchain. Among scholars, there is a clear majority researching the design aspects of the blockchain, while there is a limited amount among the research on the impact of the blockchain technology (Risius & Spohrer, 2017). Moreover, the scholars who do study the blockchain from a business and managerial perspective either non-critically adopt the notion that the blockchain is a trustless system by providing a short definition of the term trustless, or refuting the notion by simply pointing out instances where trust is still important. We see the debate among scholars as binary where one wing says that the blockchain is trustless (Christidis & Devetsikiotis, 2016) and where the other side try to prove them wrong by pointing out instances where trust still exists (Lustig & Nardi; 2017).

The blockchain has the potential of becoming as big as the internet, thus, if society has the wrong understanding of the technology it could have devastating consequences. The blockchain is deemed to be a trustless system and a majority of the people engaged accept this notion, but what if it is not? What if we, in 20 years, notice that the technology is not living up to the so-called "truths". Since the blockchain has a huge potential of being implemented in many different use cases, the more it is used without a correct understanding, the bigger the potential consequences might be. Therefore, we argue that before blockchain based technologies get a widespread implementation and adoption, there must be an understanding of the fundamental aspects of the technology, trustless system being one of them.

Since the technology is in its infancy and might vastly change in the near future, we believe that when researching the notion of the blockchain being a trustless system it is not enough to only present instances where trust still exists. Therefore, to provide a long-lasting and deeper understanding of the topic, we deem it important to look at trust and the blockchain from a fundamental level to see if the blockchain is or even has the potential of being trustless. However, just because the blockchain might have the potential of being trustless,

it does not say that it is trustless today. Therefore, it is still relevant to also investigate if trust exists in any form, and if so, where it is put. This does not only develop the academic literature on the blockchain but also provide managers, developers, and future blockchain entrepreneurs a better understanding of the limitations and potential of the technology.

However, in order to understand how the blockchain might be trustless one has to understand what trust is. According to Das and Teng (2004) trust is the expectation of gain. Therefore, trust deals with the perceived probability that another party will act in a favourable manner. Like trust, risk also deals with probability but from the point of view of expectation of a loss. Thus, trusting is a risky endeavour where one is vulnerable to someone- or something else's behaviour. Like previously stated, when trusting a bank to fulfil its' obligations one is also vulnerable to the potential of misconduct. Thus, when the customers entrust the banks with their money, the risk of misconduct and incompetence arises and they become vulnerable. Therefore, for Nakamoto (2008) to build a currency which is self-sustaining and not dependent on a third party, or any central organ for that matter, the variable of vulnerability has to be removed. Since trust is the act of accepting vulnerability, the technology of which the currency is built upon must remove and replace the need for trust. In order for the technology to be able to replace trust, Luhmann (2005) argues that for two things to be substitutable, they must be functionally equivalent. This means that two things must in its foundation do the same thing for it to be substitutable. Thus, we argue that for the blockchain to even have the potential to be trustless, i.e. remove the need for trust, it must be functionally equivalent with trust.

1.2 Purpose

The purpose of this study is to develop an understanding of why the blockchain is or ever has the potential to be, trustless. Therefore, we ask the following questions:

1. Is the blockchain trustless today?
2. Does the blockchain have the potential to become trustless?

2. Theoretical framework

To understand if the blockchain is a trustless system, an understanding of both the blockchain and trust must be established. Consequently, this section is divided into two parts. We will in part one define what the blockchain is, provide a basic explanation of how it works, and present why scholars think it is trustless or not. Part two presents a review of trust literature, provide an overview of trust theory and its connection to risk, and explain Luhmann's trust theory. The aim of this section is to provide a foundation of which an analysis of the blockchain's trustless nature could take place.

2.1 Blockchain

2.1.1 Definition

The blockchain is a fully distributed system that is based on cryptography to ensure a transparent and immutable log that records transactions of value between users in a chronological order (Risius and Spohrer, 2017). Since Satoshi Nakamoto published the white paper of Bitcoin, the blockchain as a technology has received a lot of attention and been adopted in many other projects. Christidis and Deevetsikiotis (2016), explains that there are so-called public blockchains and private blockchains. The difference between these is fairly straightforward; in a public blockchain, everybody is allowed access to the network whereas in a private blockchain only a number of selected, entrusted, actors are allowed access. Furthermore, a private blockchain is more suitable in a controlled and regulated environment where all parties are not allowed to transact freely (Christidis and Deevetsikiotis, 2016). In this thesis, we are focusing on public blockchains since the element of trust between actors in the private blockchain is already existing, i.e. by being evaluated and selected, they are automatically trusted parties. Thus, we argue that a private blockchain cannot, per definition, be a trustless system and therefore it is not within the context of this thesis.

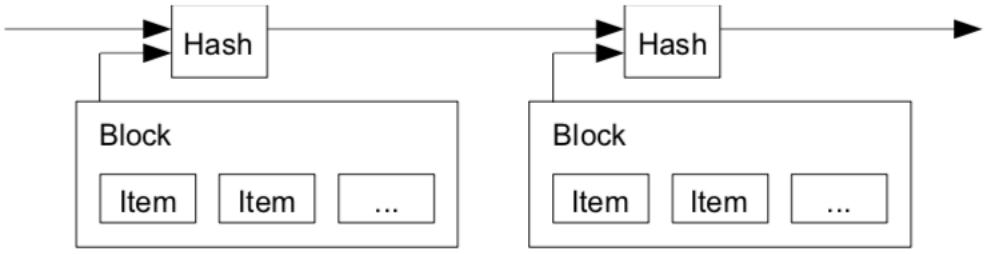
2.1.2 How does the Blockchain Work?

Timestamp server

As the blockchain is a chain of blocks containing information of transactions, each block has an identification, also called a hash, that is the product of the contents of the block itself and the previous updated block's hash. Consequently, a block's hash represents the contents of the block and is timestamped by indicating which block is its predecessor, resulting in a chain of blocks, i.e. a blockchain. Thus, indirectly each block in the chain is referring to the original

block, the first block made, and by doing so validating its own existence and order in the chain. All blocks being added are further validating the existing blocks in the chain (Nakamoto, 2008) (See Figure 1).

Figure 1 Timestamp Server



Source: Adapted from Nakamoto (2008)

Decentralized network

The timestamp server and the blockchain it creates constitutes a ledger or history, of all the transactions inside it. This ledger is distributed to a decentralized network of mining nodes who are users that maintain the system by creating new blocks and verifying them. When a block is presented to the network, the network must verify that the containing transactions are valid and that there is no case of double spending (Nakamoto, 2008). In the traditional financial system, this problem has been solved by having a central bank which has a complete ledger of all transactions. Similarly, a complete ledger of the transactions is kept in the blockchain; however, it is distributed to all nodes in the network, creating a decentralized system of small banks working together (Tschorsch & Scheuermann, 2016). For instance, if person A would transfer the same coin to person B and C, the network will have to approve this transaction before it is authorized. It is here that the decentralized network will be able to show that this is, in fact, a case of double spending, thus resulting in both transactions determined invalid. In order for the network to be able to together validate each transaction, every node needs to have the same version of the distributed ledger, which may not always be the case. Because the network is not centralized and has no single ledger like in a central bank, the network has to come to a consensus of which version of the distributed ledger is 'true'. Since all blocks validate the previous blocks, a blockchain with nine blocks is seen as more validated than a blockchain with five. Therefore, in the case of conflicting versions of

the ledger the longest chain of blocks in the network represents the agreed-upon version. However, this is not necessarily a secure way of establishing consensus in a decentralized network where every node has a vote. Hypothetically a user can create enough nodes so he/she controls at least 51% of the network, which means that he/she can create an artificial version of the ledger by creating the longest chain of blocks. For example, person A, who is trying to double spend, could theoretically set up enough nodes so that he/she is controlling the majority of the network, thus creating a version that validates the aforementioned transactions and person B and C would have no reason to doubt this. However, Bitcoin has come up with a way of preventing this by establishing a consensus mechanism called Proof of Work (PoW) (Tschorsch & Scheuermann, 2016).

Consensus mechanism

The idea of PoW is to shift the way of establishing consensus from a majority of identities to a majority in computing power (Tschorsch & Scheuermann, 2016). This is done by forcing nodes to complete a difficult cryptographic puzzle to create a block - the first node to solve the puzzle gains the right to create the next block. Thus, when a node broadcasts the block to the network, it has to broadcast the solution to the puzzle as well. Other nodes in the network approve the new block and the solution by continuing to work on the next block in the chain, i.e. validating the broadcasted block. Moreover, since the consensus now is established by computing power, a node could theoretically gain control of the network by controlling more computing power thus solving puzzles faster than the average node. To mitigate this, Bitcoin has implemented an exponential mechanism which increases the difficulty level of the puzzles for nodes solving them faster than the average, reducing the advantages of the nodes with better computing power (Nakamoto, 2008). This creates barriers which make it more difficult and expensive to try to take control of the network than just being a supportive part and maintaining it. However, why are people interested in putting in the effort of maintaining such a network?

Incentives

In the case of Bitcoin, the number of coins to be created are predetermined and limited to 21 million (Lustig & Nardi, 2015). The only way for an emission of new coins to happen is through mining, i.e. creating new blocks. The miner is incentivized to create new blocks in the form of receiving a certain amount of Bitcoin from every new block that is created. For instance, today a miner who creates a block receives 12,5 Bitcoins for every new block created (Gobel & Krzesinski, 2017). In addition to the coins received, the miner also earns a

transaction fee that is paid by the users submitting transactions. Therefore, when all Bitcoins are mined, the miners will be incentivized to maintain the network by the transaction fee earned.

Smart contracts and Internet of Things

To further automate business practices and remove the need for trusted intermediaries smart contracts have been implemented. In 1994 Nick Szabo introduced the concept of automating contracts by translating clauses into code. He visualized a system where contracts are self-enforcing to eliminate the need for trusted mediators and other intermediaries. When applied to the blockchain a smart contract is a string of code residing on it. It generally has its own id and address and is triggered by being addressed to. In Bitcoin, a smart contract might be a string of code that exchange currencies. Furthermore, in an attempt to connect the physical world to the blockchain, technology scholars and practitioners have been looking into the Internet of Things, IoT (Christidis & Deevetsikiotis, 2016; Waltonchain, 2018). IoT is the process of connecting otherwise analogue products to the digital space or the Internet. In terms of the blockchain, this could be done through chips that communicate with a blockchain. For instance, Waltonchain (2018) have developed chips that communicate a product's location, properties, and other important information to a blockchain. This is beneficial as it removes the human factor of communicating information to the blockchain, further automating the process and decreasing the need for trusted intermediaries. When bringing all these concepts together, and apply it to, for instance e-commerce, an almost fully automated system is created: (1) the blockchain provides a transparent, traceable, and immutable ledger of information, (2) IoT communicates information to the blockchain, and (3) smart contracts are automatically enforced only when agreed upon conditions are met. For instance, a customer in Sweden orders a product from a Chinese manufacturer. With the help of IoT, the customer can read about the location, properties, and other important information about the product on the blockchain and can be assured that the information provided is true. Finally, with the implementation of smart contracts, the customer will not be charged anything until all required conditions are met, e.g. the good is within a specific geographical location or that the good is in the correct condition (Christidis & Deevetsikiotis, 2016; Waltonchain, 2018).

Therefore, the blockchain might not only be applicable in the financial industry but in other industries as well. Apart from the examples above, the blockchain technology has been

theorized to be used to trace the origin of goods (Provenance, 2015), to verify the authenticity of digital documents such as property titles (Kairos Future, 2017), and creation of peer-to-peer markets (WePower, 2017).

2.1.3 Trustless System

As previously mentioned, there is an abundance of bloggers and journalists who frequently refer to the blockchain as a trustless system and there is a limited amount of research on this topic. However, researchers argue differently for why the blockchain is a trustless system. According to Christidis and Deevetsikiotis (2016), the blockchain is a trustless system because it allows parties to transact with each other without having to trust each other or having to use a trusted third party to mediate. The reason why transacting parties do not need to trust each other is due to the technology's properties which enable security and transparency. For instance, by understanding the blockchain technology and being able to see the progression of the transaction, one does not have to trust that the transaction will go through; parties know what is going on due to the transparent nature of the blockchain (Beck, Stenum, Lollike, & Malone, 2016). Tian (2016) agrees with the definition of the blockchain being a trustless system due to its transparency. The author argues that since the system is open source there is no need for trust among the nodes and no one can ever cheat (Tian, 2016). Nonetheless, Glaser (2017), argues that the blockchain is a trustless system because the blockchain enables decentralized control and that it is immutable. Furthermore, Glaser briefly mentions that the blockchain is a trustless system because of the autonomous nature of smart contracts:

"Additionally, blockchain systems introduce new ways of decentralisation and delegation of services into the hands of autonomous interacting pieces of code, also referred to as smart contracts. These autonomous and hence trust-free setups also attack current trust establishing institutions and intermediaries, such as banks or marketplace operations" (Glaser, 2017, p. 1543).

Notably, the purpose of the articles of the above-mentioned authors was not to critically view the blockchain as a trustless system; nevertheless, the lack of scrutiny and proper explanation is confusing and potentially misleading. Moreover, there are scholars who argue that the blockchain is not a trustless system, but argue that trust merely shifts from one focal point to another.

"*For Bitcoin to work, one does not have to trust Nakamoto, a bank, or any other person or institution. One must simply trust the code - or, more precisely, the cryptographic algorithms*" (Maurer, Nelms, & Swartz, 2013, p. 264).

Maurer et al. (2013) state that the case of Bitcoin is all about trust, but it's about eliminating the need for governmental and corporate trust and learning to trust code instead. Likewise, Lustig and Nardi (2015) argue that a lot of people are using bitcoin, for example, due to several reasons such as a lack of trust in institutions, fear of corrupt governments, or other moral reasons. They continue to state that rather than trusting a central organization the trust shifts to trust in the code. However, Lustig and Nardi (2015) use the same argument for the blockchain not being a trustless system that Beck et al (2016) use to argue that it is a trustless system, i.e. transparency, which leads to confusion. Maurer et al. (2013) state that users trust the code because they are collectively able to review the code and together decide to change it. The authors also argue that trust in code replace the credibility previously put in persons, institutions and governments (Mallard, Méadel, & Musiani, 2014). However, Mallard et al. (2014) argue that trust in code is needed but trust in persons is also still needed. The authors mean that the system is so complex that not only does one have to trust the technology but also the people behind the technology, i.e. the coders. This shows that some researchers, such as Lustig and Nardi (2015), Maurer et al (2013), agree that trust shifts from people and institutions to code, whereas others, Mallard et al (2014), mean that users have to trust both the code and the people behind the code. These diversely spread arguments for the blockchain being, or not being, a trustless system lead Risius and Spohrer (2017) to encourage researchers to critically examine the generally accepted notion that the blockchain is a trustless system.

2.2 Trust

2.2.1 Definition of and Conditions for Trust

Trust takes different kinds of forms depending on where trust is put. One of the most mentioned types of trust is interorganizational trust (Bruneel, Spithoven, & Clarysse, 2017; Zaheer, McEvily, & Perrone, 1998) since it facilitates cooperation between organizations in a world of uncertainty (Zhong, Su, Peng, & Yang, 2017). Trust always originates from the individual but may be placed in different referents (Zaheer et al., 1998). An example of this is Pennington, Wilcox, and Grover's (2004) referent of trust in systems, so-called system trust, or institutional trust. Indeed, the literature states that interorganizational trust and

system trust are two different types of trust. However, Zaheer et al. (1998) argue that trust always originates from the individual, but may be placed on different entities, or focal points. Therefore, no matter what type of trust is being discussed, such as interorganizational- or system trust, they are not different types of trust, but merely different focal points for trust.

To critically understand if the blockchain is a trustless system, an understanding of trust itself has to be established. The notion of trust has been widely researched in fields such as psychology, sociology, economics, and management. While the research has been extensive it has been fragmented and sometimes contradicting. Moreover, the different fields of study provide different scopes and level of analysis, which may cause confusion (Das & Teng, 2004). For instance, scholars of psychology look at trust from the individual's perspective; sociologists look into the scope of groups, societies, and systems; while economists take the perspectives of firms (Rousseau, Sitkin, Burt, & Camerer, 1998). However, while the scope and level of analysis differ between fields, methods and perspectives may transcend the fields of study. For instance, psychologist Deutsch (1962), sociologist Coleman (1994), economist Williamson (1993), and management scholars Das and Teng (2004) rationalize trust from a calculative perspective. More specifically, Coleman (1994) view trust as a rational choice where the potential gain should be greater than the potential loss. Moreover, trust emerges in decisions based on risk. Thereby, risk is a precondition to trust (Coleman, 1994; Das & Teng, 1998 & 2004). Similarly to risk, interdependence is viewed as a precondition to trust. While Sheppard and Sherman (1998) agrees that risk is needed for trust to emerge, they argue that the nature of the risk and the form of trust is dependent on the extent of interdependence. Taking these considerations into account, then trust is the "willingness to be vulnerable" (Mayer, Davis, & Schoorman, 1995), "willingness to rely" (Doney, Cannon, & Mullen, 1998), and "confident, positive expectation" (Lewicki & McAllister, 1998) under conditions of risk and interdependency. Rousseau et al. (1998) consolidated previous literature and argued that trust is not a choice or a behaviour, but a psychological condition. Consequently, Rousseau et al. (1998), defined trust as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" (p. 395).

Das and Teng (2004), however, developed further and divided previous literature on trust into three concepts: "trust propensity", "subjective trust", and "behavioural trust". According to the authors, subjective trust is an expectation that someone or something will act

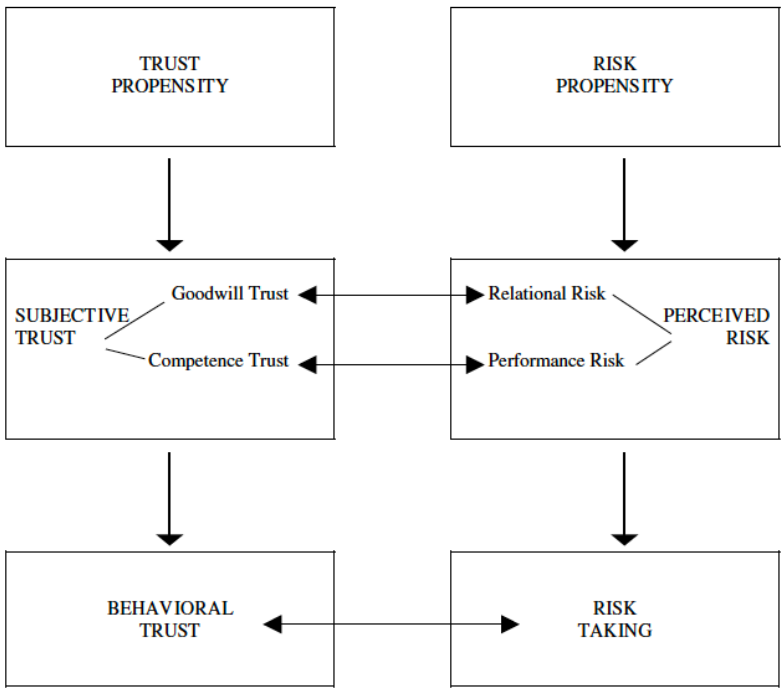
favourably, where behavioural trust is the act itself that is based on the expectation, and trust propensity is the personal characteristics that lead and shaped the expectation. From this light, trust is viewed from a risk perspective and probabilities (Deutsch, 1962). Similarly, Gambetta (2000) argues that people do not simply trust or distrust someone, but trust should be viewed as something elastic. The author writes that trust can take any number between 0 and 1, where 0 is "complete distrust", 1 is "complete trust" and values in between are "uncertainty". The amount of trust is based on one's expectation of other people's' behaviour, the uncertainty of people acting in a manner that is beneficial for us. Therefore, Gambetta (2000) states that if people were able to conclude all the possible outcomes and ways of people's behaviour, then trust would not be relevant. Additionally, Das and Teng (2004) emphasize that to trust is not equal to have 100% confidence in a person. McAllister (1995) shares this view by stating that the knowledge necessary for trust is anywhere between total knowledge and total ignorance. If total knowledge is obtained, then trust is not necessary; likewise, given total ignorance, there is no foundation for trust to be built (McAllister, 1995; Möllering, 2001; Luhmann, 2005). From this perspective, for trust to be relevant, there must exist the possibility for betrayal, i.e. the uncertainty of behaving opportunistically for the trustor, i.e. the person putting trust in someone or something, (Gambetta, 2000). Moreover, in situations where actors do not have enough knowledge about, for example, a technology, risk is not easily assessed. In these situations, actors are not able to make decisions themselves, and instead put trust in experts (Seigrist & Cvetkovich, 2000).

2.2.2 Subjective Trust and Risk Perception

Das and Teng (2004) define subjective trust as the perception that a person will perform as expected, which is in line with Rousseau et al's. overarching definition of trust (Delbufalo, 2015). Since subjective trust is viewed as the perception of the probability of a gain, Das and Teng (2004) argue that it is a mirror image of risk perception, which is the perception of the probability of a loss. The reason why the authors state that trust and risk have a mirroring relationship is that both concepts deal with probability estimates. Because of this relationship between trust and risk, Das and Teng (2004) argues that "*a perception of low trust necessarily implies a perception of high risk, and vice versa*" (p.99), i.e. where there is a certain level of risk, there has to be a certain level of trust as its counterpart. Moreover, according to Sitkin and Weingart (1995), risk perception plays a moderating role between risk propensity and risk-taking. Due to the relationship between subjective trust and risk perception, Das and Teng

(2004) argue that subjective trust also must play a mediating role between trust propensity and behavioural trust. By doing so, Das and Teng connect these three concepts of trust to the three concepts of risk: (1) trust propensity - risk propensity, (2) subjective trust - risk perception, (3) behavioural trust - risk-taking (see Figure 2).

Figure 2 The Relationship Between Trust and Risk



Source: Adapted from Das and Teng (2004)

According to McAllister (1995), subjective trust consists of two dimensions: affect-based trust and cognitive-based trust. Cognitive-based trust is built on reliability and dependability on a person, whereas affect-based trust consists of care and concern, it is rooted in emotional bonds between individuals (McAllister, 1995). According to Das and Teng (2004), subjective trust is founded on two similar types of trust, namely goodwill trust and competence trust. The authors argue that a trustor has to believe that the trustee, the person to whom trust is given, has to have the intention to behave as the trustor expect and that the trustee will be able to behave as expected. An example is that a family friend may be considered as being highly responsible and has good intentions, but may not be suited to be a business partner, i.e. goodwill trust is high but competence trust is low. On the other hand, a stockbroker may

be very competent but one might question her goodwill since she might be incentivized by commission (Das & Teng, 2004). Similarly, perceived risk consists of two dimensions: relational risk, which is connected with goodwill trust, and performance risk, which is connected with competence trust. Relational risk is the probability that a trustee will not commit to the relationship and therefore not behave in a predictable manner and performance risk is the probability that the trustee will be able to achieve the goals of the relationship despite the level of goodwill (Das & Teng, 2004). The authors explain the relationship between goodwill trust and relational risk, and competence trust and performance risk as inverse and further argue that there is no relationship between the other types of risk and trust. For example, relational risk and competence trust has no clear relationship since relational risk is only regarding the probability that the trustee may not act with good intentions and does not take competence into consideration whatsoever.

Since the blockchain is a technology it could be argued that goodwill will disappear and perhaps competence remains. However, it is important to note that a blockchain is also a network of nodes, of users or miners, that have different motivations and intentions. While the consensus mechanism, such as PoW, in combination with incentives is set up to curb the chance of a node or nodes taking over the network, it is still a possibility. It is highly unlikely that nodes would be able to control a network; however, there are cases where mining pools have demonstrated the ability to do so. A mining pool is a group of mining nodes pooling together their resources and share the rewards to become more competitive and increase their chance of mining the next block. On the Bitcoin blockchain there exist a few mining pools that individually account for a large minority of the total network's mining power (Blockchain.info, 2018). Moreover, Zcash, a cryptocurrency based on Bitcoin, was reported in 2017 to be under the control of a mining pool called Flypool (Buntinx, 2017). In this scenario, Flypool had enough power to change, and potentially destroy the currency. It was clear for all other nodes in the network that this mining pool had the competency to manipulate the blockchain, but relied on their intention and goodwill not to do so.

Due to this close relationship between trust and risk, some scholars argue that trust is not an independent construct since both deals with probability (Coleman, 1990; Williamson 1993). Das and Teng (2004), however, take it further and see the inverse relationship between subjective trust and risk perception. Moreover, they highlight that the two constructs originate from completely different concepts; trust- and risk propensity. These two concepts

differ as a trustor might have low trust propensity, belief in the trustee's goodwill and competence, but decide to trust anyways since they have a high risk propensity, tolerance to risk (Das & Teng, 2004).

2.2.3 Luhmann's Function Equivalence Theory

Like Das and Teng (2004), Luhmann (2000) view risk as an important part of trust. However, while Das and Teng (2004) look at trust from a structural level, Luhmann (2005) goes deeper and look at its functionality. According to Luhmann (2005), it is at the functional level where you truly may understand the order of things. The logic is that if two things are functionally equivalent then they may be substitutable. For instance, the function of a car is to transport someone or something from point A to point B, and the function of a bike is also to transport someone or something from point A to point B, then they are functionally equivalent and possibly substitutable. Therefore, if the blockchain is functionally equivalent to trust, then it might substitute trust entirely. Consequently, the blockchain will then have the fundamental possibility to be trustless. According to Luhmann (2005), the function of trust is to reduce complexity. The author, argues that the world is inherently complex and that for people to function in this complex world one must find ways to reduce this complexity. Therefore, trust is used as a bridging mechanism to reduce complexity and enables people to function in a universe where many different outcomes may occur. Consequently, this complexity is the uncertainty of outcomes, or risk, and the inability to predict how 'things' behave and manifest themselves. Moreover, while 'things', such as non-social objects, may promote a certain type of complexity, people inject a new level of complexity. This is because we are all conscious beings who have first-hand experience and interpretation of the world. Additionally, we view each other as other versions of 'myself'; thus, we not only view each other as different 'things' that might behave unpredictably, we also view each other as independent agents who view and interpret the world differently and act with different motivations. For instance, we cannot for sure know if a tree will fall, but we can understand why it could fall and become familiar with the different scenarios and cope with the uncertainty. People, however, will not only act unpredictably but may also do it for unknown reasons that we cannot easily foresee. Moreover, since we view other people as another 'me' then we know that they view us as another 'me', which adds to the complexity. Therefore, while trust is vital in a complex-, or differentiated world, other mechanisms are needed to further reduce the complexity.

In this setting Luhmann (2005) introduces familiarity. Familiarity is established when one can know that others experience the world the same way as 'I' do, and if they do not then they are crazy, evil, or foreign. Therefore, 'I' know to a certain degree what actions others will make and the reasons behind it. Historically, familiarity has been established through religion, culture, and social norms. While Luhmann (2005) sees trust and familiarity as functionally equivalent, since they both reduce complexity, he does not view them as mutually substitutable. This is because while Luhmann sees a scenario where familiarity prevails and there is no need for trust, he argues that there cannot be a scenario where trust may solely prevail. This is because societies based on familiarity use past experiences when making decisions about the future. As a result, familiarity establishes a logical consensus of which future decisions should be based on; thus, the society is functionally able to make decisions about the future. Trust, however, deals with expectations about the future and is solely future-oriented. Thus, in a differentiated world with no logical consensus trust cannot solely help in order to make decisions, since there is no common ground of which decisions, or trust, to be based on. Therefore, both familiarity and trust are always needed for decisions to be made in a differentiated world, while familiarity alone is needed in a familiar world (Luhmann, 2005). This is interesting for this thesis as blockchain features such as the timestamp server and consensus mechanism forces all nodes in the network to use previously presented blocks to establish a common worldview. This worldview has to be shared with the majority of the nodes in the network for a new block to be presented. Looking at these features it would seem as if the blockchain establishes a familiar world.

While familiarity and trust reduce complexity, so does confidence. Confidence is similar to trust as both deal with future expectations which may result in disappointment. Luhmann (2000) see the distinction as to how the expectation forms. While trust is the product of risk, confidence is the product of contingencies and danger. Moreover, confidence is the subconscious expectation of minute and almost negligible cases of uncertainty where no other alternative is perceived or considered. For instance, in Sweden, it is illegal to carry a gun and people generally do not expect to be shot in the streets, so no one carries a gun on the streets. Consequently, behaviour based on confidence are made automatically without an actual decision, while behaviour based on trust is based on active decisions. Thereby, Luhmann (2000) agrees with Coleman's (1990) and Williamson's (1993) views' that trust is based on choices; however, according to Luhmann (2000) trust does not occur in calculative decisions where the expected gain is greater than the expected loss. Rather, the author takes

the position of Deutsch (1962) that a decision based on trust can only occur in situations where the potential loss is greater than the promised gain. Thus a 'further element' or a 'leap of faith' is involved in the decision to trust (Möllering, 2000). Consequently, trust only occurs where a bad outcome ensues regret. While there might be less need for trust in situations of high confidence, they are not mutually and symmetrically substitutable. The economic system is a great example to explain this point as people both have almost total confidence in money, but there still exists a need for trust. Confidence in money lies in the day-to-day usage of it. When receiving money, no one stops and ask if the money is good, or whether they may use it somewhere else - they just accept it. However, people put trust in money and the economic system when they decide whether to save or invest it. We have confidence in money as the likelihood of the value of a nation's currency to disappear is minimal. Moreover, if such an event would happen, no inhabitant would feel a sense of regret as none of their decisions alone was the cause of it. However, we put trust in the economy when we participate and decide on whether to save or invest our money. This is because, in the event of loss, we have ourselves to blame that we made the decision to place the money in a savings account when we should have invested and vice versa.

Since familiarity, confidence, and trust are similar in nature and all functionally equivalent, they are also substitutable. However, not entirely. Luhmann (2000) argues that they all, to some extent, depend on each other; thus, "[i]t is not possible [...] to completely replace with yourself something on which you also depend" (p. 101). Therefore, while the blockchain might be functionally equivalent to trust, it does not equate that it will necessarily entirely replace it, but that it has the potential to do so.

3. Methodology

In this chapter, the reader will gain an understanding of the researchers view on how reality looks like and how reality will be interpreted through research. Furthermore, a thorough explanation of how data was gathered and analyzed will be presented. Finally, arguments are given for why this study is following ethical considerations and is trustworthy.

3.1 Research Philosophy

The purpose of this thesis is to understand if the blockchain is a trustless system by investigating whether the blockchain and trust are functionally equivalent and to see what type of trust still might exist. We argue that reality is socially constructed and thus it varies in meaning from person to person. Moreover, this social reality is created by people through language and discourse, i.e. the reality is internal and not external. Therefore, we reject the ontological view of realism that views the reality as external and objective (Easterby-Smith, Thorpe, & Jackson, 2015). Since people interpret the notion of truth differently, there is not one universally objective truth. Consequently, it could either be argued that there are many different truths (relativism), or that since there is no universal truth there is no truth at all since the world is just the interpretation and experiences of people (nominalism) (Easterby-Smith, et al., 2015). We argue for the relativistic view by stating that everything the human considers as facts and sees as objective truths stem from one's own experience and internal interpretation of the external world. Berger and Luckmann (1966) view this objectivity as something that has become institutionalized from a shared knowledge base, which instructs people's conduct. Therefore, people's shared knowledge may differ depending on their shared experiences. For instance, for Swedes it is absolutely normal, if not natural, to dance like frogs around a pole and eat pickled fish on a certain day in the middle of the summer, while someone who does not share this knowledge base would be very confused by the idea alone. Therefore there is no such thing as an external reality, as humans create their own reality through experiences, which is reified through language.

Since we see the world as internally created by people's interaction with each other, we believe that reality should be interpreted from a social constructionist epistemology. Subsequently, as experiences are reified through language, then knowledge can only be

attained through conversations and discourse (Berger & Luckmann, 1966). Therefore, we explore what scholars *say* the function of trust is and what experts *say* the function of the blockchain is and where trust might exist, in order for us to achieve our purpose to understand if the blockchain is trustless. Thus we use communication as a tool to try to understand our topic of research, which is in line with the social constructionist epistemology (Easterby-Smith, et.al, 2015). Having that said, we are aware that communication is limited as one cannot expect to grasp the full reality that another person tries to convey. Not only due to the limitation of one's ability to communicate but also due to the limitations of the listener. While this might be true, we still argue that communication is the best way of expressing and interpreting one's own reality.

3.2 Research Purpose

According to Saunders, Lewis, & Thornhill, (2007), there are three main research purposes one can adopt: descriptive, explanatory, or exploratory. If one is to describe a profile, events or situations, it falls under the descriptive purpose. However, since our thesis aims to understand and not to describe if the blockchain is trustless, the descriptive purpose is therefore not suitable for this study. Furthermore, since this thesis is to explore what scholars *say* and what experts *say* we are not looking at causal relationships between variables and therefore we are not conducting an explanatory research (Saunders, et.al., 2007). Finally, due to the lack of previous business and management research about the blockchain and trustless systems, there is little foundation for us to test a theory. As a result, the purpose of our study is focused on shedding light and form new insights about the blockchain as a trustless system; thus, our research purpose is exploratory in nature (Robson, 2002).

3.3 Research Approach

Saunders et al. (2007) present two research approaches; deductive and inductive. The deductive approach starts by looking at previous literature in order to form a theory that is then empirically tested, while induction seeks to get an understanding of what is going on or an understanding of a specific problem by allowing empirical findings to build theory. As we were novices going into the topic of the blockchain, we chose to mix these two approaches and adopted an abductive approach. Therefore, we started our research through a superficial review of scholar literature and media publications on the blockchain. We realised that trust was highly intertwined with the blockchain and that media and proponents- and scholars of the blockchain maintained the strong position that the blockchain is a trustless system

(Christidis & Devetsikiotis, 2016; Beck et al, 2016; Glaser, 2017; Tian, 2016). To triangulate this observation we conducted three pilot interviews with experts, which all confirmed what we had experienced. All this, pilot interviews and a superficial research about the blockchain, guided us to our purpose and research questions. Therefore, since we try to answer the question if the blockchain is a trustless system, we deemed it necessary to gain a deeper understanding of trust. By conducting a deeper research into the literature we were able to frame the problem into a manageable form and helped us realize that a way of viewing trust is through its functionality (Luhmann, 2005). This research was not made with the purpose of testing theory but rather used as a foundation of our research design. As we became more knowledgeable, it allowed us to be sensitive, flexible, and more aware of topics discussed in our interviews. The strength of this abductive approach is that it combines the two strengths of inductive and deductive approach. By inductively confirming our assumptions in the field we were able to confirm with the community what was relevant and interesting to conduct research on. Moreover, by using a deductive approach, we were able to get a deeper understanding of the phenomenon being researched. Thus, we are avoiding the risks of conducting research on something irrelevant or not getting a deep understanding of the research and thus limiting the contribution of the study.

3.4 Research Strategy

When conducting research there are some alternatives one can choose from regarding strategy. According to Saunder et al. (2007), there is a selection including experiments, surveys, case studies, action research, grounded theory, ethnography, and archival research. Since there is little managerial research conducted on the blockchain, the purpose of this thesis is to generate new insights and shed light on this under-researched topic. We have used a grounded theory strategy in order to build theory from the collected data.

Usually, when conducting grounded theory the researcher starts collecting data without reviewing the existing literature about the topic. The researcher usually conducts many "visits" to the field to gather data and reviews the data between the visits (Saunders et al., 2007). However, here is where the field of grounded theory is divided. Originally Glaser and Strauss (1967) argued that researchers should start with no existing knowledge and should allow ideas to emerge from the data. However, Strauss and Corbin (1990) deviated from this idea and recommended that familiarizing oneself with the literature first is beneficial to become flexible and sensitive when collecting data, which is in line with our abductive

approach. As discussed in the previous section, we deemed it necessary for us to familiarize ourselves with the literature in order to not miss important topics brought up in our research.

3.5 Qualitative Research

When conducting qualitative research one of the most adopted form of collecting data is through interviews where the focus lies on what participants are saying. Qualitative data can be distinguished by its non-numerical form and the high level of interaction of the researcher (Easterby-Smith, et al., 2015). Furthermore, qualitative research tends to be more explorative in nature, which is in line with our research purpose. As the world is internally created by people's interactions and language, we argue that conducting qualitative research is the most appropriate way of gaining understanding. Moreover, as knowledge can only be attained through discourse, we deem interviews as the proper method of gathering data. Therefore, to achieve the thesis' purpose, interviews have been conducted with experts in the field of blockchain to explore what the participants say the function of the blockchain is.

What differs qualitative interviews from everyday conversations is that the questions being asked in an interview focus on a particular purpose, which is usually an in-depth understanding of a particular phenomenon or experience (Easterby-Smith, et.al., 2015). Interviews may vary from one another depending on the structure: formalized and structured or informal and unstructured. For the case of this thesis, semi-structured interviews have been conducted for the pilot interviews, the in-depth interviews, and the final interview. This is because the topic of research was known but the aim was to explore and go more in-depth than in a structured, quantifiable, form of interview. Furthermore, semi-structured interviews are in line with research of exploratory nature to gain new insights (Saunders et al., 2007). To reduce the risk of deviating from our topic, we constructed topic guides for our pilot- and in-depth interviews. Moreover, a topic guide is important to make use of in order to ensure the questions being asked are relevant. If the questions are not relevant or hard to understand the interviewee might lose interest and the quality of the interviews will suffer (Easterby-Smith, et.al., 2015). Due to the open-ended nature of the questions when conducting semi-structured interviews the need for audio-recording arises. On that note, all the interviews were audio recorded and the in-depth interviews were transcribed. This decision was made in order to stay focused on the interviews and not being distracted by writing comments. Moreover, audio-recording is also useful in order to stay unbiased and produce reliable data for future analysis (Saunders et al., 2007). However, all but two interviews were conducted

in Swedish, and thus were transcribed in Swedish. As a result, the quotes used from these interviews has been translated by us. As previously stated, we are aware of the limitations of language to express one's interpretation of reality, translating the quotes could further add to this limitation.

3.6 Data Collection

3.6.1 Sampling

Collecting data can be very time-consuming and sometimes even impossible if one tries to gather all data that is available to your study. Sampling techniques allow one to reduce the amount of data by only considering a small group of the entire population (Saunders, Lewis, & Thornhill, 2016). In our study, since the blockchain is such a new phenomenon, the target population itself was very limited. Therefore, the sampling methods used were non-probability convenience sampling and snowball sampling. Convenience sampling is often used when selecting samples because they are easily obtained. However, a risk of this is that it may lead to biased findings because the only people who choose to participate could be people who feel strongly enough about the topic (Saunders et al., 2016). Convenience sampling was used because the only requirement for our sampling is that the interviewee is an expert, or working within the field of blockchain technology. This is once again due to the fact that the target population is so small that finding blockchain experts has been very limited.

We started by contacting people involved with the blockchain technology all over the world, e.g. Denmark, South Korea, Sweden, and United Kingdom. However, the only people responding were based in Sweden. When contact was established, we also used snowball sampling so the interviewee could refer us to our next interviewee. We decided upon this method as not only was the population limited but also hard to identify (Easterby-Smith et al., 2015). Therefore, we immersed ourselves and participated in meetups to find our first interviewees. Once a couple of actors were identified snowballing proved to be a successful sampling technique as they referred us to our next interviewees. The aftermath of these sampling techniques was that the study focused on Sweden and more specifically Stockholm as our initial contacts were active in this area. Although the Swedish blockchain community is in its early phase and may be difficult to identify, due to its smaller size it is a tightly connected group that frequently interacts through various meetups and events. However, due to the interconnected blockchain community, there is a risk that the interviewees are

affected by each other, which could lead to homogeneous answers, thus homogeneous findings.

For the pilot interviews, 15 companies were contacted whereby three agreed to participate. Thereafter, a mix of snowball sampling and convenience sampling was used to contact 16 companies for in-depth interviews. This resulted in 11 agreeing to participate where the majority of the companies were start-ups with the exception of one university employee and two consultants.

Table 1 Pilot Interview

Name	**Company**	**Sampling method**
A1 & A2	Company A	Convenience sampling
B1	Company B	Convenience sampling
C1	Company C	Convenience sampling

Table 2 In-depth Interviews Round 1

Name	**Company**	**Sampling method**
D1	Company D	Snowball sampling
E1	Company E	Convenience sampling
F1	Company F	Convenience sampling
G1	Company G	Convenience sampling
A1	Company A	Convenience sampling

Table 3 In-depth Interviews Round 2

Name	**Company**	**Sampling method**

H1	Company H	Snowball sampling
C2	Company C	Snowball sampling
I1	Company I	Snowball sampling
J1	Company J	Snowball sampling
K1	Company K	Convenience sampling

Table 4 Final Interview

Name	**Company**	**Sampling Method**
C3	Company C	Snowball sampling

3.6.2 Interviews

With our initial understanding of the blockchain in mind, we constructed a topic guide for our pilot interviews (see appendix 1). This guide covered a general discussion on the blockchain and the potential of the blockchain. These pilot interviews confirmed our assumption that trust is an important aspect of the blockchain. Following the pilot interviews, a deeper understanding of the blockchain and a thorough analysis of trust literature was conducted. Based on this acquired knowledge, the question of whether the blockchain is a trustless system or not arose, and thus our purpose was discovered. In order to fulfil our purpose, a second topic guide was made for the in-depth interviews. The topic guide covered three topics: (1) the function of the blockchain, (2) settings, and (3) the blockchain as a trustless system (see appendix 2). The first topic regarding the function of the blockchain was created to get the interviewee to reflect and define the function of the blockchain. Settings were used in order to get a more nuanced picture of the interviewee's view of the blockchain and its function in different settings such as on a macro, meso, or micro level. Finally, after having saturated the discussion of the function of the blockchain a blunt question was asked whether or not the blockchain is a trustless system. This allowed the interviewee to reflect on their opinion and gave the opportunity for more in-depth answers. Furthermore, it provided this thesis with a deeper understanding of why or why not the blockchain is a trustless system, other than on a level of functionality.

When the first round of interviews had been conducted and coded, an additional analysis of the trust literature was conducted. Taking the subjects provided by the interviewees in mind a new search with a specific focus on trust's function and system trust took place. This resulted in an understanding of Luhmann's definition of confidence and familiarity and the topic guide was refined (see appendix 2). The new topic guide still had the foundation as the first one but included a couple of sub-questions about confidence and familiarity. Mainly, the insights from the first interview and literature made us more sensitive to topics involving confidence and familiarity, which improved our probing. After the second round, an additional interview was conducted to ensure saturation, which was established and the decision to move on to analysing data collected was made.

3.6.3 Ethics

The consideration of ethics is of great importance when conducting research. The cornerstone of research ethics is making sure no one participating in the study gets harmed. Thus, by doing an ethically sound study it involves the researcher behaving appropriately and sensitively to the rights of the participants of the study or those that might be affected by it. In order to ensure this, it involves the researcher dealing with considerations of how to design the study, how to gain access, how to collect data, how to store the data, analyse, and present the findings (Saunders et al., 2007). Bryman and Bell (2007) list ten key principles in research ethics where the first six are about protecting the interests of the interviewee and the last four are about protecting the integrity of the research community.

In order to protect the interest of the participants, every interview was fully voluntarily from the participants' side and the interviewee decided themselves whether or not to be anonymous; however, the result was that none of the interviewees wanted to be anonymous. Furthermore, in order to protect their privacy and to ensure confidentiality, the gathered data is stored in a cloud-based service that only the researchers have access to. Even if the researchers do not see any way of the gathered data being able to harm the participants, that does not mean that the data is not sensitive. Therefore, although an informed consent of using the real names was given, in order to prevent harming the participants a decision was made to keep their personal names and names of their belonging organizations anonymous.

Finally, in order to protect the integrity of the research community, Bryman and Bell's (2007) last four principles were taken into consideration. Firstly, we were as open as possible with the purpose of the thesis in order to avoid deceiving the interviewees of the nature of the study. Moreover, in order to make sure no misleading or false reporting of the data was made, all the interviewees were asked for the consent to audio-record the interview so a transcript of the interviews was made possible afterwards. Finally, this study is not funded or managed by any third party; therefore, we see no possible conflict of interest.

3.6.4 Analyzing the Empirical Data

As this thesis is following a grounded theory strategy, the natural way of conducting the analysis is to do a grounded analysis (Easterby-Smith, et al., 2015). The authors provide a seven-pointed list to follow which we have been inspired by (1) familiarization, (2) reflection, (3) open coding, (4) conceptualization, (5) focused re-coding, (6) linking, and (7) re-evaluation. We conducted four rounds of interviews, one round of pilot interviews, two rounds of in-depth interviews, and one last interview to confirm that we have reached saturation. As the pilot interviews and the last saturation interview was only used to guide us, we decided not to transcribe or code them. After every interview round a familiarization and reflection of the data was made in order to be able to learn more from theory before moving on to the next round of interviews. After each in-depth interview, we conducted a brief review in order to gain an overview of the data. Thereafter we started with an initial open coding of our in-depth interviews in order to structure the data somewhat and gain a clearer overview. Moreover, we decided that each researcher should code the interviews separately to decrease the risk of missing important findings in the data. When the individual coding was done, the two sets of codes were compared and merged together to find common patterns. Thereafter, an additional re-coding was conducted to help us rank and map the categories into themes, categories, and subcategories. This resulted in two themes, five categories, and eight subcategories. In relation to our purpose, we looked into what the data said about the function of the blockchain but also noticed there might still be a need for trust. Therefore, the main themes emerged were Focal Points of Trust and Reducing Risk. For clarity, full description and map of the categories will be presented in chapter 4, Empirical Findings.

3.7 Research Analysis

Aligned with our purpose, we analyzed our research questions separately. Our first research question is if the blockchain is trustless today; therefore, to answer this we analysed our data to find if trust exists anywhere, and if so, what type of trust. Thus, we use data coded under Focal Points of Trust and appropriate theories provided in the theoretical framework as the foundation of our analysis. Consequently, to answer if the blockchain has the potential to become trustless we used data coded under Reducing Risk as a foundation for our analysis. Here we use Luhmann's theory of functional equivalence (2005) to see if the blockchain and trust may be substitutable. From the theory, we know that risk and complexity are equal and that trust's function is to reduce these. Therefore, in a similar way we are analysing if the blockchain's function is to reduce complexity.

3.8 Research Quality

Being able to ensure trustworthiness and quality in qualitative research has often been questioned by positivists who argues that qualitative research cannot be assessed in the same way as quantitative research (Shenton, 2004). Quantitative research relies on validity and reliability to ensure replicability and generalizability (Wahyuni, 2012). If a study is reliable it means that the measurements are consistent over time, which facilitates that the study is replicable. Validity refers to the accuracy of the findings, whether the results are what they seem to be, which in turn can ensure if it is generalisable (Saunders et al., 2007). However, in order to ensure trustworthiness in qualitative research, Guba (1981), presented four criterions: (1) credibility which mirrors validity, (2) transferability which parallels external validity (generalizability), (3) dependability mirroring reliability, and (4) confirmability resembling objectivity.

Like validity, credibility refers to the accuracy of the data. In order to ensure credibility, Shenton (2004) argues that by using triangulation, using different sources and different methods, it enables rich data. As previously mentioned, we started by familiarizing ourselves with what the blockchain is and noticed that trust played a big role in the discourse. We then conducted pilot interviews in order to triangulate our observation about trust and the blockchain. By triangulating we warranted confirmability through our pilot interviews which ensures that the findings are not biased of us as researchers. Furthermore, after every topic discussed in our in-depth interviews, we summarized our understanding of the interviewee's statements to see that we had understood correctly, which also is seen as a form of

triangulation (Saunders et al., 2007). Moreover, data from a qualitative study can be considered as impossible to apply in a different setting. However, in order to ensure transferability, this thesis conducted interviews with blockchain experts that were active in different industries such as healthcare, finance and business applications. To achieve dependability, we have been as honest and transparent in our design and process as possible which helps future researchers to replicate a similar study. Since dependability is not about enabling future researchers to get the same result in a similar study but rather to conduct a similar study with the same tools, the topic guide used is accessible in the appendix.

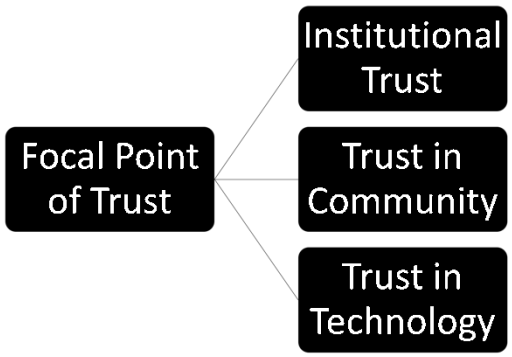
4. Empirical Findings

From our data, we have discovered two main themes, Focal Points of Trust and Reducing Risk. Focal Point of Trust has three categories: (1) Institutional Trust, (2) Trust in Community, and (3) Trust in Technology. Reducing Risk, in turn, contains two categories: (1) Removing Human Intermediaries and (2) Shared Truth. This chapter will present the findings from Focal Points of Trust and Reducing Risk, respectively.

4.1 Focal Points of Trust

The first theme that arrived from our data, when discussing the trustless nature of the blockchain, was The Focal Point of Trust. More specifically, three different focal points of trust were identified: (1) Institutional trust, (2) Trust in Community, and (3) Trust in Technology (see Figure 3).

Figure 3 Focal Point of Trust



4.1.1 Institutional Trust

The data tells us that the blockchain is providing the possibility to cut oneself loose from institutions, such as banks and governments, and thereby no longer have to trust them. A1 argued that even though we have been trusting our institutions, and that we have felt safe relying on them, this might change:

"We have gone to the big banks because they are a big and safe actor, we have entrusted them with our money, your hard earned money! This is going to be put to the test when these types of [blockchain] technologies are being introduced".

E1 gave a very vivid example of how the blockchain enables people to cut themselves loose from institutions:

"Yes, or even, for it also makes a difference for us [people in Sweden]. Because it puts some sort of fundamental possibility to always say 'oh, fuck it! I do not care about Sweden right now, I am opting out! I buy my Bitcoins and take care of myself, you can all go to hell!'. […] Because I can say 'you banks can do what you want, do misconducts, do what you want! I am not going to put my money over there, I have got my bitcoin because I trust it more!'"

However, F1 states that in Sweden there is not necessarily a need to stop trusting these institutions because:

"I have no reason... Or we, the inhabitants of Sweden, have a reason to trust each other. Or maybe even more of a reason to trust a bank than our self. But this may not be the case in other countries".

A recurring example provided by the interviewees where there has been a need to cut oneself loose from institutions is the case of Venezuela where the country is in the middle of an economic crisis leaving the inhabitants powerless. E1 says:

"As we can see in Venezuela today, the government is printing Bolivar so they have an inflation of 2000%, so your entire pension is screwed. You would have liked to convert it to USD but you are not allowed to. You would have liked to buy food or medicine, but you can't because there is no more medicine, so [you] want to import but how are you going to do that when you are not allowed to convert to USD? [...] With Bitcoin you can connect to the internet in Venezuela, get hold of some Bitcoin by consuming electricity and all of the sudden you can buy food and medicine online and have it shipped from the USA. So the advantage is that it becomes an open network for transfer of value. This is not necessary for you and me because we have Swish and we trust our bank".

When discussing different scenarios of institutional trust most of the interviewees argued that when using the blockchain the traditional trust in institutions now shifts to something else, either trust in the community and/or trust in technology.

4.1.2 Trust in Community

H1 states that when using the blockchain technology, there is no longer a need to trust an institution or a person but rather one has to trust the collective in the network to behave as agreed upon:

"It's a different sort of trust. Instead of trusting any corporation or individual you are trusting in a network of them. In order for that trust to be broken the trust as well is decentralized. So, with a private network, if you've got a private blockchain with ten different, no seven, different nodes. You are trusting that four of them wouldn't collaborate to go back and change everything. So, that could still happen, there is nothing that stops that if those people would collaborate. So, you are still trusting in that. But, it's a different level of trust you are not trusting one person, you're trusting in a group. So, it can't be purely trustless, but the larger the set of nodes on the network the smaller, the lower level of trust you need".

J1 has similar views that one has to trust that the group within a private blockchain behave "correct":

"We trust on the nodes and most of all that the majority of them will behave correctly. So, in this case, the consensus mechanism is not that important. It [consensus mechanism] is usually when you have an open system that these are more intricate, as in the case of Bitcoin for example where everybody who wants to join is allowed to".

H1 gave an example of where a mining pool, a group of users, who got close to own 51% of the Bitcoin network and then decided to limit the people who could join their collaborative. The reason was that if they kept growing in numbers they would soon grow too powerful in the network. The reason why they did not desire to become too powerful was simply due to the element of trust. The mining pool had a lot of money tied up in the network, and if owners of Bitcoin started noticing that this collaborative would have the possibility to dictate the network then the users could stop trusting the network and abandon the network, resulting in monetary losses for the mining pool.

"Yes exactly, so for them [...] having the power to kind of break the system would ruin the system and ruin the value of being able to break the system. You see what I mean? 'we could break it, but then it is gone and then we got nothing by breaking it. So, it's better to limit our own scopes so we can't'".

However, not only does one have to trust that the community will behave correctly and not destroy the network, but one also have to trust that the people within the community are knowledgeable enough to take care of the system itself and that they will alert if there are any types of errors or failures within the system. H1 says:

"I think you then place your trust in the community. It's a bit like nuclear physics. There are huge amounts of literature published on it, I can go out and read it all but I wouldn't understand a word of it. But, I believe that it is right because there are other very bright [people] out there who can read it and are commenting on it and do agree with it. In the same way, I can't read the code for blockchain, and I'm not going to understand it, but I know, because it is open source, there are other people reading and if they would be able to poke holes in it, it would be found out and published online very quickly".

A1 agrees by saying that if you do not understand everything that a blockchain is doing, then you do not directly trust the system because then you put all your trust in the community who actually possess the knowledge. In that case, you use the community as a mediator of trust in order to trust the system.

"Otherwise you have to trust like I do, that there are a bunch of smart people who can read the open source code and know exactly how the system works. A lot of technically knowledgeable and smart people. Everybody who understands it says that it's good stuff. There are very few technical people who have come forth and said that it's not good. So I trust in that. Actually, if you don't understand everything then you don't trust the system. I trust the system but it's only because I trust them [the community]".

4.1.3 Trust in Technology

The other focal point of trust when one no longer place trust in institutions is technology. The arguments have been that one has to trust in the community to behave correctly and that they are knowledgeable, but one also has to place trust that the technology is working properly. As J1 argued, *"you [have to] have some kind of trust for the technology and the math behind it [blockchain]"*. Moreover, A1 agrees by saying *"You have to trust the technology if you don't then it's pointless"*.

D1 agrees that trust shifts to technology but argues that the blockchain removes the need to trust any individual at all:

"I mean the word trustless is maybe not the best way to shape it in my view. I mean you don't trust…if trust is a word you use to a particular individual, a human being only, then yes it's trustless. But if it's trusting something, like a system, or a set of policies or a piece of code, then trust still exists but it's from trusting an individual to trusting the code".

He continues his thought, and find the word trust difficult to place into this context:

"The thing is that you put trust in… you emphasize, let's say predictability. Predictability can maybe be the more, the better, more meaningful word here. Humans are not necessarily predictable but code is predictable. Because code sticks to what it does, 1+1=2, you cannot expect it to give you 3. So that is perhaps, you put trust in computer systems rather than human beings."

However, D1 made it clear that the word "trust" may not be the best word to use with regards to the blockchain and particularly not suitable in his own native language, Arabic:

"So yeah, if you are going to use trust with humans that are involved in the picture, then you no longer need to trust anyone on the blockchain. But if you use trust for anything they produced, which even if they're long dead, then yeah, I mean you can use trust but I would favor not because I would associate the word trust in linguistics in my own native language, in Arabic, you actually use trust only with someone who's living, someone who's actually has… you've given him your money and you trust that he would not do something bad with it. So he's a human being at the end. But if it's code, you can predict what it will do because it's open source, you can see what it can do.".

Stepping one step back from the data, what it tells us is that when using a blockchain technology, it may affect ones trust in institutions and shift that trust towards the blockchain community or directly towards the technology itself. However, if one places their trust in the technology, the word "trust" may not be the best word to use since it may be more about predictability.

4.2 Reducing Risk

The second theme that emerged from the interviews was Reducing Risk. As mentioned in the method, like Luhmann (2000), we equalize risk and complexity, as they are both connected to uncertainty of possible outcomes. J1 went straight to the point:

"...so we get a simpler data system where blockchain is contributing by removing complexity from the system. And, I think that is very important because these data systems contain a lot of unnecessary complexity, so it is [...] an expectation that we can reduce complexity in systems."

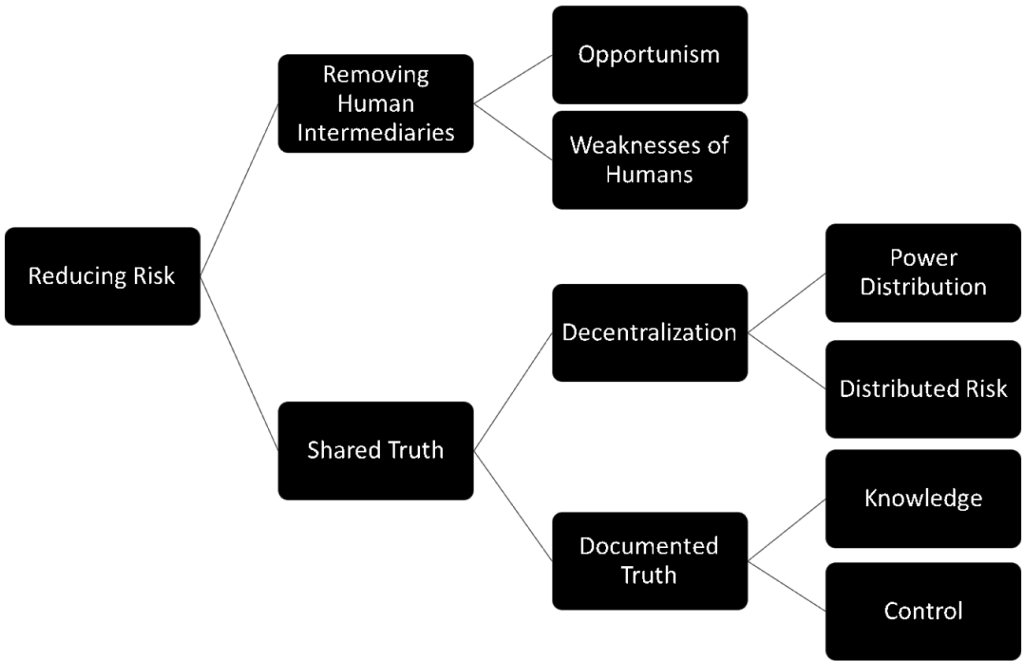
This quote caught our attention and provoked the question if reducing complexity might be the fundamental function of the blockchain. J1 affirmed and provided an example of how reducing complexity in the banking system is beneficial:

"Yes, absolutely! I really do think so. Take the banks for example… I have heard that approximately 40% of the banks' infrastructure is dealing with making sure that data obtained is correct. These 'parts of settlement' between the banks, that they have to double check everything… so, they are interested in blockchain between the banks, because they can be sure that the information and capital that is transferred [is correct]. So, if they are able to reduce [the amount of infrastructure dealing with double checking data] from 40% to 30% it would entail huge profits. If they are able to reduce it to 5%, which I think should be reasonable… that is an extreme shift."

While risk is reduced, it is not eliminated. For instance, F1 mentioned that *"it does not eliminate the risk but minimizing the risk. And, then you cannot say that it is 100% trustless, but it is as trustless as it can be"*. Furthermore, G1 talked a lot about security and risk in relation to the blockchain and when asked if the blockchain is reducing risk he said, *"yes, we are pushing it as close as we possibly can at the moment"*.

When looking at our empirical findings we found that Reducing Risk could be branched into two categories: (1) Removing Human Intermediaries and (2) Shared Truth. Furthermore, these two categories could then be branched into further subcategories (see Figure 4).

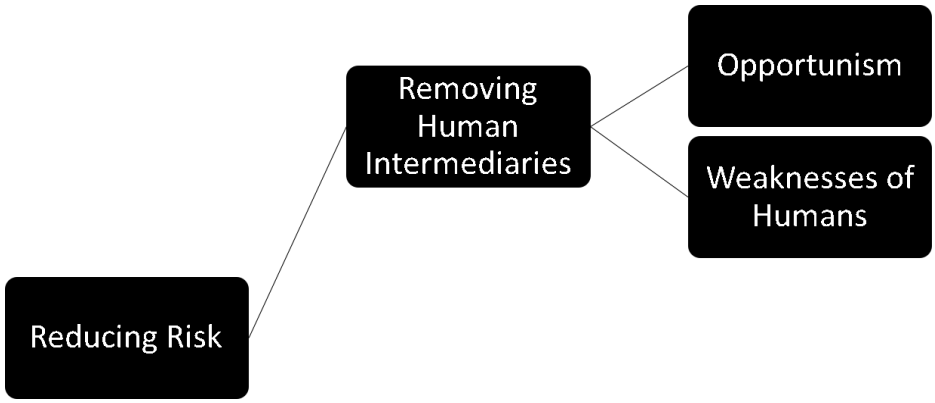
Figure 4 Reducing Risk



4.2.1 Removing Human Intermediaries

Removing human intermediaries is an essential part of reducing risk. When examining the quotes that pertained Removing Human Intermediaries, we found two subcategories: (1) Opportunism, and (2) Weaknesses of Humans (see Figure 5). One way the blockchain is reducing risk is by removing human intermediaries. As a result, it removes the risk of opportunism and weaknesses of humans, both cognitive and physical. Therefore it is clear that Opportunism and Weaknesses of Humans together reduce risk.

Figure 5 Removing Human Intermediaries



Removing Human Intermediaries was extensively talked about by our interviewees. According to D1 the blockchain:

"…would replace the human intermediary […] and the value here is simply eliminating the human element. You eliminate the intermediary and make the code become the intermediary, and once the code is intermediary the code is immutable, it's not possible to change."

C2 also talked about the Removing Human Intermediaries. When asked why she thinks the blockchain has become as popular as it has, she rejected that notion and argued that the blockchain is not yet too popular. However, she saw the benefit of the blockchain in banking, and talked about why it is beneficial for the banks:

"...but then one has seen some adoptions of blockchains that could be good for particular product segments within the bank, for instance, international payments. Because today it must be sent to a clearinghouse and then treated by European clearinghouses before it is sent forwards. So, it is just a bunch of intermediaries and blockchain predominantly cuts out the intermediaries."

Opportunism

When asked what the benefits of the blockchain are, I1, said that *"it is to be able to make safe transactions between each other without intermediaries and it does not matter where in the world you are. Everyone gets the same terms."*. When asked why it is important to not have intermediaries he said: *"just because of that! You do not need to trust anyone!"*.

D1 elaborated on the idea that one does not have to trust anyone:

"Well, some people find it more important because the risk of being abused or exploited is high, and we can see from examples what is happening today. Facebook for example, where you have the data taken and used by… particular elements that were entrusted so you gave trust to a person and that person actually backstabs you and abuses that trust and so… not all humans are worthy of trust, unfortunately. […] That's why the idea of what we call decentralized apps, DAPS [...] that [...] actually take on the role of the Kickstarter, or the Facebook, of the Ubers, of the Airbnbs and puts it in code and eliminates the need for you to worry that someone would backstab you or distrust you."

Here D1 talked about the risk of being backstabbed or exploited. Similarly, E1 talked about the risk of being exploited and backstabbed, but not only from companies but from your own government:

"But in countries in Asia and Africa where […], if you are making a transaction, you are not sure that it will go through because someone at the bank has decided to freeze or confiscate the money, or that you have money at an account but the government decides that 'no, now we are confiscating all personal property' and freezes all your assets. That is where I see the real application and strength of Bitcoin and blockchain."

Weaknesses of Humans

While the interviewees saw that removing human intermediaries could result in removing the risk of opportunism, they also spoke about the weaknesses of humans. F1 provided his view on the issue:

"I am no mathematician, but what I understand about the math is that the probability of a computer system [like blockchain] would fail versus a person would fail, at the bank or something, then I believe that it is a higher risk that a human would become corrupt or make a mistake than a computer system would fail, or that the math does not add up. In my opinion, most shit that fails seem to be 'human error'. When looking at the traffic, air traffic, the heavy industry – mostly it is people that are making the mistakes and the bad deeds."

While F1 mainly spoke about human weakness in terms of making mistakes; additionally, D1 argued that humans are vulnerable and may also fail due to physical pressures:

"I mean… and I need to underline the fact that humans are vulnerable too. Not only the issue of mistrust but also to pressure, of decease, of death of all sorts of weaknesses that put humans in a much less favourable position compared to a robot, or to a code. When it comes to money that's even higher, that's why people are moving towards bitcoin and away from cash because they don't trust or don't think that their governments are capable… maybe they might think of them as in negative terms as being dishonest but they actually can be exposed to all kinds of pressure. That doesn't mean that they are dishonest, but you are putting a lot of emphasis on a human element that is vulnerable to many factors."

So, according to D1, humans are not necessarily only dishonest and vulnerable to social pressures, but they are also vulnerable to physical pressures that might lead to systems and governments failing.

Thereby, the blockchain is removing human intermediaries, and by doing so removes the risk of opportunism, and reduces the risk of succumbing to any human weakness such as disease and death.

4.2.2 Shared Truth

When sifting through our findings, we found that shared truth is a big part of why risk is reduced. J1 explained why shared truth is important:

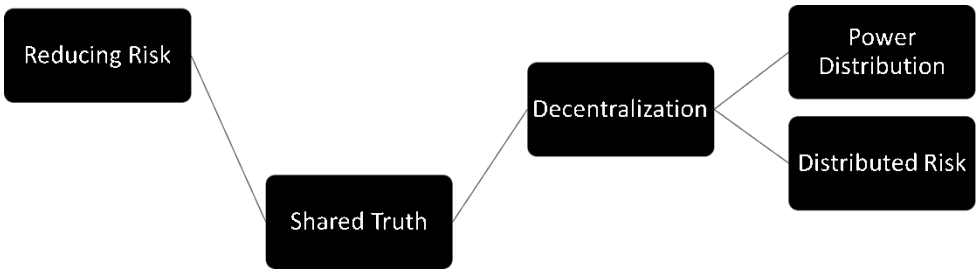
"...with these characteristics regarding hashing and so on, it makes one trust that this information cannot be changed later without it being noticed. So, you can yourself verify that all these hashes and signatures are correct, then you can trust that it is correct, and it creates a type of open trust in a system - we are talking about a shared truth."

Shared Truth contains two subcategories: (1) Decentralization and (2) Documented Truth.

4.2.2.1 Decentralization

Decentralization entails the structure of the blockchain, and what it means for the system itself. While decentralization is a subcategory itself, we found that it can be further separated into two subcategories: (1) Power Distribution and (2) Distributed Risk (see Figure 6). While both subcategories touch upon a similar topic, decentralization, they are being talked about from different perspectives. Power distribution deals with the destruction of central authorities by moving the control to the peripheral, and Distributed Risk looks at it from the point of view of the risk of internal failure and resilience from external attacks.

Figure 6 Decentralization



Power Distribution

Power distribution was one of the most talked about topics where eight of ten interviewees talked about it more than once. Collectively, they mention that the data is no longer owned by a central authority, but it is distributed to all nodes in the network. According to H1, this is due to practical and trusting reasons: *"there is, and it goes back to the trusting, there is nobody sitting holding that database of transactions who can change it and go back and undo something or do something that they haven't done"*. However, F1 had more of an ideological view and said that *"ideologically I believe that many think that 'now we are reclaiming the power of our money!"*. Similarly, E1 spoke about the blockchain as a method of regaining the power:

"…then you can build a decentralized or uncensored network. Because, the goal of the blockchain, from the start, is to build a network like our Internet where I can E-mail you without anyone in the middle that says 'no, I do not like that definition,' or, 'you cannot E-mail him' – an open network."

Moreover, when asked about the function of the blockchain, D1 stated that *"it simply is a solution that moves the authority to control value from a centre to the periphery, [...] so the idea is that instead of having a centre, one centre that does all the verification, you distribute verification tasks on lots of nodes across the network"*. While the system is open and the power is distributed to all nodes in the network, the blockchain may be difficult to understand. E1 entertained the idea of a knowledgeable technical elite taking over the system and writing codes that benefitted themselves; however, quickly answered his own thought by pointing out that the decentralized nature and distributed power in the network mitigate this:

"But if we need to trust a technical elite what happens then if they write [a code] that lets them get all the money? Then theoretically it is not trustless. But, what happens is that all of us that have connected to the network will, if it is to our benefit, upgrade to their system. But, if it isn't, people will not. […] So, actually it is trustless in this way because it is the user that is in charge. […] So, what we see today, practically, is that everyone who is connected has a vote."

Distributed Risk

While the blockchain was, as I1 put it, *"an ideological reaction [to the recession in 2008]"* the decentralized nature of the blockchain is also, according to our findings, beneficial from a security point of view as it distributes the risk and makes the system more robust, or as D1 put it:

"It replicates how nature evolves, you don't have one single tree that every other tree will rely on, they are actually disseminated in different decentralized ways. So, we embrace nature in that sense. So, if it makes

sense for networking, it should make sense for data as well. Because if you attack one single node that controls a lot of records, then you are possibly putting it in a vulnerable position. But if you distribute the data it makes it much more resilient."

F1 echoed this argument and added the element of corruption from an internal central authority. When asked to describe the blockchain he provided us with the following:

"I would define it as a decentralized or distributed database where you have spread out the risk of 'a point of failure' to the whole network instead of a third party that holds the security for the system. And, that it is a chain of information that is not corruptible."

Lastly, J1 provided the benefits of an open and distributed network from the perspective of hackers. He saw that this network, instead of shutting out hackers, inviting and indirectly rewarding hackers to test the system:

"…Ethereum was exposed to a lot of hacker attacks and what is interesting about that is that […] hackers traditionally have lived in an existence where one tries to earn money from illegal things; credit card information, darknet, and all those things. But, if you find a security gap in Ethereum and you can exploit it, […] then you can short the cryptocurrency [Ethereum] and speculate that the value of it will decrease when you release the 'feed'. Even if its value only decreases incrementally, you will make a lot of money. So, when it is known what has happened, the security gap is fixed. The funny thing about this is that [the hackers] receive a 'bug bounty' instantly. They are making money legally, and it can be quite large sums. So, one can say that hackers, in this case, […] are good as they are constantly discovering weaknesses…"

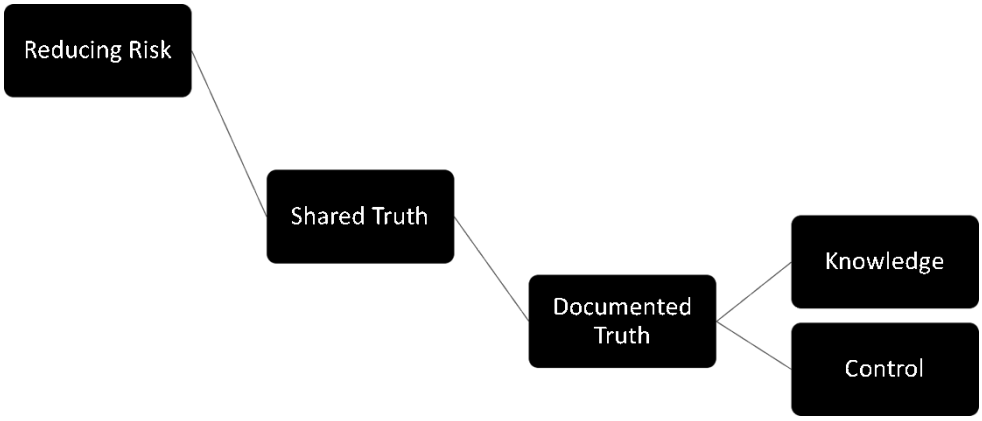
Consequently, according to our findings, decentralization is very important in Shared Truth and ultimately Reducing Risk. It distributes the power from central authorities, which reduces the risk of corruption and manipulation, as well as reducing the risk of one point of failure. Lastly, the decentralized and open nature of the blockchain allows anyone to view the system and find exploits and security flaws that, in the long run, make the system more resilient and robust. There is a connection between the decentralized nature and the next subcategory of Documented Truth, as when something is documented in the system it is distributed to the whole network.

4.2.2.2 Documented Truth

Documented Truth ties to Shared Truth as it is the documented truth that, when distributed, becomes shared truth. Moreover, Documented Truth is divided into two subcategories: (1)

Knowledge and (2) Control (see Figure 7). Knowledge ties to the ability to understand the information that resides in the blockchain and Control ties to the ability to be certain that the information on the blockchain will not change or behave unexpectedly. Due to these reasons, we see how Documented Truth and its subheadings are ultimately connected to Reducing Risk.

Figure 7 Documented Truth



Knowledge

When asked about the blockchain's trustless nature, our interviewees discussed the need to have knowledge to remove risk and make it trustless, or as trustless as it can be. For instance, I1 stated that:

"It depends on how you… I mean, 100% trustless... then you have to be a really sharp developer that has a very good understanding. So, one is able to look at the source code and know exactly what happens on the computer, and exactly know what software you use to connect, your private keys, how you store them. Absolutely, then it is trustless..."

E1 also discussed the need to have a good understanding and knowledge about the blockchain for it to be trustless. However, he highlighted the potential of gaining knowledge:

"Because you can be in Venezuela and say 'damn I cannot use the banking system! But, I do not trust Bitcoin either! So, I am going to sit down and study C++ enough to be able to evaluate Bitcoin, download my own node, connect to the system, exchange Bitcoins to my own node, make my own transaction, broadcast

it to the whole network all from my own node, and then see it getting accepted. I can trust myself now, it is possible, it is a living hell and it is not meant for anyone to do it, but it is possible.'"

Here E1 also touched on the transparency of the blockchain. This transparency manifests itself through the open nature of the source code and the ability to see all transactions broadcasted live. J1 agreed with this description and stated how special this feature is:

"blockchain is a special system in the way that all data in the system and all code is known. There are no other systems where both the data and the systems' source code is known by all users. It doesn't exist. All business systems that exist today are closed."

The blockchain was also discussed as being traceable, which, in combination with the transparency, enables one to audit the system. According to G1, this ability itself provides trustworthiness: *"so the system in itself is trustworthy, especially if the source code is open so you can audit and look at it"*. Moreover, it was brought up by A1 that this auditability makes it so that anyone may see if anyone tries to cheat inside the blockchain. For instance, in the case of charity organizations a blockchain may record and track where the donations go and where it disappears, making the money trail more transparent and possibly trustworthy:

"Precisely, safety, traceability, and transparency in functions where we need it. It does not hinder anyone from cheating, but then everyone sees it, and that is the point. What happens in a welfare system where, at least on the international market, cheating is prominent. Money disappears and in great quantities. What would happen with such a system if cheating was not possible, or at least if everyone could see if someone was cheating?"

A1 used the following example:

"We trust the Red Cross! We trust Doctors without Borders! But, we know as well that there is so much stuff that happens with our money along the way, and that is my taxed money that I give to charitable purposes. What does it mean for the organizations that we put our trust in? Do we trust them more or less, because you can see how much money that disappears along the way, and how little money that actually goes to the purpose?"

Since knowledge ties to the ability to understand the information on the blockchain, transparency and traceability allow insights into the technology and network, so knowledge can be attained.

Control

While knowledge is important as it enables the users to learn what the blockchain does and see what is going on in the blockchain, it was also established that control is important to ensure that the information and source code in the blockchain will not change or act unexpectedly.

One thing that enables that data will not be changed is the consensus mechanism, e.g. Proof of Work. However, it does not make the data 100% immutable, but it does make it immensely difficult for anyone to change any piece of data in the blockchain. E1 explained:

"So, what is meant by trustless? Generally, if you look at Bitcoin, it means that you have the blockchain […] and then you have Proof of Work, that is this energy that is consumed that works like […] blocks of stone that are built on-top of each other so that the stones below are getting more expensive to change."

So, by using E1's analogy, each new block in the blockchain is like a block of stone that is added, which makes it difficult to change previous blocks. H1 added:

"Once you have networks set up and a chain [that] has been created over a period of time, you know that's not going to change. [...] It's about trust, but if you look at something like bitcoin the amount needed to actually change anything is so vast, you know it's largely immutable, and when you go to the smaller blockchains, that trust is easier to break. Even so, it would need quite a lot of effort."

In this way it is, as D1 says, it is like: *"carving stone where you don't really have the ability to do it again when it's done it's done"*.

While you can rely on the data on the blockchain because it is largely immutable, you can also rely on the code of the blockchain since it is predictable. D1 makes the following argument: *"Humans are not necessarily predictable, but code is predictable. Because code sticks to what it does, 1+1=2, you cannot expect it to give you 3."*. Moreover, according to D1, the predictability of the code aligns expectations so that people can more easily understand what is going on:

"So it means that whoever wrote the code, and whoever read the code, assuming that people read, can understand what this code does. They are in an agreement of what the risks are, what the expectations are, everything in the code will be an agreement among the various players, so they can just send the money or send the value and then forget about it because the process will exactly meet their expectations."

Therefore, Control, through immutability and predictability, makes sure that what is viewed on the blockchain will not change as time goes by. This is beneficial as it allows people to rely on the data on the blockchain as well as aligns their expectations of what will happen to the data since it is all in code.

5. Analysis

In this chapter, the reader will be reminded of both theory and gathered empirical findings as this chapter brings the two together in order to conduct an in-depth analysis. The chapter is structured in a way that it starts by analyzing components needed to answer research question 1, which is divided into trust in community and trust in technology. The way this is done is by first analyzing what type of trust is placed in the focal points. The second step of analysing the focal points of trust is to see if it really is trust that is put in them, or if it is familiarity or confidence. Finally, in order to answer research question 2, the function of the blockchain will be analyzed and compared with Luhmann's function of trust. This is also divided into two steps where it starts with seeing if the blockchain and trust are functionally equivalent, and thereafter to see if they are substitutable.

5.1 A Shift in Trust

There is a consensus in the blockchain literature on trust that when using a blockchain, trust shifts from institutions to technology. However, here the research community is divided into two schools of thought. Lustig and Nardi (2015) and Maurer et al. (2013) argue that trust shifts to code whereas Mallard et al. (2014) argue that trust is put in the programmer, i.e. the person creating the code. Our findings indicate that trust is put in the technology; additionally, our findings show signs that trust is also put in the community. Since our findings are divided between trust in technology and trust in community, this section will use the literature in combination with our findings to take a closer look and analyze the focal points of trust separately to understand where and what type of trust is placed: the community, the programmer, or the technology itself – the code.

5.1.1 Trust in Community

Our findings show that one focal point of trust that differs from the literature is trust in the blockchain community. This trust takes shape in two ways: (1) one has to trust that a majority of the community will behave correctly and (2) that the community is knowledgeable enough to maintain the system. If one looks deeper at what actually is stated, it is evident that the types of trust can be connected to Das and Teng's (2004) concept of goodwill- and competence trust. Trusting that the community will behave correctly is a type of goodwill trust, i.e. the trustee, has to have the intention to behave as the trustor expect. Furthermore, trusting that the community is knowledgeable enough to maintain the system is competence

trusting. Here, the focus lies on the ability of the community to behave as expected (Das and Teng, 2004). However, the question remains why this trust exists. As Das and Teng (2004) argue trust is used to counter risk, goodwill- and competence trust are only necessary where their counter types of risk exist, i.e. relational- and performance risk. Therefore, one reason why these types of trust are put in the community is that there are specific types of risks. Relational risk is present because the users of a blockchain cannot be certain that the community will behave as expected, therefore they trust it to do so. Moreover, there is also a performance risk, i.e. the risk that the users in the community are not able to achieve what is expected of them, and thus the need for competence trust. An example that shows competence trust, and consequently performance risk, is when H1 argues that he trust the blockchain the same way he trusts nuclear physics:

"I think you then place your trust in the community. It's a bit like nuclear physics. There are huge amounts of literature published on it, I can go out and read it all but I wouldn't understand a word of it. But, I believe that it is right because there are other very bright [people] out there who can read it and are commenting on it and do agree with it. In the same way I can't read the code for blockchain, and I'm not going to understand it, but I know, that because it is open sourced, there are other people reading and if they would be able to poke holes in it, it would be found out and published online very quickly".

A clear example that relational risk exists is when H1 explained that there was a mining pool that was close to getting 51% control of the Bitcoin blockchain. Fortunately, they decided to split up so that they would not gain control but could have if they wanted to. Thus, the risk of people not behaving as expected is present and goodwill trust is necessary.

Thus far, we have gained an understanding that the type of trust put in the community is goodwill- and competence trust. However, as this thesis takes the theoretical point of view of Luhmann (2000; 2005), who states that trust, familiarity, and confidence are functionally equivalent, it is of importance to analyse whether it really is trust that is put in the community or if it is familiarity or confidence.

The argument that trust does not exist can be considered as it might be familiarity and not trust that exists in the blockchain community. According to Luhmann (2005) familiarity is a shared worldview or consensus of what the world looks like. This entails that every actor in that world knows that other actors see the world in the same way, and thus will act the same

way as themselves. Therefore, there are no uncertain outcomes that may happen, as one knows what one's own action would be in a certain situation. Nakamoto's Bitcoin whitepaper (2008) maps out how the blockchain creates consensus through the immutable nature of the hashing timestamp server, PoW consensus mechanism, and transparency. This view is in line with our findings that states that:

"...with these characteristics regarding hashing and so on, it makes one trust that this information cannot be changed later without it being noticed. So, you can yourself verify that all these hashes and signatures are correct, then you can trust that it is correct, and it creates a type of open trust in a system - we are talking about a shared truth." (J1)

However, the PoW consensus mechanism does not make it impossible to take over a blockchain and gain 51% control of it, but it makes it very difficult as PoW forces nodes in the network to spend computing power to create new blocks. Moreover, the coin emission incentive makes it economically beneficial to help to maintain the system rather than breaking it. This means that if one or a group of nodes would have the ability to take over the system, they would be more financially incentivized and inclined to support the system instead of breaking it. Therefore, the relational risk is vastly reduced. However, an anarchistic and nihilistic figure that is incentivized by "sending a message" rather than financial gain (like the Joker in Batman – The Dark Knight) would still have the possibility to take over such a system just for the heck of it, which indicates that there is some amount of goodwill trust placed in the blockchain community. Luhmann (2000) emphasized that the level of perceived risk is one of several distinctions between trust and confidence. He argues that confidence deals with situations that are considered very unlikely to happen, whereas trust deals with situations where the risk is at a level where it is considered. The likelihood that Joker-figure would both have the incentive and ability to break the system could be argued to be minimal; therefore, it could be argued that it is not trust that is put in the community but confidence.

Luhmann (2000) identifies the similarities between trust and confidence as both deal with future expectations which may result in disappointment. Aforementioned, he makes the distinction between the two in the amount of risk perceived. He argues that confidence is the subconscious expectation of minimal cases of uncertainty where no other alternative is considered. One could argue that the likelihood that someone in the community would perform an attack is so minimal that no one would ever consider it. Albeit this risk may be

minimal, the known events of mining pools almost gaining control of blockchains has realized this threat. However, the question arises whether these events have increased the perceived risk of a system breaking by ill-wishing individuals enough to be considered as trust or confidence. While such a discussion may be fruitful, there is one aspect of the relationship between trust and confidence that suggests that trust, instead of confidence, is put in the blockchain community. According to Luhmann (2000), confidence is the product of contingencies and danger, while trust is a product of risk. This is interesting as the question if the event described above is one of risk or danger. We argue that this is an event of risk, since if a blockchain would break, such as the Bitcoin blockchain, it would result in economic losses for the people investing in it, but would not entail any real danger of personal damage. Moreover, we argue that, as it is now, Bitcoin and other systems like it are not big enough that them failing would result in a global financial crisis, which would entail danger. However, if the world's finances are tied in a blockchain, such as Bitcoin, then the event of it breaking is an event of danger. Moreover, blockchains that deal with personal data, such as medical records, would involve danger in the case of it breaking. Consequently, we see that the answer, if confidence or trust is put in the blockchain community, depends on the size and nature of the blockchain. However, presently, there are no running blockchains that are big enough or that deal with personal data to have confidence placed in them. Therefore, we argue that the future expectations when using a blockchain today is based on risk, and not danger – trust is placed in the community.

5.1.2 Trust in Technology

The other focal point of trust discovered was trust in technology which is in line with the blockchain literature on trust (Lustig & Nardi, 2015; Maurer et al., 2013). Regarding trust in technology, our findings show that it is necessary to trust that the technology is working properly. For instance, I1 said, *"you [have to] have some kind of trust for the technology and the math behind it [blockchain]"*. An interesting finding is that competence trust is the only type of trust that is put in technology since the only risk present is performance risk. D1 argued that relational risk does not exist since code is predictable, there is no risk that the code will not behave as expected *"...code sticks to what it does, 1+1=2, you cannot expect it to give you 3"*. Since the code does exactly what it has been programmed to do, there is no risk of, for example, opportunism - the code does not have a will on its own. Moreover, D1 added that there is no need to trust the programmer when he is no longer working on the code.

"...if you are going to use trust with humans that are involved in the picture, then you no longer need to trust anyone on the blockchain. But if you use trust for anything they produced, [...] then yeah, I mean you can use trust but I would favor not because I would associate the word trust in linguistics in my own native language, in Arabic, you actually use trust only with someone who's living, [...] you've given him your money and you trust that he would not do something bad with it. So he's a human being at the end. But if it's code, you can predict what it will do because it's open source, you can see what it can do.".

As seen in this quote, the code is predictable because of the transparent nature of the blockchain. However, if the code is auditable and one can see and predict what it supposes to do, is performance risk and competence trust involved? Additionally, what does it mean to be able to predict the code? We argue that to be able to predict the outcome with certainty, one needs to be aware of and know all possible outcomes. Therefore, in order for one to know all the possible outcomes, one has to have 100% knowledge about what the code says and what it will do. If this is true, and one knows 100% what the code will do, then there is no performance risk, and no trust is needed (McAllister, 1995; Gambetta, 2000). Luhmann (2005) similarly states that if one can predict what others will do then familiarity is established. Moreover, he argues that if there is 100% familiarity then there is no need for trust. Therefore, one has to have 100% knowledge in order to have 100% familiarity. According to our findings, due to the transparent nature of the blockchain, users have the ability to gain knowledge of what the technology is meant to do:

"I mean, 100% trustless... then you have to be a really sharp developer that has a very good understanding. So, one is able to look at the source code and know exactly what happens on the computer, and exactly know what software you use to connect, your private keys, how you store them. Absolutely, then it is trustless." (I1)

Here the interviewee emphasizes the fact that in the blockchain, one has the possibility to know exactly what happens. However, another interviewee argued that one cannot be 100% sure because there will always be a security risk:

"there is always a security risk, you can always find a flaw or a way to modify the blocks or get around it in any way. Something that we all experience as secure today, but we do not know. They hacked [...] the Intel core processors that no one found in 15 years or something like that. There is always a risk…" (G1)

Therefore, there is always a factor that is not known, or that has not been considered; thus, one cannot have 100% knowledge. This reinforces Luhmann's (2000) argument that familiarity, confidence, and trust are not fully substitutable as they all depend on each other. This means that no matter how much familiarity exists there will always be some need for trust. Therefore, we argue that no matter how much knowledge one has and how well one can predict an outcome, there is always some factor that is overlooked, unknown, or simply too complex to predict. Consequently, a performance risk exists; however, where does it exist?

Since performance risk is regarding the ability to perform a task, we argue that this risk cannot exist in the technology itself. This is because technology is the creation of humans, it has no will on its own, it will only do what it has been instructed to do. Therefore, if a code, for example, is not behaving as expected it is only doing so because of a faulty construct, i.e. the person who created the code did not possess the ability to write a flawless code. Therefore, performance risk exists in the programmer; consequently, that is where competence trust is placed. Alternatively, as earlier argued, if trust cannot be placed in a person that is not present anymore, then the competence trust is placed in the blockchain community's ability to understand and spot the flaws in the code. This is in line with Seigrist and Cvetkovich (2000) who argues that when actors do not have enough knowledge about, for example, technology, they cannot make decisions on their own and instead put their trust in experts. Therefore, we argue that regarding the blockchain, trust in technology does not exist.

5.2 Function of the Blockchain

While there still exist trust in the community, the question remains if the blockchain has the potential to become trustless. Taking Luhmann's theory of functional equivalence (2005), for the blockchain to have the potential to substitute trust and be trustless it first must have the same function as trust. This part of the chapter will analyze what the function of the blockchain is and if it has the same function as trust. Therefore, this part will conclude in a discussion about whether the blockchain can substitute trust.

From the findings we see that the function of the blockchain is reducing risk, but how and why is risk reduced? According to our findings, the blockchain is reducing risk by removing human intermediaries and establishing a shared truth. As the blockchain removes the human intermediary and replaces it with code, both the risk of someone behaving opportunistically

and the human weakness are removed. As mentioned earlier, code does not have a will of its own; therefore, there is no possibility that it will execute in any other way than it is programmed to, which reduces the number of possible outcomes, i.e. risk.

While the blockchain is a technology that removes human intermediaries there are still humans maintaining and using the system, which entails uncertainty. Moreover, as our findings suggest, the blockchain disrupts central authority by creating a decentralized system. The benefits of such a system are that it distributes both power and risk to all the nodes in the network. As every node in the network now possesses an amount of power, it is crucial to establish consensus in the network to prevent chaos. This is enabled by establishing a shared truth. However, to establish a shared truth it is paramount that the users in the network can be certain that the data and code residing on the blockchain is what it says it is and that it is immutable. This is done through the hashing ability of the timestamp server and the consensus mechanism, which creates a documented truth that is very difficult to change. Moreover, the transparency of the blockchain enables people to audit what is happening in it, which lets them view and understand the documented truth. When this documented truth is distributed in the decentralized network it becomes a shared truth and a consensus is established as everyone in the network knows that the majority have the same worldview. Consequently, the blockchain creates familiarity as one can be sure that the majority see the same as oneself. Moreover, as familiarity deals with the past, so does the blockchain, as every new block created is referring to its predecessor in order to establish its own existence in the blockchain. Therefore, since the blockchain creates a familiar world through its shared truth, and removes the possibility of opportunistic behaviour, our findings conclude that the blockchain profoundly reduces risk, and so complexity.

Due to this finding, we can see that the blockchain creates familiarity that ultimately reduces complexity, which results in it being functionally equivalent to trust. As stated in the case of trust in the community, familiarity and trust are dependent on each other which means they will never be able to be fully substitutable. As such, since the blockchain creates familiarity, we conclude that the blockchain will never be able to fully substitute trust.

6. Conclusion, Contributions, Limitations, & Future Research

This chapter will use the results of the analysis in order to answer the research questions. Moreover, the theoretical and practical contributions of this thesis will be presented and a self-evaluation is made to consider the limitations of the study. Finally, suggestions for future research will be provided.

6.1 Conclusion

This thesis explored the trustless nature of blockchains. This was done as a response to the generally accepted notion that blockchains are trustless systems. Therefore, the purpose of this study was to develop an understanding why the blockchain is or ever has the potential to be, trustless. Consequently, two research questions were formed:

1. Is the blockchain trustless today?
2. Does the blockchain have the potential to become trustless?

Is the blockchain a trustless system?

Our empirical findings suggest that trust still exist when using a blockchain, more specifically trust in the community and trust in technology. However, our analysis suggests that no trust is placed in technology but in the community. This is due to the nature of technology itself, it has no will by itself, and therefore pose no relation- or performance risk. Mallard et al. (2014) state that trust is put in the person behind the technology, but our analysis shows that this trust is rather put in the community's ability to monitor the code and system. To answer our question, since trust is placed in the blockchain community, we conclude that the blockchain is not trustless.

Does the blockchain have the potential to become trustless?

While the previous answer provides a snapshot of the blockchain as it is today, we also asked if the blockchain has the potential to become trustless in the future. We did this by analyzing the blockchain's functionality and compare it to the functionality of trust. The result was that the two are functionally equivalent, thus establishing the potential of being substitutable. We found that the blockchain is functionally equivalent to trust as it creates familiarity, which reduces complexity. Therefore, we could see that the blockchain, per definition, has the potential to substitute trust. However, our analysis concluded that since the blockchain

creates familiarity it cannot fully substitute trust. Therefore, the blockchain does not have the potential to become trustless.

6.2 Contributions

Since this thesis is one of few papers that critically discuss the trustless nature of the blockchain, the contributions of this thesis are manifold. First of all, our findings map out the limitations of the blockchain as a trustless system. From a theoretical point of view, this thesis tries to provide clarity in the binary debate about the trustless nature of the blockchain as it does not merely look at the current state, but also takes a fundamental perspective of the possibility of the blockchain being trustless. We deem this type of analysis and discussion beneficial for the academic community as it provides nuance in what aspects of the blockchain makes it trustless but also highlights where it fails to replace trust.

As a result, this type of functionality analysis has allowed us to pinpoint the blockchain's fundamental function - reducing complexity. This does not only advance the academic understanding of the blockchain but also have practical implications for blockchain managers and designers. For instance, now designers may be more aware of what to take into consideration when designing blockchains, especially when considering what risks users are facing when using a blockchain. This new understanding of the function of the blockchain may also help managers and designers to understand where the blockchain might be applicable, i.e. where it can reduce complexity. Moreover, as this thesis highlights what characteristics of the blockchain make it still risky, users are able to look and understand why the blockchain they are using is risky or not. We find this especially important regarding a technology that the community has dubbed trustless since it sends the message that there is no risk.

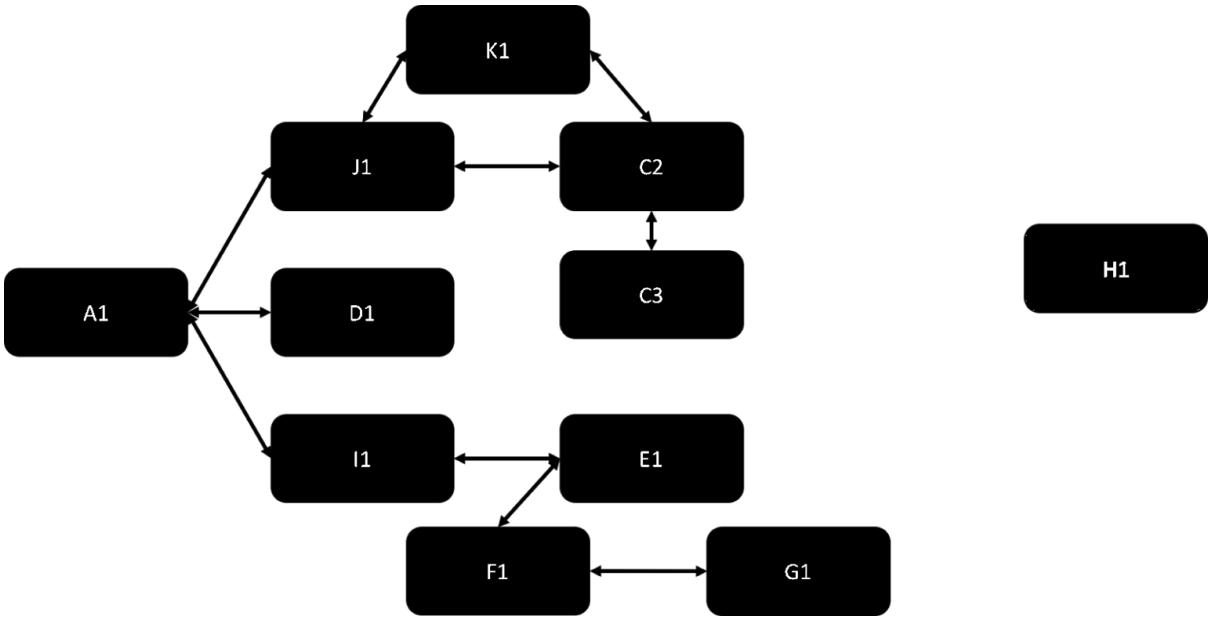
Furthermore, this thesis maps out how the blockchain reduces risk that, as discussed above, provide contributions to the understanding of the blockchain. However, it might also provide contributions to risk theory in general. As our model is mapping out the blockchain's function and how the blockchain is reducing risk, we also mapped out a way how risk can be reduced. We see the potential that this model may be applicable in other theoretical settings as well as practically where one wants to reduce risk. Consequently, we might not only have created a model of how the blockchain is reducing risk but possibly also how risk is reduced in general.

Finally, this thesis contributes to the trust literature, more specifically literature regarding trust in technology. By providing findings that suggest that trust in technology does not exist in blockchains, this thesis is contradicting current trust literature regarding the blockchain that states that trust is put in code (Lustig and Nardi, 2015). Ultimately, it might be possible to deduce that trust in technology as a concept does not exist, but that trust is put somewhere else, which is in line with Seigrist and Cvetkovich's (2000) view.

6.3 Limitations

One of the limitations of this thesis is one regarding the sampling techniques used. The blockchain is a novel technology, therefore there is a limited number of experts in the field. Thus, convenience sampling and snowball sampling were good techniques to gather data. However, when conducting the interviews it was evident that a lot of them mentioned similar examples and had similar views on the topic. It was further noticed that a part of them had some sort of relationship, either personal or professional, as indicated by the arrows in *Figure 8*. This can, in turn, affect the answers in the interviews, thus affecting the findings of this thesis. Moreover, due to the small population of blockchain experts, all the interviewees were based in Stockholm which limits the findings from a rich cultural diversity and might create homogenous findings.

Figure 8 The Relationship of Interviewees



The blockchain has become somewhat of a marketing term, which means that the definition of it may differ depending on who you ask. This was apparent especially when we asked our interviewees to define the blockchain their answers varied all from it being a distributed ledger, just being the chaining timestamp server, while others say that it is a paradigm shift of how to store information that moves authority from centres to the periphery. The definition of the blockchain depends on who you ask because they will describe it in terms they are familiar with. For instance, if you ask someone from finance they will say that the blockchain is about transactions. Moreover, there is a variation of different blockchains depending on how it is constructed. For instance, a blockchain that is based on the consensus mechanism Proof of Work is different from a blockchain based on Proof of Stake, and there are many more ways one blockchain can differ from another. This thesis has focused on public blockchains as we saw them having the largest potential of being trustless. Moreover, as we discussed the trustless nature of blockchains with our interviewees, the type of blockchain most commonly mentioned was a PoW blockchain, much like the Bitcoin blockchain. As a result, this thesis may lack somewhat in transferability of different types of blockchains.

The topic of trust is vast and has been studied by many different scholars from many different schools of thought and academia. While there is an abundance of research talking about why trust is or is not risk-based, calculative, a choice, psychological state, etc. we decided to focus on trust in the blockchain from one perspective; functionality. We chose this method as we wanted to analyze if the blockchain could substitute trust and become trustless. However, we understand that there are various other perspectives to take on trust, which could provide a fruitful analysis and, perhaps, different result. For instance, in our empirical findings, we found that the blockchain enables collaboration. However, since we analyzed the data from the functionalist perspective, we deemed it not appropriate to present. This is because we argue that collaboration is only a result of the function of the blockchain, i.e. reducing complexity, and not part of the function. However, by looking at our own theoretical framework we can see that collaboration is an important aspect of interorganizational trust and that possible and interesting findings may be unveiled if one would take another perspective of trust and include collaboration. Therefore, we are humble in that we chose one school of thought out of many possibilities, which lead to our conclusions.

6.4 Future Research

Due to the exploratory nature of this thesis, we took a first step towards understanding the trustless nature of the blockchain. Moreover, due to the research design, this study is interpretive in nature. Therefore, we urge future researchers to test our main assumption, that the blockchain is not and cannot be trustless. Additionally, we encourage future researchers to test our model on risk reduction to see if it carries weight and, if so if it is applicable to other settings than the blockchain.

Furthermore, in this study the types of blockchains mostly discussed are the ones based on PoW from a function perspective. To further advance the understanding of trust within the blockchain, we suggest that future research should include other types of blockchains as well as look at them from a different perspective than function, e.g. structure perspective.

Lastly, as discussed by A1 in the empirical findings, the transparency of a blockchain allows users to see if anyone tries to cheat. We agree with A1 that it is an interesting question what happens to the trust of charity organizations when users see how their donations are treated and deem this a great case of analysis. However, due to the exploratory nature of this study, it resulted in a broad scope of trust and the blockchain. Therefore, we suggest future research to look more closely at different cases where the blockchain is used and how it affects trust.

As previously stated, this thesis found an interesting connection between the blockchain's function and collaboration. However, since it was deemed that collaboration was not part of the function but rather an outcome of the function this was not thoroughly analyzed. We suggest future research should look more closely at how the blockchain enables collaboration and what effects this might have on an organizational as well as from a trust perspective.

Finally, we concluded our analysis by questioning whether trust in technology exists. According to our findings, trust in technology is not present in the blockchain, but is it present elsewhere? This is something that we believe could be interesting to further explore and discuss.

We hope that this thesis will be just one of many that analyze and discuss the connection between trust and the blockchain. Trust plays a huge role in general, whether it is personal, business, or governmental relationships, and we see that the blockchain will have a significant

impact on it. Therefore, as the blockchain has a vast potential, we deem it necessary to further research the topic to build a good understanding of its connection with trust.

7. Additional Thoughts

This final chapter of the thesis will discuss additional thoughts that are beyond the limitations of the purpose.

Since this study has followed Luhmann's theory of functionality (2000; 2005), it was concluded that the blockchain cannot theoretically become trustless since familiarity, trust, and confidence cannot fully substitute each other. However, it could be argued that this is not a true representation of reality, as theory is just a way of interpreting it. Therefore, it is possible that the blockchain could become virtually trustless as it may reduce risk to the extent that risk becomes infeasible to consider; consequently, make any level of trust needed redundant. Further, from a relativistic perspective, we collectively create our reality. Therefore, if the community considers the blockchain to be trustless then that is the reality they live in, no matter what a theory says. Thus, the blockchain can be perceived to be, or become, trustless no matter what this study is suggesting. Another interesting question that arose in the interviews was whether there is any value of making a trustless system. Even though the result of this thesis is that it is impossible to build a completely trustless system, we argue that there is a great value of building a system that reduces as much risk as possible, thus making it as trustless as possible.

An interesting finding that unfortunately did not fit into our purpose and research questions is that as a result of the blockchain reducing complexity, it also promotes collaboration. Now when there is a shared truth, entities like banks and businesses are more able to collaborate as they know that the information residing on the blockchain is true and not corrupted by their competitors. This has obvious benefits for the different industries where the blockchain will be applied to as it streamlines workflows and provides efficiency in day-to-day operations. While this is a beneficial outcome of the blockchain's function, the blockchain is, paradoxically, in itself vulnerable to too much collaboration. As discussed in the analysis, if a group of nodes gain at least 51% control of the network the system might fail, and the mechanisms that create a documented truth are jeopardized. We see this as an interesting discussion as it seems like blockchains are vulnerable to the very thing it promotes.

While the concepts of trust, familiarity, and confidence are fundamental to the society they are, and have, changed throughout history. Luhmann (2000) concluded that the conditions of trust, familiarity, and confidence have changed as a result of new technologies. He argues that writing, literacy, and the printing press have had an important impact on familiarity. He argues that as these new technologies were created, libraries of knowledge that might be unknown to some are now known to someone else. Thereby, as people might have different bases of knowledge, the border between what is familiar and unfamiliar becomes blurred. As a result of this, institutions, such as religion, loses its ability to establish familiarity. Now it is not possible to communicate what is bad and wrong, but that the question is now how the knowledge is used, positively or negatively? Moreover, he argues our societies have become more contingent with changing laws, fluctuating economies, and new scientific discoveries. Due to this, he argues that the relationship between trust and confidence have changed, to the point where trust only deals with interpersonal relationships and confidence deals with the participation of functional systems, like the economy or politics. Interestingly, we see how the blockchain could be the technology that flips this on its head. While the printing press has disseminated knowledge and blurred the border between what is familiar and unfamiliar, the blockchain makes this line distinct through a shared truth that everyone sees and everyone can be certain will not change. Moreover, as Luhmann (2000) discuss how the ever-changing system, the society as a whole, is making confidence more important, we see how the blockchain does the opposite, through its immutability, which would mean that it creates a system where trust prevails. Interestingly, this is in line with our findings as the concept of trust was predominantly discussed. Furthermore, Luhmann argues that choices of inclusion or exclusion are no longer a rational choice or a risk-taking endeavour as there is no way for any participant to 'opt-out' from the system. This is also very interesting as that the very invention of the Bitcoin blockchain gives participants of the society the option to, if not fully, partially opt-out from society. Therefore, to participate in the society is no longer a decision based on confidence, but a decision of trust as there now exists a feasible alternative.

References

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS. *Twenty-Fourth European Conference on Information Systems* (pp. 1-14). Istanbul: European Conference on Information Systems.

Berger, P. L., & Luckmann, T. (1966). *The Social Construction of Reality.* New York: Penguin Books.

Bruneel, J., Spithoven, A., & Clarysse, B. (2017). Interorganizational Trust and Technology Complexity: Evidence for New Technology-Based Firms. *Journal of Small Business Management, 55*(1), 256–274.

Bryman, A., & Bell, E. (2007). *Business Research Methods, 2nd edn.* Oxford: Oxford University Press.

Buntinx, J. (2017, November 13). *One Zcash Mining Pool Controls Over 51% of the Network Hashrate.* Retrieved from https://themerkle.com/: https://themerkle.com/one-zcash-mining-pool-controls-over-51-of-the-network-hashrate/

Christidis, K., & Devetsikiotis, M. (2016, June 3). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 2292-2303.

Coinmarketcap.com. (2018). *Bitcoin.* Retrieved from https://coinmarketcap.com/: https://coinmarketcap.com/currencies/bitcoin/

Coleman, J. S. (1994). *Foundations of Social Theory.* Cambridge: Harvard University Press.

Das, T. K., & Teng, B.-S. (1998). Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances. *Academy of Management Review, 23*(3), 491-512.

Das, T. K., & Teng, B.-S. (2004). THE RISK-BASED VIEW OF TRUST: A CONCEPTUAL FRAMEWORK. *Journal of Business and Psychology, 19*(1), 85-116.

Delbufalo, E. (2015). Subjective trust and perceived risk influences on exchange performance in supplier—manufacturer relationships. *Scandinavian Journal of Management, 31*, 84-101.

Deutsch, M. (1962). Cooperation and Trust: Some Theoretical Notes. *Nebraska symposium on motivation* (pp. 275-320). Lincoln: Nebraska University Press.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the Influence of National Culture on the Development of Trust. *Academy of Management Review, 23*(3), 601-620.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2015). *Management & Busienss Research 5th edn.* London: Sage Publications Ltd.

Gambetta, D. (2000). Chapter 13: Can We Trust Trust? In D. Gambetta, *Trust: Making and Breaking Cooperative Relations* (pp. 213-237). Oxford: University of Oxford.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory - Strategies for Qualitative Research.* New Brunswick, USA: Aldine Transaction.

Glaser, F. (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 1543-1552). HICSS.

Gobel, J., & Krzesinski, A. (2017). Increased block size and Bitcoin blockchain dynamics. *27th International Telecommunication Networks and Applications Conference.* IEEE.

Goldman Sachs. (2018). *Blockchain - The New Technology of Trust.* Retrieved from http://www.goldmansachs.com/: http://www.goldmansachs.com/our-thinking/pages/blockchain/

Kairos Future. (2017). *The Land Registry in the blockchain - testbed.* Lantmäteriet, Landshypotek Bank, SBAB, Telia Company, ChromaWay, Kairos Future. Stockholm: Kairos Future.

Lewicki, R. J., & McAllister, D. J. (1998). Trust and Distrust: New Relationship and Realities. *Academy of Management Review, 23*(3), 438-458.

Luhmann, N. (2000). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta, *Trust: Making and Breaking Cooperative Relations* (pp. 94-107). Oxford: University of Oxford.

Luhmann, N. (2005). *Förtroende - En mekanism för reduktion av social komplexitet.* (E. Backelin, Trans.) Göteborg: Diadalos AB.

Lustig, C., & Nardi, B. (2015). Algorithmic Authority: The Case of Bitcoin. *48th Hawaii International Conference on System Sciences* (pp. 743-752). IEEE.

Möllering, G. (2001). The Nature of Trust: From Gerog Simmel to a Theory of Expectation, Interpretation and Suspension. *Sociology, 35*(2), 403-420.

Mallard, A., Méadel, C., & Musiani, F. (2014). The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin. *Journal of Peer Production*, 1-10.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics, 23*(2), 261-277.

Mayer, R. C., Davis, J. H., & Schoorman, D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

McAllister, D. J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *The Academy of Management Journal, 38*(1), 24-59.

McIndoe-Calder, T. (2018). Hyperinflation in Zimbabwe: money demand, seigniorage and aid shocks. *Applied Economics, 50*(15), 1659-1675.

Nakamoto, S. (2008, October). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved April 2018, from https://bitcoin.org/: https://bitcoin.org/bitcoin.pdf

Pennington, R., Wilcox, H. D., & Grover, V. (2004). The Role of System Trust in Business-to-Consumer Transactions. *Journal of Management Information Systems, 20*(3), 197–226.

Petroff, A. (2017, November 17). *How Robert Mugabe killed one of Africa's richest economies.* Retrieved from http://money.cnn.com/: http://money.cnn.com/2017/11/15/news/economy/zimbabwe-economy-robert-mugabe-history/index.html

Pozzebon, S. (2018, January 17). *You can't get $1 out of the bank in Venezuela. I tried.* Retrieved from http://money.cnn.com/: http://money.cnn.com/2018/01/17/news/economy/venezuela-cash-crisis/index.html

Provenance. (2015, November 21). *Blockchain: the solution for transparency in product supply chains.* Retrieved May 8, 2018, from www.provenance.org: https://www.provenance.org/whitepaper

Risius, M., & Spohrer, K. (2017, December 5). A Blockchain Research Framework. *Busniess & Information Systems Engineering, 59*(6), 385–409.

Robson, C. (2002). *Real World Research.* Malden, MA, USA.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust. *The Academy of Management Review, 23*(3), 393-404.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methids for Business Students 4th edn.* Harlow, Essex, England: Pearson Education Limited.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students 7th edn.* Harlow, Essex, England: Pearson Education Limited.

Seigrist, M., & Cvetkovich, G. (2000). Perception of Hazards: The Role of Social Trust and Knowledge. *Risk Analysis, 20*(5), 713-719.

Shenton, A. K. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information, 22*, 63-75.

Sheppard, B. H., & Sherman, D. M. (1998). THE GRAMMARS OF TRUST: A MODEL AND GENERAL IMPLICATIONS. *Academy oi Management Review, 23*(3), 422-437.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal, 38*(6), 1573-1592.

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* Thousand Oaks, CA, USA: Sage Publications, Inc.

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. *13th International Conference on Service Systems and Service Management* (pp. 1-6). Kunming: IEEE.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun Surv Tutor, 18*(3), 2084–2123.

Wahyuni, D. (2012). The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies. *Journal of Applied Management Accounting Research, 10*(1), 69-80.

WePower. (2017, November). *Energy trading platform powered by blockchain technology.* Retrieved May 8, 2018, from icorating.com: https://icorating.com/upload/whitepaper/CDt62AS6IjlVUY8CNdHk0aYJycsT7ez8Yp5HgKod.pdf

Williamson, O. E. (1993). Calculativeness, Trust, and Economic Organization. *The Journal of Law & Economics, 36*(1), 453-486.

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance. *Organization Science, 9*(2), 141-159.

Zhong, W., Su, C., Peng, J., & Yang, Z. (2017). Trust in Interorganizational Relationships: A Meta-Analytic Integration. *Journal of Management, 43*(4), 1050 –1075.

Appendix 1: Topic Guide for Pilot Interviews

Introduction • Start by introducing ourselves and the purpose of the interview • Ask for anonymity and approval for audio recording. • Ask them to introduce themselves
Blockchain • Why did you become interested in blockchain? • Do you work with blockchain today? - If yes, how? - If no, why? • What is the best thing with blockchain? • What do you think blockchain is contributing with? - What purpose do you think blockchain is fulfilling? • Is there a specific industry where you think blockchain has the biggest potential? • What do you want to know more about blockchain?

Appendix 2: Topic Guide for In-depth Interviews

Introduction

- Start by introducing ourselves, our research topic and the purpose of the thesis.
- Ask for anonymity and approval for audio recording.
- Ask them to introduce themselves
  - How did you get interested in blockchain?
  - What made you move from a merely interest in blockchain to work with it?
  - In what way do you work with blockchain today?

Function of Blockchain

- How would you describe blockchain?
  - You mentioned XXX, what does that mean to you?
  - Why did you use XXX to describe blockchain?
  - Why is XXX and XXX important for you?
- What function does blockchain fulfil?
  - In what way does blockchain do this?
  - What kind of pains could blockchain solve?
  - Why is this important?
- **What is the most important part of blockchain?**
  - **What is its role?**
  - **Why is it important that it is doing what it is doing?**
  - **How come blockchain works?***

Settings of Blockchain

- Where do you see the biggest need for blockchain?
  - Why?
- Where do you see blockchain working best/worst?
  - Micro (peer-to-peer)
  - Meso (interorganizational)
  - Macro (System/institutional)
- How would the dream scenario with blockchain look like?

Blockchain as a Trustless System

- There are people stating that blockchain is a trustless system, what are your thoughts on this?
  - Do you see that blockchain removes trust or simply reduces the need for it?
- How do you define a trustless system?
  - Explain how such a system would look like.
- **Why do you think people take their money from the banking system and put them in blockchain technology, cryptocurrency?**

* Bold text indicates questions added for in-depth interviews round 2