MODUL VIENNA UNIVERSITY
WKO WIEN PRIVATE UNIVERSITY

An Assessment of Trust in Blockchain and Bitcoin in Financial Applications

Bachelor Thesis for Obtaining the Degree

Bachelor of Science

International Management

Submitted to Dr. Horst Treiblmaier

Hannah Nicole Griesmayr

1721038

Vienna, 31st July 2020

Affidavit

I hereby affirm that this Bachelor's Thesis represents my own written work and that I have used no sources and aids other than those indicated. All passages quoted from publications or paraphrased from these sources are properly cited and attributed.

The thesis was not submitted in the same or in a substantially similar version, not even partially, to another examination board and was not published elsewhere.

July 31st 2020

Date

Abstract

Over the past decade the use of blockchain technology has strongly increased as its secure and immutable characteristics have enabled anonymity, privacy and security for many users. It has created a wave of disruption across a spectrum of businesses and industries, especially within the financial sector. As blockchain technology will be adopted increasingly in many fields, it will most likely impact peoples' lives at some point. However, with the adoption of a new technology that involves personal information or data, an environment of trust has to be created by businesses in order for people to be willing to use their services. This holds particularly true in services and systems involving peoples' finances.

This thesis assesses the layers of trust involved, and how the factors within them create trust towards the blockchain based financial system Bitcoin. Previous research finds that when it comes to trust in a technology based financial services or systems, four main attributes of trust have to be considered in addition to a persons' general propensity to trust in technology in order for a basis for trust to exist. These are: 'competence and ability', 'integrity and consistency', 'benevolence, concern and shared values' and finally, 'communications and transparency'. By studying these four attributes in both Bitcoin and the underlying technology blockchain as well as propensity to trust in technology, it was found that knowledge and comprehension are vital components when it comes to trust. Demographic groups that indicate to having more knowledge, understanding and exposure to technology, such as level of education, were generally found to have a higher propensity to trust in technology. Likewise, the trust attribute 'competence and ability' of both blockchain and Bitcoin was found to be the most important component when trusting either of the technologies. This suggests that industries and businesses primarily have to create knowledge and understanding in their users if they want to inspire trust in their product, when blockchain technology is involved.

Table of Contents

List of Tables

List of Figures

1. Introduction

In today's day and age being 'digital' is like bread and butter. Services and technologies offered on an online basis are essentially a part of almost every process of our day, be it when we get on our morning commute and check Google maps at what exact minute the train will arrive, or when we go online to order our lunch from the next deli to work. However, when we use these technological facilitators in our day-to-day lives, we also put a specific amount of trust into them by allowing them to access and potentially use our personal data. A recent study shows that around 80% of US American internet users 'go online' every day, and many seemingly constantly (Pew Research Center, 2019). When they go online, they mainly use social media applications, search engines and of course many services that facilitate their day-to-day lives, which also includes financial applications (Chakravorti, 2018). When it comes to their finances, people tend to be more critical of the services and systems they use, as this is an integral part of their lives. Thus, it is important that financial services and the systems they use are of a trustworthy nature from the user's perspective.

Using any form of technology requires a specific amount of trust into the technology from the person using it. This trust may be a development of several factors, a layer of which is the user's general propensity to trust in technology (Jessup et al., 2019). This tendency and attitude towards technology is an essential factor to consider before delving into trusting any specific technology. A person's propensity to trust in technology can be directly affected by several elements, one of which being their general background and demographic group. Other influences can include previous occurrences as well as knowledge and understanding of the technology in question, among others (Jessup et al., 2019).

When exploring the trust in financial systems and services based on an online technology or not, it is important to study the characteristics of trust involved. Mayer et al.'s (1995) research on trust, the attributes of it and how trustworthiness of a product or service is fostered in people breaks down trust into three qualities: ability, benevolence and integrity. These are three constructs make the backbone of any action involving a form of trust from one or more parties. However, when considering finances, previous research has indicated the presence a fourth construct, namely transparency (Ennew and Sekhon, 2007). Transparency is a fundamental component of trust in all financial proceedings as the knowledge and clarity of the movement and actions involving finances is of essence (Ennew and Sekhon, 2007 and Esterik-Plasmeijer & Raaij, 2017).

Since the emergence of Blockchain over the past decade, its functionalities and use cases have expanded exponentially. Blockchain technology was originally introduced by Satoshi Nakamoto in 2008, with the aim of creating a digital currency, Bitcoin, that enables users to take part in transactions without the involvement of a trusted third party, such as a bank. Over the years, this technology has disrupted the global financial industry in almost every form. A possible reason for this is that blockchain technology essentially takes out the factor of 'trust' within a transaction, because it is completely transparent and can be tracked fully (Tabora, 2018). Involvement of blockchain can aid people in having an increased level of trust in transactions within all digitally recorded business transactions, as blockchain is resistant to any form of alterations or modifications (Iansiti and Lakhani, 2017). As the underlying technology behind Bitcoin, it is essential that blockchain is functional, reliable and secure. Likewise, as the financial system based on this immutable technology, Bitcoin must also be of a dependable and transparent nature, in order for users to utilize it for financial or any other form of transactions.

1.1. Practical Relevance

As Blockchain technology is increasingly being applied across a multitude of industries, the probability of coming across it at some point in the near future as a user is very likely. Thus, businesses in all industries require knowledge on their customers stance and attitude towards Blockchain technology, in order to create their products in a user-oriented manner. By understanding how users trust technology in general and the difference in relevance between the different attributes of trust involved, businesses can create a product that people will use and can trust with their personal information and sensitive data. By focusing on trust in the financial application of blockchain and Bitcoin, which is an important part of life to many people, a critical overview of trust within blockchain as the underlying technology has to be studied.

Businesses, and in the future perhaps also governmental institutions will need to know what the most relevant and pressing aspects are to consumers and users when trusting these new and developing technologies.

1.2. Aim of Research

The purpose of this thesis is to explore the aspects of trust involved in trusting Blockchain as a financial service as well as Bitcoin as a financial system. The main research question to guide the thesis was formulated as follows:

> ***RQ:*** *How does trust in Bitcoin relate to trust in the underlying Blockchain technology within financial systems and what factors lead to this relationship?*

Essential questions that also have to be considered in the research when answering the main questions are:

a. To what extent does people's propensity to trust in technology in general affect their trust in a specific technology (i.e. Blockchain and Bitcoin)?
b. Does the extent of trust differ between the different attributes of trust ((i) competence & ability, (ii) integrity & consistency, (iii) benevolence, concern & shared values and (iv) communications and transparency)?
c. To what extent does trust in Blockchain, as the underlying technology, affect Bitcoin as a financial system?

A rigorous literature review and quantitative research will be performed in order to answer these questions. Furthermore, it is also an to aim to find out whether of the attributes of trust have a higher influence when considering trusting Blockchain and Bitcoin, as well as the reason behind this. The data will be collected using a quantitative research approach and the analysis will focus on hypothesis testing. Finally, by combining the findings of the quantitative data with the literature review, a deeper analysis will be performed in order to answer the main research question.

2. Literature Review

In this chapter several relevant factors will be presented from the literature review. The research topic is technological trust within the decentralised system of Blockchain as a financial transaction application for the cryptocurrency Bitcoin. At first, a brief overview of trust in general will be presented, after which the attributes of trust in technology will be discussed in detail. Subsequently, the construct trust in Bitcoin will be examined with respect to the underlying technology of Blockchain, after which the topic of blockchain technology as a whole will be discussed, including its potential uses and future impacts and then its application specifically as a means of financial service. Finally, the cryptocurrency Bitcoin will be reviewed, and its applications will be discussed.

2.1. Trust

In this section of the thesis an overview of trust will be presented in order to gather information on people's general propensity to trust, the attributes of trust required for financial services and trust in technology. Additionally, these trust constructs will be adapted and translated into a form that is relevant to Bitcoin and Blockchain technology. In general, trust is considered to be "the willingness of a party to be vulnerable to the actions of another based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor and control that other party" (Mayer et al., 1995, p.712). In this definition the authors of the thesis stated the trustor as the party that gives their trust, whereas the party being granted the trust is the trustee (Mayer et al., 1995). The trustee's trustworthiness is dependent on their attributes and actions, which can be perceived subjectively by different trustors (Sadhya et al., 2019). Therefore, formation of trust occurs when the trustors perception of trustworthiness aligns trustee's attributes and actions.

2.1.1. Propensity to Trust and Factors of Perceived Trustworthiness

In order to understand the formation of trust between two or more parties, that eventually leads to an action, it is important to understand the precise characteristics of the development of trust itself (Alarcon et al., 2017).

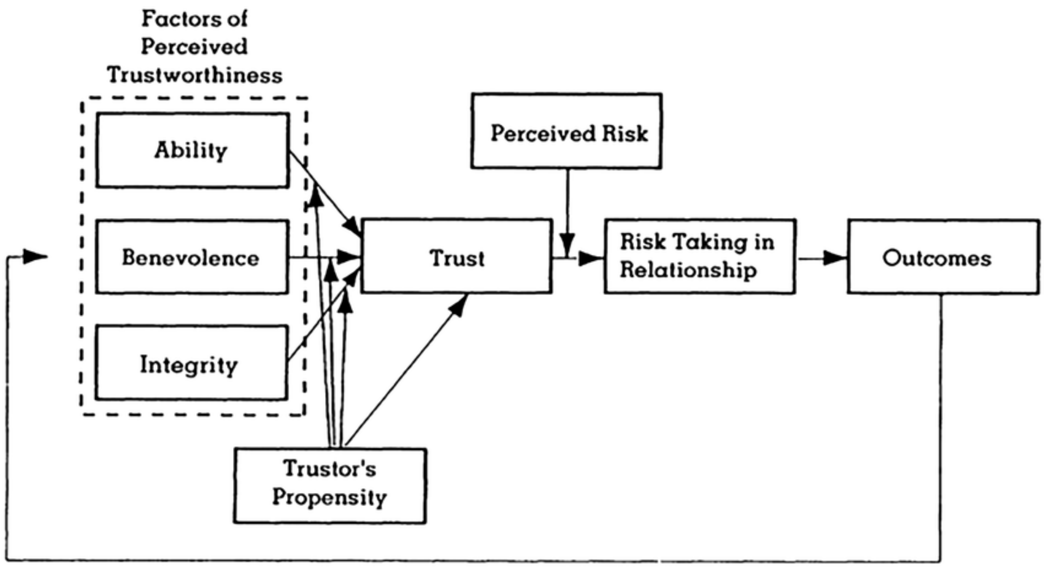

Figure 1. *Model of Trust Development (Mayer et al., 1995).*

As depicted in the Mayer et al. (1995) model, these characteristics are the trustors' factors of perceived trustworthiness and the trustor's general inclination to trust another entity, which can differ from person to person. As a personal trait, the propensity to trust is usually developed throughout a person's lifetime and can depend on their former experience in outcomes when the element of trust was involved (Berneth and Walker, 2009). These can also depend on several demographic factors of the trustor, such as age, education, socioeconomic sector, employment, origin, gender among others. Findings related to propensity to trust by Rotter (1980), point out that the likelihood of people to act dishonourably or in an untrustworthy manner is lower in people in people who have a higher propensity to trust, than those who have a low propensity to. Moreover, people who have a higher propensity to trust are also more likely to be trustworthy in a given situation (Rotter, 1980). This is underlined by Colquitt et al.'s (2007) study, which found a positive correlation between trust propensity and citizenship behaviours. This further suggests that propensity to trust is a critical factor leading towards an action involving trust between two entities. Mayer et al.'s (1995) model also shows that there are three factors involved in the perception of a trustor's determination of trustworthiness in a trustee; ability, benevolence and integrity. These are the three key elements when dissecting the perception of trustworthiness. Where ability is defined as "the group of skills, competencies and characteristics that enable a party to have influence within some specific domain" (Mayer et al., 1995, p.717).

A person or even a technological system or organisation may have higher competencies and skills within their field in comparison to other possibly competing entities (Svare et al., 2019). For example, if a person wants a specific financial service to be performed, they will look for a system or institution that has a good reputation and high competency level in this field to fit the persons specific needs. Mayer et al. (1995), describe benevolence as "the extent to which a trustee is believed to want to do good to the trustor, aside from an egoistic profit motive" (p. 118). This is a critical factor within the determinants of trust as the trustee's true motives are being evaluated by the trustor. In this case the trustee has to show that their intentions are not only for their own benefit, but they are also looking out for the welfare and best interests of the trustor (Esterik-Plasmeijer and Raaij, 2017). An example to illustrate this would be a bank analysing their customers financial situation and suggesting a service or plan that would be most beneficial to the customers situation, even if it is not the most optimal and economically rewarding transaction for the bank itself. Integrity is defined by Mayer et al. (1995) as "the trustors perception that the trustee adheres to a set of principles that the trustor finds acceptable" as well as "the consistency of the party's past actions, credible communications about trustee from other parties, belief that the trustee has a strong sense of justice, and the extent to which the party's actions are congruent with his or her words" (1995, p. 719-720). In this case the trustor has to be positive about the trustee's general code of morality and honesty. Using a banking institution as an example, it is important that the bank does not take part in corruption, bribery, nepotism in addition to always adhering to professional as well as governmental regulations (Esterik-Plasmeijer and Raaij, 2017). However, Esterik-Plasmeijer and Raaij (2017) argue that in the situation of institutional trust the customer is more inclined to care about the company's benevolence, as high levels of integrity may sometimes be viewed as too bureaucratic, which could lead to delayed processes.

Still, the perception of ability, benevolence and integrity, as also seen in the Mayer et al. (1995) model, also depends on the trustor's general propensity to trust. The general perception of trustworthiness of a trustor is a result of a combination of these factors and even though these factors are essentially inherent factual information on the trustee, the trustor may have their own perception them at the beginning of a joined affiliation (Alarcon et al., 2017). Consequently, it is important to note that the more information and knowledge the trustor gains on the trustee, the more his perceptions of the trustees' trustworthiness may change (Alarcon et al., 2017). This is on account of the three factors of trustworthiness being dependent on the trustee's actions, which the trustee will see as the relationship develops (Alarcon et al., 2017). Hence, once the trustor sees that the trustee has his best interests at heart the perception of benevolence may increase and thus the trustor may put a higher level of trust into the trustee. Furthermore, a result of a longer relationship between them, the trustor will depend more on the actions of the trustee rather than his personal disposition to trust (Jones and Shah, 2016).

2.1.2. Trust in Financial Systems

Throughout history trust has always been an irreplaceable factor within any form of financial transaction. Particularly in the financial sector, trust is an essential factor in any transaction as when people's finances are concerned, in extension so are their livelihoods. There has to be a level of trust between all parties involved in a transaction, may it involve goods, money, intelligence or any other form that holds value in trade (Möhlmann & Geissinger, 2018). Financial systems are globally considered to be the intermediaries between lenders, investors and borrowers. These can be banks, insurance companies, stock exchanges and a multitude of other companies facilitating the exchange of funds between people and organisations (Ergungor, 2004). Throughout history trust has evolutionarily developed from social trust to institutional trust, which is where we are currently (Yahya, 2018). In his 2018 keynote address on Web 3.0 in Los Angeles, Yahya also mentions that of these are somewhat based on human trust, as even within institutions most of the proceedings and decisions go through a human element at a given time. At present institutions are trusted as a result of their three titular factors of trustworthiness: integrity, competence and benevolence.

Previous research argues, however, that these dimensions can be expanded. Ennew and Sekhon (2007) developed a trust index in financial service institutions, finding that trust in financial services is built upon benevolence, integrity and ability as well as two additional factors, namely shared values (similar values between the customer and the institution) and communication, meaning their level of transparency. These factors are further supported by more recent research exploring the differences between the factors determining trust and trust itself, finding trustworthiness as a characteristic of trust (Sekhon et al., 2014). Schumann et al. (2010), however, characterises only one other factor of trustworthiness in addition to ability, benevolence and integrity: predictability. Where predictability is defined by a combination of the institution's level of stability, continuity and lack of sudden changes (Schumann et al., 2010). In further research, Hurley et al. (2014) propose an amalgamation of these, by categorising trustworthiness into six determinants: Similarities (shared values), interest alignment, capability, benevolent intentions, predictability and integrity as well as transparency and communication.

Thus, research confirms that that trust in financial institutions and their services can be determined by several factors, but the three main factors of ability, benevolence and integrity are omnipresent when the determination of trustworthiness is in question. A further important factor exhibited by this research is the openness in communication, which includes the transparency of information that the institution displays to the trustor. In their research Esterik-Pleismeijer and Raaij (2017) confirm this combination of perceived trustworthiness factors as the defining ones when considering trust in systems in banking and financial systems.

2.1.3. Technology Trust

In the past several years the ways in which transactional methods and business agreements occur have changed drastically, as technological advances in all fields are changing the most basic processes in our society. This, in turn asks for a change in many mechanisms that people have been used to for decades. As these mechanisms and processes have been part of our daily lives for so long, we have naturally developed trust in how they work, their processes and also their outcomes (Pennington, Wilcox and Grover, 2003). Now, as a result of these fast paced and radical changes there has to be a change in the way of particular mindsets and ways of thinking as well (Collins, 2018). Over the past decade, with technological advancements not only in industrial and back-end sectors, but also in the direct consumer area, customers have become far more knowledgeable about how specific 'behind the scenes' processes work (Su, 2018). They are exceedingly more informed about everything, as information is readily available to them on their smartphones, smart tablets and other devices. Subsequently consumers are more cautious as a result of their increased awareness in what businesses do with the information they provide and how it is then processed (Su, 2018).

The Facebook-Cambridge Analytica data scandal of 2018, which revealed the breach of millions of people's personal data without consent for political advertising, did not help soothe customers' trust in technology companies. In fact, this disclosure was considered to be a breaking point in the general public's realization and understanding of the use of their personal data by businesses (Bownes 2018, cited in Griggs, 2018). Trust levels in Facebook decreased substantially following the scandal. According to a user survey conducted by the Ponemon Institute that asks respondents whether they believe if Facebook is 'committed to protecting the privacy of their personal information' the number of respondents that answered with positive feedback decreased by a considerable 66% within the first week after the data breach (Weisbaum, 2018).

Resultantly, businesses in all industries have to adapt to this new wave of 'informed customers' and create and develop their platforms in a way that inspires trust in consumers, so that they use their services (Collins, 2018). Moreover, due to the advancement of technologies and digital transformation, to which all businesses must adapt and adhere to at some point, they have to take their customers along with them and ensure and establish trust between their consumers and the services (Collins, 2018). The advancement of technology will naturally be bound to processes becoming digitalised and transformed and businesses as well as consumers will inevitably have to adapt to this. The establishment and further growth of trust between them will progress in fruitful continuation of transactions and economic advancements (Möhlmann & Geissinger, 2018). In the process of this digital transformation institutions such as banks, offering financial services to the people will inexorably also have to adapt and evolve.

2.1.4. Constructs of Trust in Technology

Research on aspects of trust within technology, in comparison to other fields is still a largely unexplored area (Marella et al., 2019). When trusting technology, the morality factor in technology can principally be excluded, as one needs to rely on a programmed device or software which predominantly works based on mathematical algorithms (Marella et al., 2019). This can be particularly applied to technologies that have to ability to work autonomously, such as Blockchain or many technologies within the Internet of Things field (Marella et al., 2019), as human intervention is excluded from the process. Many self-driving vehicles and other machines based on artificial intelligence are also among these. When considering these technologies, the user is left to trust a machine or computer program to help them. Examples can range from trusting a calculator to give the correct answer to a complex equation to a smart car informing the driver when to refill the oil or even a smartphone automatically connecting to a free Wi-Fi network when in range, to save its user money. Subsequently, the question of what makes users trust this remains to be answered (Marella et al., 2019).

As previously defined, trust is a precedent of trustworthiness and propensity to trust, when considering interpersonal trust (Mayer et al., 1995). Propensity to trust will remain always remain as one of the factors playing into a trust action, as this depends on trustors individually. McNight et al. (2011) suggest that trust in technology is a result of three elements: propensity to trust in technology in general, institution-based trust in technology and trust within a particular technology. In relation to technology, McNight et al. (2011) indicate that it is a user's personal disposition to depend on technology throughout any situation and any technology.

Institution based trust in technology refers to the trust within a group of technologies (McNight et al., 2011). Within this element trust is split into two contexts; situational normality and structural assurance, wherein situational normality refers to a user's "belief that success is likely because the situation is normal or favourable" and structural assurance denotes the belief in success of a user is because "contextual conditions like guarantees and regulations are in place" (McNight et al., 1998, Table II, entry 4, p. 7-8). This means that a user trusts the company of the technology item to have installed the product with all the expected functionalities and for these to work in the expected manner.

The final element, trust in a specific technology, is a partial antecedent of the user's belief in structural assurance of the given technology. This is the element wherein the user's actual belief in trust in a technology is defined. It can conversely be argued, as done so by Friedman et al. (2000), that "people trust people, not technology" (p.36). However, technology is becoming increasingly more human-like in its interface as well as user-friendliness, which can be argued to be a precedent to ensure trust within its users (Marella et al., 2019; Lankton et al., 2014). Henceforth, it can be argued that labelling characteristic of technologies with human-like qualities, the trust within the specific technology can be determined (Lankton et al., 2014). If the three fundamental constructs of trust in humans are ability, integrity and benevolence, then interpreting them into technological characteristics could be: functionality, reliability and helpfulness (McKnight et al., 2011; Lankton et al., 2015). These are also the three constructs presented by McNight et al. (2011) as the ones making up the trusting belief in a specific technology. These translations of trust in technological characteristics into their human counterparts is imperative to gain understanding, because they reveal the significance of each construct of trust within the technology (Marella et al., 2019). To illustrate this further, McNight, Carter and Thatcher (2011) presented the example of a user determining the security against attacks to a financial system, wherein the user compares the safety of his money in the bank to it being within Bitcoin and backed by blockchain technology. Thus, if the user believes that due to the immutable and decentralized structure, blockchain is the more secure option, it adds to blockchains trustworthiness within the user's belief (McNight, Carter & Thatcher, 2011).

Constructs	Human-Like Comparison	Description	Operations
Functionality	Ability	Functions needed to accomplish the expected tasks	Performs a function for the user, provides system features the user needs to do a task, provides the user with the appropriate functionality
Reliability	Integrity	Continually operating properly or in a flawless manner	Performs functions reliably, does what the function says it will do, gives accurate and unbiased facts and information, calculates correctly, does not crash
Helpfulness	Benevolence	Providing adequate and responsive aid	Provides help, understands and caters to needs, does not cause harm, is responsive to user needs and requests

Table 1. *Constructs of Trust in Technology (Lankton et al. 2015)*

Table 1 shows the three human-like comparisons technology has to offer in order to determine a user's trust within it: functionality, reliability and helpfulness (Lankton et al., 2015). A human's ability or skill in a specific area and the functionality of a technology is quite comparable, as Marella et al. (2019) uses the example of translating a phrase; if a user trusts that an interpreter has the appropriate skill level to translate a phrase the same way they could trust a translating software, e.g. Google translate, to have the functionality to translate the same phrase. Thus, the trustor expects the software to have the appropriate functionalities to complete the task and to do these in the way expected by the user. Reliability refers to the characteristic that allows the technology to perform a function in the manner it says it will and does so consistently, whereas a trustee's integrity is defined by their principles aligning with those of the trustor (Merella et al., 2019). Using the same example one can say that the integrity of the interpreter to translate the phrase in a timeframe acceptable to trustor proves their integrity the same way Google Translate can be relied upon to have all the functions to perform the translation correctly and consistently at all times (Marella et al., 2019; Lankton et al., 2015). Comparing the benevolence of a human to the helpfulness of technology could be compared by the interpreter correcting the user's phrase if it is inappropriate in the translated language and Google Translate suggesting the correct word automatically if the user misspelled it by accident.

2.2. Blockchain as a Decentralised Service

In this chapter the background and history of blockchain technology will explained followed by the underlying technology and its application within financial systems and beyond.

2.2.1. Background and History of Blockchain

Blockchain technology has been a buzzword in the past decade. Since its invention in 2008 by 'Satoshi Nakamoto', a pseudonym used by either an individual or a group of people, blockchain utilisation in various forms has skyrocketed over the past years and has disrupted a plethora of industries (Werbach, 2018). Blockchain was already being considered as a game changer in many aspects in 2015, according to a study by the World Economic Forum, and has a significant future impact within society even having the potential of "10% of global gross domestic product being stored on blockchain" by the year 2025 (Chung and Kim, 2016, p.1314). Moreover, with this prediction of deep shift, the 2015 WEF study also considers blockchain to be a significant part of the fourth industrial revolution. As blockchain has the potential to create such a large scale impact on so many industries in the near and far future, governments are also considering its importance and calculating it into their long term strategies, as the UK government states "we have seen open data revolutionize the citizens' relationship with the state, so may the visibility in these technologies reform our financial markets, supply chains, consumer and business-to-business services, and publicly-held registers" (Walport, 2016).

Originally the primary usage of blockchain, and therefore potentially the reason of its creation by Nakamoto, was to enable the Bitcoin cryptocurrency and create a public transaction ledger for it (Marella et al., 2019). The reason for this was to create a technology that facilitated transactions without the need of a centralised authority, such as a bank or governing body (Marella et al., 2019). In his paper, Nakamoto describes the problem meant to be solved, is effectively eliminating the need for a third party, which the parties on all transaction sides must trust (Nakamoto, 2008).

This will be elaborated upon in a later section of this chapter when discussing Bitcoin. Blockchain, by definition is an "open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way" (Iansiti and Lakhani, 2017). It is in essence a decentralised data structure that allows for transactions to happen in an open and transparent manner for all parties involved as well as the public when the blockchain is public and permissionless, often in a peer-to-peer network (Swan, 2015).

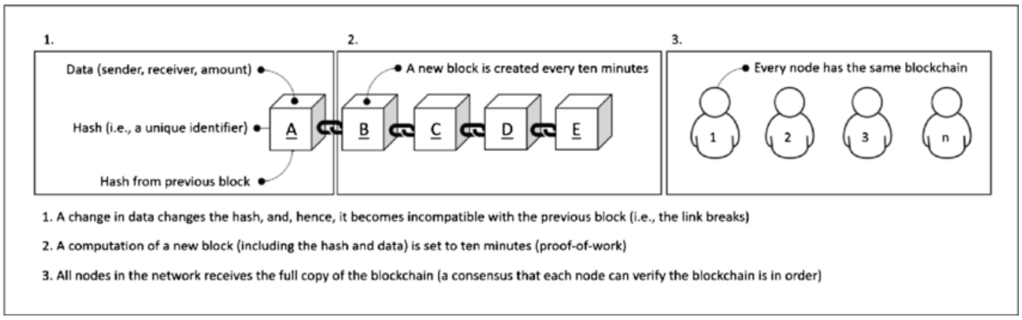

Figure 2. *A simplified representation of a blockchain data structure (Narayanan et al., 2016).*

Due to its inherent data structure, blockchain is generally considered immutable and therefore a very reliable and secure method for transactions of any kind (Underwood, 2016). Figure 1 shows a simplified representation of the blockchain data structure (Narayanan et al., 2016). In their publication Narayanan et. al (2016) define blockchain as a decentralised and distributed database, spread across a complex network of computing machines called nodes. In this distributed network all nodes have access to the data within all the blocks of the blockchain (Marella et al., 2019). Each block within the blockchain can be differentiated as they all have a unique identification called a hash, which is characterized by the contents of the current block as well as the hashed header from the previous block (Marella et al., 2019). This header is entered automatically into the following block on the chain, which happens approximately every ten minutes in the Bitcoin blockchain, and so the chain continues (Marella et al., 2019).

According to Nakamoto (2008) the variable making this a highly trusted network is its timestamp server. The server timestamps each hash and distributes this information across all nodes, thus verifying the existence of a transaction at a specific point in time (Nakamoto, 2008). The timestamp of the current hash integrates the timestamp of the previous one, thus chaining together the blocks in a unique chronological order which is strengthened by each additional block being added to the network (Nakamoto, 2008). Marella et al. (2019) state that the hash value of each block will be altered when "backdating, revising, deleting or tampering with any of the blocks", which would cause a disruption between the blocks, and thus the entire blockchain. This quality is what makes the blockchain such a trusted technology, as when modifying data within a block, the chain is disrupted and all the hashes in the blocks following the modified one would have to be computed accordingly, all before a new block can even be added to the chain (Marella et al. 2019). In his original white paper Nakamoto (2008) states this as one of the primary incentives to fend off any potential cybercriminals, as the process of altering data in the blocks for personal gain takes infinitely more effort than it is worth.

Historically, even though Bitcoin was the original reason of the creation of Blockchain Technology by Nakamoto, following its release, numerous entities invested into its development and functionalities, and over time discovered that there were limitations to its programmability (Marr, 2018). According to Tapscott and Tapscott (2016), this was the reason for the proposal of a new blockchain network in 2013, which would be able to utilise the blockchain for several other functionalities such as contracts and loans. This proposal was made by a researcher and programmer in the cryptocurrency field, Vitalik Buterin (Tapscott and Tapscott, 2016). Buterin and his co-founder Gavin Woods presented the Ethereum Blockchain that would soon expand the range of applications within the blockchain and expand its reach to a plethora of fields, due to its ability to secure transactions other than ones solely for the sake of a digital cash payment (Marr, 2018). However, Nakamoto (as cited in Alberti et al., 2020, p.33) also stated that the first blockchain design was merely a starting point for a potential revolution "*the design [of blockchain] supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multiparty signatures, etc. If Bitcoin catches on in a big way, these are things that we'll want to explore in the future, but they all had to be designed in the beginning to make sure they would be possible later*".

2.2.2 Applications of Blockchain

As mentioned, blockchain technology has a disruptive effect on numerous industries and this trend will most likely continue in the future. The concept of blockchain technology is already a common term in the finance industry, due to the very well-known origin of blockchain, the cryptocurrency Bitcoin (Nofer et al., 2017). Nevertheless, with the emergence of Ethereum, blockchain technology is already being used over an array of industries, spanning from legal applications through smart contracts all the way to data storage, where users may store documents without the involvement of a third party over a distributed cloud storage platform within the decentralized peer-to-peer network (Nofer et al., 2017). According to Swan (2015) the applications of blockchain can be divided into three pillars: Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0. These pillars also coincide with Ethereum's development into the Ethereum 2.0 phase which, amongst other things, aims to improve security measures and allow for "transactions and validations to pe processed from a typical laptop" (Github, 2020).

The first pillar, Blockchain 1.0, mainly concerns currency and cash in forms of cryptocurrency, including the largely known cryptocurrency Bitcoin (Swan, 2015). Thus, one can say that Blockchain 1.0 mainly involves the simpler financial transactions, such as online payments and transfers. Effectively, as Blockchain 1.0 merely concerns these aspects it can be seen as the original backbone behind what Nakamoto wanted to achieve with Bitcoin, a secure method to transfer digital currency without the need for a centralized third party which has to be trusted (Swan, 2015). However, as Blockchain 2.0 already delves a little further into the complexities of the financial markets and the economic systems of the world. Swan, 2015 explains Blockchain 2.0 as "the entire slate of the economic, market and financial applications using the blockchain that are more extensive than simple cash transactions: stocks, bonds futures, loans, mortgages, titles, smart property and smart contracts". Hence, blockchain 2.0 still largely concerns finances and is mainly applied within things concerning money and its flow between individuals or groups in some form or another.

The further usage and development of applying blockchain technology in fields outside of finance is generally considered within the term Blockchain 3.0 (Swan, 2015). Here blockchain could be applied to a vast amount of industries, including education, the Internet of Things, the medical and health industry, scientific research, governments and even within music, art and culture (Swan, 2015). Large scale potential also lies within the energy sector (Andoni et al., 2019). The energy industry, specifically the renewable energy industry, has been developing increasingly, as the nature of it relies a lot on flexibility, causing a lot of flexibility measures having to be taken in order to gain access to an efficient and effective manner of generating energy (Andoni et al., 2019). In their research Andoni et al. (2019) also elaborate on this by stating that integration of energy storage and demand-response services as well as fast acting supply are measures having to be taken to support the flexibility needed to support this system. Furthermore, the implementation of smart meters in buildings in several countries shows that distributed energy resources and renewables are on the verge of entering the digital era (Andoni et al., 2019 and Vos & Sawin, 2012).

2.2.3. Blockchain in Financial Applications

As previously discussed, the highest extent of blockchain technology so far lies within its application for financial services. This can be mainly attributed to Nakamoto's original aim to create a network allowing for the elimination of the involvement of a centralized third party, such as a bank, within a transaction between two or more parties (Swan, 2015). Within the finance market, blockchain has found a home in many fields, and its market share is continuing to inflate. A recent Markets and Markets study forecasts the market size to lie at an impressive 39.7 billion USD by 2025 from its current 3.0 billion USD, at a CAGR (Compound Annual Growth Rate) of 67.3% between these years (Markets and Markets, 2020). Blockchain utilisation within the finance world ranges from simple payments over remittances, payment gateways and trade finance to the improvement of record keeping among numerous others (Swan, 2015).

2.2.4. Blockchain Applications and the Involvement of Trust

Applying blockchain technology poses numerous potentials for many industries. Nofer (2017) suggests that most systems in which an intermediary is relied upon as the party establishing 'trust' within a transaction will be the ones that are most likely to be phased out due to 'trustless systems'. The notion that blockchain can basically apply a layer of trust that creates a system which can eliminate trust in the classic context, is a fundamental misinterpretation (Glaser, 2017). Nevertheless, in 2010 there was a major breach in the Bitcoin blockchain network due to a loophole in the programming which allowed for the generation of an infinite number of coins (Sedgewick, 2019). The hacker managed to generate a transaction involving 184 billion coins, however, due to the constant public recording of all of transactions it was reversed as soon as it was discovered (Sedgewick, 2019). Following this there have only been breaches of a lesser extent, making this the largest incident in Bitcoins history. Furthermore, in a recent keynote about trusting bitcoin and the blockchain at the Hyperledger Global Forum, Bruce Schneier of Harvard University stated that simply the nature of trust has changed, the trust from inter human and institutional trust is shifting towards trust in technology, which may be difficult for many. The lack of legal or governmental regulations is one of the main concerns people have, when considering trusting in blockchain (Werbach, 2018). However, there are arguments suggesting that due to the fast-paced advancements in the technological and digital realm people will want to be involved due to the sheer facilitation and economically beneficial character that the blockchain could offer (Atzori, 2015). This also shows that there may be a natural timeline for governments, our societies and simple systems we know now to be restructured in the future (Nofer et al. 2017).

2.3. Bitcoin as a Financial System

This section of the thesis will look into the background and history of Bitcoin and explain the underlying technology behind a Bitcoin transaction, based on blockchain technology. Following this, the advantages and disadvantages of utilising Bitcoin as a financial system will be outlined.

2.3.1. Background of Bitcoin

Bitcoin was introduced in 2008 by Satoshi Nakamoto as a digital cryptocurrency system using a peer-to-peer network (Swan, 2015). It's main purpose, as stated by Nakamoto (2008) in his white paper is to remove the need of a trusted third party in a financial transaction, as well as preventing the possibility of double spending. It is based upon the secure and immutable technology of blockchain.

2.3.2. Underlying Technology behind a Bitcoin Transaction

For a transaction to occur in the Bitcoin system three key technological elements are required: cryptocurrency wallets, blockchain and exchange platforms (Marella et al., 2019). In order for a transaction to be initiated a wallet, on either a private computer or a mobile, is needed in addition to a public address and a private key. Personal information does not have to be disclosed within any process of a transaction (Sas and Khairuddin, 2017). For further privacy and anonymity Nakamoto (2008) advises to use a new address for each transaction. When a transaction occurs, the user's private key is required to prove ownership of the Bitcoins he wishes to transfer, in order to show that he actually owns these bitcoins and is able to commit to a transaction with another user (Sadhya et al., 2018). The Bitcoin system does not actually contain "coins" within it, but rather just the verification and validity of transactions. It is the private key, contained in the wallet, that the user requires in order to prove that he is the owner of his bitcoins and thus, the security of this is the responsibility of the user (Sadhya et al., 2018). So, the bitcoin system, by aid of the blockchain technology structure, tracks the constant changes of ownership of the bitcoins involved in transactions in the form of inputs and outputs (Zohar, 2015).

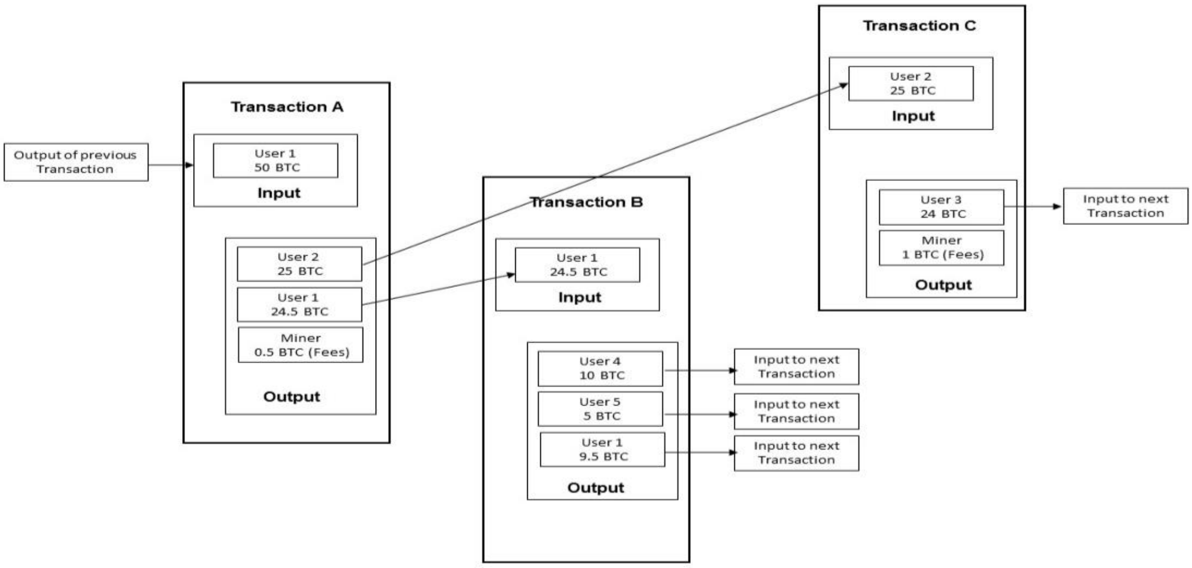

Figure 3. *Three bitcoin transactions comprised of inputs, outputs and miner fees (Sadyha et al., 2018, p.5).*

Another vital part of the bitcoin structure are the mining nodes, called miners. They are the ones creating the blocks in the system and checking the validity of the transaction within each block (Zohar, 2015). Miners consume a high level of computational power and energy resources for the process of creating the new blocks (Sadhya et al., 2018). The miners therefore receive a transactional fee for each transaction they include in the block (Sadhya et al., 2018). The miner receives a further reward by the system for each block being produced, which currently lies at 6.25

Bitcoins. Once a miner completes the creation of a block, this is broadcasted to the entire network of nodes and miners, who verify the validity within the created block so it can be added to the chain (Sadhya et al., 2018). Following this the network of miners will seek to create a new block, comprising of transactions waiting to be validated and processed by the network (Sadhya et al., 2018)

2.3.3. Advantages and Disadvantages of Bitcoin

Using Bitcoin comes with many benefits, nevertheless, even though it is considered a very reliable and stable technology it also comes with several disadvantages that go hand in hand with the aspects making it so widespread (Georgios, 2020). As a cryptocurrency, Bitcoins primary application is in electronic cash payments. The primary benefit for this is that a trusted third party, such as a bank, is not required to process the transaction (Galar et al., 2020). A further advantage of using Bitcoin for cash transactions is the pseudonymity and privacy it offers to its users with the element of the private key that does not carry any identifying information and the usage of new addresses for each transaction (Singh and Chahal, 2020). Likewise benefits of Bitcoin are its durability, due to it being a non-physical entity and its ability to work at all times at a constant rate of about 10 minutes per block with transactions happening between 10 to 30 minutes, as no central authority is involved that has opening hours or additional time consuming hindrances (Singh and Chahal, 2020).

On the other hand, Chiu and Koeppl (2017) argue that this time efficient capability of Bitcoin allows for a minimal potential to allow for double spending even with the Bitcoins proof-of-work system. The fact that it is a globally usable currency that isn't tied to any government or nation, which would add commission fees or exchange rates when transferring money between different national currencies is also an advantage of using Bitcoin (Singh and Chahal, 2020). Nevertheless, even though it is an electronic currency meant for payments, currently most Bitcoins in circulation are being used as an investment opportunity (Georgios, 2020). Investing in Bitcoin as a cryptocurrency also has its advantages and disadvantages. Due to its unregulated nature the fluctuations of its worth can sometimes unpredictable in forecasts (Georgios, 2020). A recent statistic published on Statista (2020) has found that the exchange rate from U.S. dollars to Bitcoin has decreased to just over 9,100$ in June 2020, compared to last years' peak at just over 10,900$.That is not to say however that it hasn't been higher before, in 2017 Bitcoins exchange rate was at almost 14,000$, however with the introduction and rise of the Ether cryptocurrency it decreased (Statista, 2020). This shows that when investing in Bitcoin, or any other cryptocurrency for that matter, there is a certain amount of unpredictability that has to be considered. Using Bitcoin also has numerous disadvantages, for example if a transaction is made, it is near to impossible to reverse it (Singh and Chahal, 2020). This can become a problem when accidentally transferring too much Bitcoin in a transaction, there is no way of getting it back unless the receiver of the superfluous Bitcoin initiates a new transaction to return it (Singh and Chahal, 2020).

3. Methodology

In order to conduct a rigorous research project a clear research design is a core part of the study (Cooper and Schindler, 2006). The methodology of the research supports and guides the researcher throughout the entirety of the project, so it is critical to develop a well-formulated design in order to create clear guidelines for the collection of data, which will subsequently be analysed and interpreted (Creswell, 2009). This project investigates the trust or mistrust people have within the digital world surrounding the sharing economy and how a possible application of blockchain technology could have an effect on this.

3.1. Quantitative Research Design

The Saunders Research Onion describes the process of a research design development by way of the layers in which the study is built up (Saunders et al., 2007). The onion model is considered an advantageous approach to developing a productive research design as it "creates a series of stages under which the different methods of data collection can be understood and illustrates the steps by which a methodological study can be described" (Emmanuel, 2019, para. 4). Furthermore, it aids the researcher in staying consequent throughout the study by following the onion.

In order to investigate and explain this research project I decided to pursue a quantitative research method, by way of a survey. A combination of positivist and pragmatic world views will be consistent throughout all phases of the study in order to apply empirical observations and measurements as well as real world practices that are problem oriented (Creswell, 2009). The quantitative approach has been determined to be more effective over a qualitative one in this particular study.

3.2. Data Collection and Analysis

A cross-sectional survey will be the primary source of data collection throughout this study. As Babbie (1990) states, survey research studies the trends, attitudes and opinions of the participants by means of numerical descriptions and looks to generalize from a sample to a population. Using a questionnaire I ask participants about various aspects of their trust, or mistrust, in technology in general to determine their propensity to trust. Additionally, questions aimed to determine the subjects trust in decentralised systems as well as trust in Bitcoin will be developed. These questions will be built upon a format looking to determine which attributes of trust are most relevant to the subjects. In the case of this research project an online survey will be used by means of 'Google Forms', in order to allow for a cost-effective data collection method, that still produces a large sample size in a short period of time (Nayak, 2019). Furthermore, as Nayak (2019) argues, online questionnaires also come with the advantage of enabling the participants to do the survey at a time of their choosing, without the possibility of them feeling the pressure of the researcher sitting opposite them, as well as possible personal responses to remain completely private. As sampling is an integral part of the data collection and validity, the participants will be selected by means of convenience. Benefits of convenience sampling include ease of participant recruitment, cost effectiveness and time efficiency (Bornstein, Jager and Putnick, 2013). However, as a non-probability sampling method, convenience sampling is exposed to selection bias in the study (Acharya et al., 2013). Other disadvantages that come with convenience sampling are that the sample cannot be generalised on to the population and is only valid on the sample itself (Bornstein, Jager and Putnick, 2013).

The online survey will be distributed and shared by means of e-mail through the university and workplace of the researcher, friends, acquaintances and various social media channels such as Instagram, Facebook and LinkedIn to acquire a sufficiently large sample size. As the data collection will occur at a particular period of time, the study is considered cross-sectional. The data collection process was done between

April and June of 2020. The survey contained close ended questions on a bipolar Likert scale as well as dichotomous questions concerning agreement or disagreement in a particular situation. In light of to Corona Virus Pandemic happening during the period in which the survey was conducted, an additional dichotomous question was added in consideration of this circumstance, asking whether or not the participants answers were affected by this. An occurrence of this magnitude could potentially have an effect on people's trust in the world financial market and all the systems within it, which Bitcoin is a part of. The result from this final question will be discussed briefly within the evaluations and limitations section (chapter 5) of the thesis.

The demographic section of the survey includes questions regarding gender, age, level of education, employment status and will also an open-ended question for the participants to fill in their country of citizenship. After completing the data collection process, the information will be imported into the Statistical Software SPSS to be cleaned and processed in order to be presented in a manner that is relevant to the research topic and describes the outcomes of the data clearly. The analyses of the data will be processed to show possible trends that may have come to light and these will be compared to each other as well as the theories presented in the literature review.

3.3. Theoretical Framework and Hypothesis Development

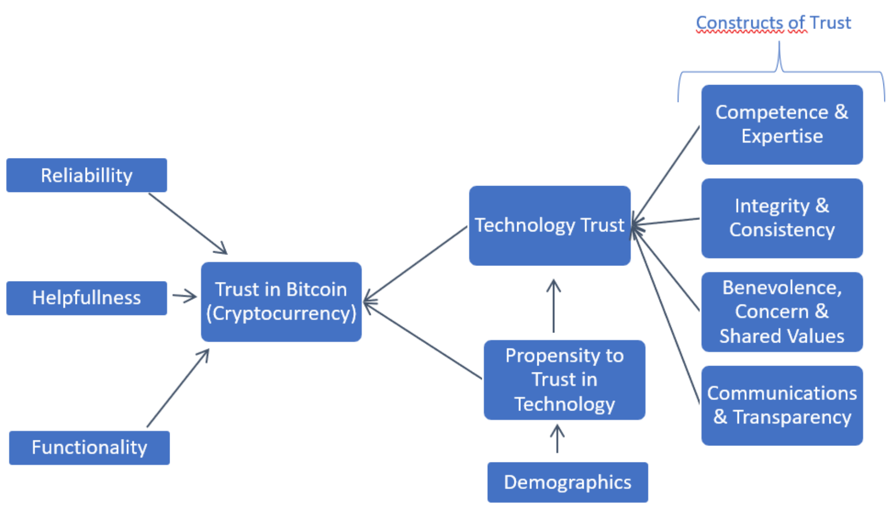

Figure 4: *Factors affecting trust in Bitcoin.*

The theoretical framework of this thesis represents the relationship of the factors that lead to trusting, or not trusting, Bitcoin. It is an adaptation of the model of trust developed by Mayer et al. (1995), as the three main attributes of trust; competence, integrity and benevolence are an integral part of determining whether or not technology trust exists, and van Raaij (2017). Additionally, a further attribute of trust was included, namely communications and transparency, as discussed in section 2.1. Previous research also deems this an essential part of the anatomy of trust when considering financial systems (Ennew and Sekhon, 2007; Esterik-Pleismaijer and Raaij, 2017). These four constructs are shown to be a part of the determination of trust in technology, along with propensity to trust in technology in general. The latter aspect has a direct effect on trusting technology as well as trust in Bitcoin in general, as if technology is not a trusted entity, then inherently Bitcoin can also not be trusted as it is a technological system. As shown in Figure 4, the demographics of the trustor can have an influence on propensity to trust technology. This since the trustors' backgrounds could have included different levels of and utilisations of technology, which could affect their disposition to trust when considering technology in general as well as a specific technology, such as Bitcoin. The left side of the model shows the reliability, helpfulness and functionality of Bitcoin, which are the adaptations of the qualities of technology into human-like characteristics (McKnight et al., 2011; Lankton et al., 2015). These are also based upon the qualities within blockchain technology, as that is the underlying technology behind Bitcoin.

Based on the theoretical framework, several hypotheses were formulated in order to thoroughly explore the research question: *How does trust in Bitcoin relate to trust in the underlying Blockchain technology within financial systems and what factors lead to this relationship?*

These are as follows:

H1: *There is a significant difference between the four attributes of trust (C/I/B/T) in trusting Blockchain as a financial service.*

H2: *There is a significant difference between the four attributes of trust (C/I/B/T) in trusting Bitcoin as a financial system.*

H3: *There is a significant difference in propensity to trust technology with respect to demographic groups (gender/ age/ employment status/ educational level/ nationality).*

H4: *There is a positive correlation between trusting Blockchain as a financial service with respect to propensity to trust technology.*

H5: *There is a positive correlation in trusting Bitcoin as a financial system with respect to propensity to trust technology.*

H6: *There is a positive correlation in trusting Bitcoin as a financial system with respect to trusting Blockchain as a financial service.*

The hypotheses *1 through 6* can be seen as a derivation from the theoretical framework and thus a build up to the core topic of this thesis, which is trust in Bitcoin in financial terms and how this trust is built up through several layers of trust within several entities.

3.4 Development of Survey

The survey consists of four main sections; (A) demographics, (B) propensity to trust technology, (C) trust in blockchain (as the underlying technology behind Bitcoin) and (D) trust in Bitcoin itself. In a final section (E) of the survey a few general questions on trust actions considering Bitcoin will be asked. In the main sections of the survey (B), (C) and (D), respondents will be asked to rate several statements on a 5-point Likert scale, where 1 is 'Strongly disagree' and 5 is 'Strongly agree'. The demographic questions of section (A) includes gender, age, level of education, status of employment and nationality. The questions in sections (B), (C) and (D) from the survey were adapted from previous research questions on trust, however, in order to suit the purpose of this research, they were slightly modified. The adaptations include slight linguistic changes as well as the complete removal of some questions when irrelevant towards the subject of Blockchain or Bitcoin. A further reason to adapt and modify existing surveys was to eliminate the need to re-validate them for their dependability (Tsang, Royse and Terkawi, 2017).

The questions in section (B), propensity to trust technology, were adapted from a study by Jessup et al. (2017), in which the focus was on determining trust in automated technology. The questions were developed and modified with the aim of finding out the participants general tendency to trust in technology. The aim of the questions in sections (C) and (D) are to determine the level of trust in Blockchain technology as a financial service and Bitcoin as a financial system respectively. In each of these two sections the questions are broken down into the four main constructs of trust deemed relevant from previous research and when developing the theoretical framework:

1) Competence and expertise
2) Integrity and consistency
3) Benevolence, concern and shared values
4) Communications and transparency

Parts 1, 2 and 3 are modified from Lin's (2011) survey on trust factors leading to mobile banking adoption. Statements in part 4 are a modification from Esterik-Pleismeijer and Raaij's (2017) research on trust within the banking system. An additional fifth part in sections (C) and (D) asks about the overall trust in blockchain and Bitcoin. Section (E) of the survey investigates whether or not a trust action would be taken in terms of Bitcoin (i.e. buying or investing in it, as well as whether or not Bitcoin has been owned or invested in before. In section (E) several answer formats exist for respondents, such as selecting *'Yes', 'No'* or *'Maybe'* as well as a short text answer depending on their answer to these.

In sections (I) and (II) below, one can find the structure of the survey including the modifications made from the original versions. The survey begins with an introductory part in order to present the respondents with a brief explanation of the topic, followed by section (A), in which they are asked to fill out their demographic information. In conclusion to the main sections (B), (C) and (D), respondents are asked a few questions aimed to determine any potential trust action they may take in relation to Bitcoin.

I) <u>Introductory paragraph:</u>

"My name is Hannah Nicole Griesmayr and I am currently a Bachelor student at Modul University Vienna. This survey is part of my Bachelor Thesis research. It is

about technology trust in decentralized financial systems such as Bitcoin and will take about 10 minutes to complete.

A decentralized system using blockchain is immutable, meaning that data and transactions cannot be changed after being recorded on the network. The data collected will be used solely for research purposes in an anonymized format.

Thank you for your participation!"

II) <u>Survey and modifications made:</u>

Section B: General Propensity to Trust

Original (Jessup et al., 2017)	**Modified for survey**
Generally, I trust technology	Generally, I trust technology
Technology helps me solve many problems	Technology helps me solve many problems
~~I think it's a good idea to rely on automated agents for help~~	~~I think it's a good idea to rely on technology help~~
~~I don't trust the information I get from technology~~	~~I don't trust the information I get from technology~~
Technology is reliable	Technology is reliable
I rely on technology	I rely on technology

Sections C.1 and D.1 - Trust attributes – competence and ability

Original (Lin, 2011)	**Modified for survey for Trust in Decentralised services as a financial service**	**Modified for survey for trust in Bitcoin as a financial system**
I think that mobile banking firms have the ability to understand my needs about managing my finances	I think that decentralised services are capable of providing a platform suitable for financial transactions	I think that Bitcoin has the potential to provide suitable payment services
I think that mobile banking firms have the expertise to understand my needs about managing my finances	I think that decentralised services are effective providing a platform suitable for financial transactions	I think Bitcoin is effective at providing payment services
I think that mobile banking firms have good knowledge about managing my finances	I think that the creators of decentralized services have good knowledge and expertise about information systems for financial purposes	I think that the creators of Bitcoin have good knowledge and expertise about finances

Sections C.2 and D.2: Trust attributes - integrity and consistency

Original (Lin, 2011)	Modified for survey for Trust in Decentralised services as a financial service	Modified for survey for trust in Bitcoin as a financial system
I think that mobile banking firms are honest	I think that decentralized services are honest as a platform for financial transactions	I think that Bitcoin is honest as a payment service
I think that mobile banking firms will keep their commitments	Decentralized services are reliable and stable as a platform for financial transactions	Bitcoin is reliable and stable as a payment service
	I would describe decentralized services as a secure platform for financial transactions	I would characterize Bitcoin as a secure payment service
I think that mobile banking firms will provide unbiased information about banking transactions	I think that decentralized services provide unbiased information as a platform for financial transactions	I think that Bitcoin provides unbiased information about financial transactions

Sections C.3 and D.3 – Trust attributes: benevolence, concern and shared values

Original (Lin, 2011)	Modified for survey for Trust in Decentralised services as a financial service	Modified for survey for trust in Bitcoin as a financial system
I think that mobile banking firms put my interest first	I think that the creators of decentralized services put my interests first	I think that the creators of Bitcoin put my interests first
I think that mobile banking firms are invested in my well-being and not just their own	I think that the creators of decentralized services are interested in my well-being and not just their own	I think that the creators of Bitcoin are interested in my well-being and not just their own
If I required help, I believe that mobile banking firms will do its best to help me	I think that I could rely on decentralized services to assist me in my financial transactions	~~I think that I could rely on Bitcoin to assist me in my financial transactions~~

Sections C.4 and D.4 – Trust attributes: communications and transparency

Original (Esterik-Pleismeijer and Raaij, 2017)	Modified for survey for Trust in Decentralised services as a financial service	Modified for survey for trust in Bitcoin as a financial system
Bank X is transparent	I think that decentralized services are transparent when providing a platform for financial purposes	I think that Bitcoin is transparent as a payment service
Bank X communicates clearly	As information systems, decentralized services are clear and understandable	As a payment service, Bitcoin is clear

Bank X is open about its procedures	Decentralized services are open about their transactional processes	Bitcoin is open about its transactional processes
Bank X is open about its costs and risks as a payment service	Decentralized services are open about their costs and risks as an information system	Bitcoin open about its costs and risks as a payment service

3.5 Ethical Considerations

It is important, when conducting any sort of research or experiment to consider ethical implications. The ethical implications of conducting a primary quantitative research project are in their foundation the same as in a qualitative one. As research in any form involves collecting information from participants about them, it is important to protect their rights and follow the code of ethics throughout all processes of the data collection (Creswell, 2009). A further conflict that can arise during data collection is the way of finding and gaining access to participants (Orb, Eisenhauer & Wynaden, 2001). To avoid this in the participant selection process the authoritative entities will be considered and asked to provide permission to do this in advance of the survey. For the purpose of this study the surveys will be conducted anonymously to protect the privacy of the participants. The participants will also be fully informed on the nature and purpose of the study and will receive notification of the results as well as receive an informed consent form.

4. Data Results and Analysis

In this section, the results of the survey will be summarised and analysed in order to explain certain characteristics that could lead to an answer to the research question posed at the beginning of this thesis: *How does trust in Bitcoin relate to trust in the underlying Blockchain technology within financial systems and what factors lead to this relationship?* To find the answer to this question, the backbone of trust in the financial system of Bitcoin and the underlying technology of Blockchain behind it as well as the general propensity of trust in technology of respondents had to be analysed. All of the trust attributes within these points are vital towards the final research question, as they are all an integral part of trust within Bitcoin as a Financial service.

4.1. General Overview and Description of Sample

The data for this thesis was collected using Google Forms and was collected between April 2020 and June 2020. In total, the number of respondents who answered the survey was 158[1]. The sample was collected by means of convenience, which may limit and restrict its external validity. An example of this can be seen in the educational level, as most respondents within the sample have at least a Bachelor's degree, if not a higher level, which is not representative for the general population. Furthermore, within the demographic section some of the results were merged in order to create larger groups within the data analysis to receive a more representative result.

- Gender: The frequency of female respondents was 86, which has a percentage value of 54.4% over the entire sample, and the number of male respondents was 72, with a percentage value of 45.6% of the sample.
- Age: The age demographic of the respondents was split into six subgroups, wherein there was a significantly higher percentage of 18-24 year-old respondents, at 38,6% of the sample, than any other subgroup. The other age groups were as follows: 25.9% 25-34 years old, 17.1% 35-44 years old, 10.1% 45-54 years old, 7.6% 55-65 years old and 0,6% of the sample was over the age of 65. This shows a clear bias in respondents with respect to age throughout the sample.
- Country of origin: The sample includes respondents from 29 countries from all over the world. In order to create larger more representative groups these were merged into two groups; countries within the EU and countries that are outside of the EU. 77.8% of the respondents were from countries within the EU, at a frequency of 123. At a frequency of 35, the percentage of respondents from outside the EU is 22.2%.
- Level of Education: The sample is split into five sections in this demographic; completion of High-School or equivalent, Bachelor's degree, Master's degree, PhD or Doctorate, Apprenticeship or other educational level. The percentage of respondents in each of these groups was 22.2%, 38.0%, 34.8%, 2.5%, 0.6% and 1.9% respectively.

[1] When calculating the statistical values, note that *N* may sometimes be a multiple of this due to the merging of questions in the survey for the data processing and analysis in order to find mean values of results.

- Status of Employment: This demographic of the sample was divided into five groups, where the respondents who answered with ‘employed’ are the leading group with 60.1% in the entire sample. The second largest group are students, at 25.3%, followed by 8.2% self-employed respondents, 5.1% unemployed and 1.4% retired respondents.

In the survey, respondents were asked to rate several statements on a Likert scale from strongly disagree (1) to strongly agree (5). There were several statements for each attribute of trust for both trust in Blockchain as a financial service (section C) as well as trust in Bitcoin as a financial system (section D) of which the mean was calculated. To determine the general propensity to trust in technology, several items were also used. As the statements in the survey were in a text format they had to be converted into a numeric value when calculating the data (as seen in table 2), and are also presented as such in all the data tables and figures in this chapter.

Statement in Survey (Text Format)	Numeric Value of Statement
Strongly Disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly Agree	5

Table 2. *Conversion of statements in the survey into numeric values.*

4.1.1. Propensity to Trust Technology

Figure 5 shows respondents’ general propensity to trust technology. The results leading to this figure came from the combination of four questions within the survey where participants had to rate statements regarding their trust in technology in general, where ‘strongly disagree (1)’ represents a lack of trust and ‘strongly agree (5)’ represents the presence of trust. These questions can be found in chapter 3, section (B).

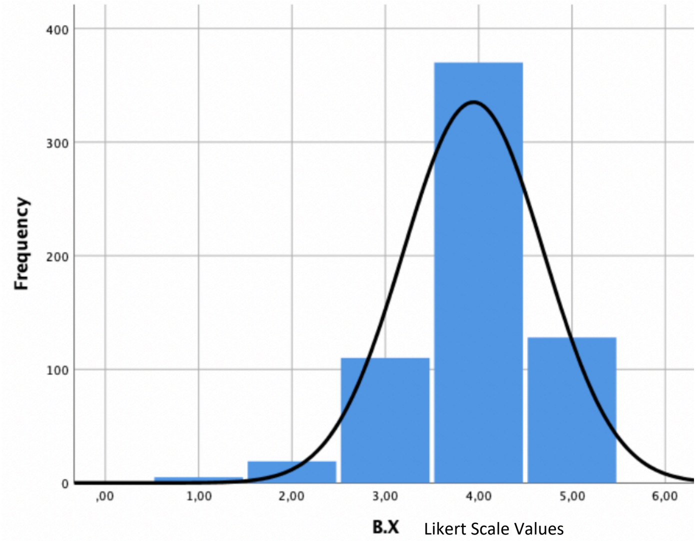

Figure 5. *Propensity to Trust Technology (B.X).*

The histogram in figure 5 represents the entire sample. It shows that in general respondents' propensity to trust technology tends to the positive side with most respondents answering with 'agree' (= 4 on the Likert scale) a mean score of 3.94/5 which shows that most respondents tend to have a relatively high propensity to trust in technology, as the mean of 3.94 is closest to the statement 'Agree' on the Likert scale.

4.1.2. Trust in Blockchain as a Financial Service and Bitcoin as a Financial System

Attributes of Trust	***Blockchain (Fin. Ser.) Average values***	***Bitcoin (Fin.Sys) Average Values***
Competence & Ability	3.61	3.12
Integrity & Consistency	3.32	2.76
Benevolence, Concern & Shared Values	3.00	2.41
Communications & Transparency	3.13	2.89

Table 3. *Respondents' trust in Blockchain and Bitcoin.*

	Average Trust
Blockchain as a Financial Service	3.26
Bitcoin as a Financial System	2.83

Table 4. *Respondents' average value of the attributes of trust in both Blockchain and Bitcoin.*

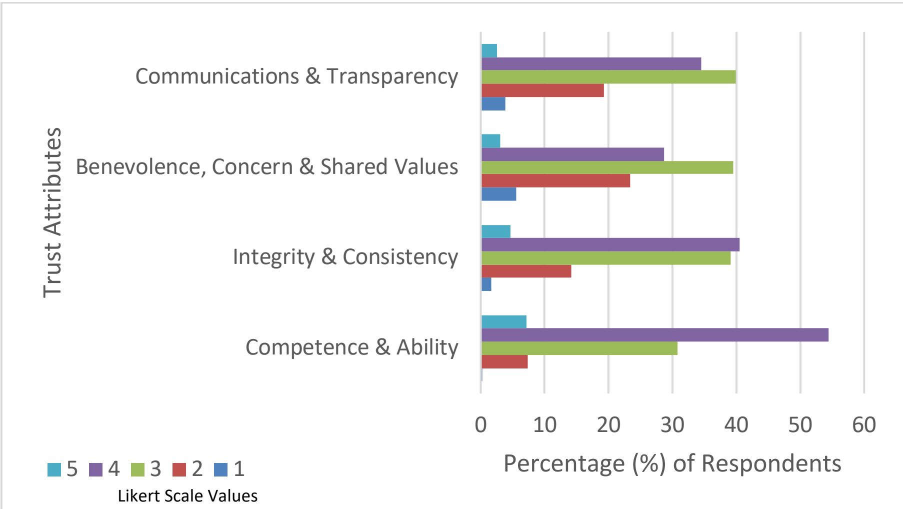

Figure 6. *Distribution of respondents' level of trust in the different Attributes of Trust within Blockchain as a Financial System*

Figure 6 shows the distribution, in percentage, between the four attributes of trust in Blockchain technology as a financial service of the respondents. The overall average of trust in blockchain as a financial service is calculated by adding all the values across all four attributes and dividing it by N; Trust in Blockchain as a Financial Service = (CA + IC + BCS + CT)/N = 3.26 on the Likert scale. As '3' represents 'Neutral' on the scale, it can be stated that on average respondents of the sample are only slightly trusting of blockchain in terms of finances. The four attributes also all have a similar distribution between each other as well as within each attribute. When comparing the four attributes of trust to each other it can be seen that the trust attribute 'competence and ability' seems to be valued as the highest, as its average value (as seen on Table 2) lies at 3.61. This is followed by 'integrity and consistency' at 3.32, then 'communications and transparency' at 3.13 and 'benevolence, concern and shared values' has the lowest average at 3.00. The significance between all four groups has been calculated by a one-way ANOVA test on SPSS, with all values at 0.05≥p, which enables us to accept H1, stating that there is a significant difference between the four attributes of trust. Moreover, it can be said that the four attributes of trust are correlated in a positive direction, due to the similar distribution of the respondents on the 5-point Likert scale across all four attributes of trust.

Still, it remains, that as all of the values are over '3' or equal to it on the Likert scale, that all four attributes of trust are considered important. Nevertheless, the attribute 'competence and ability' of Blockchain technology is considered the most important in terms of it being used as a financial service.

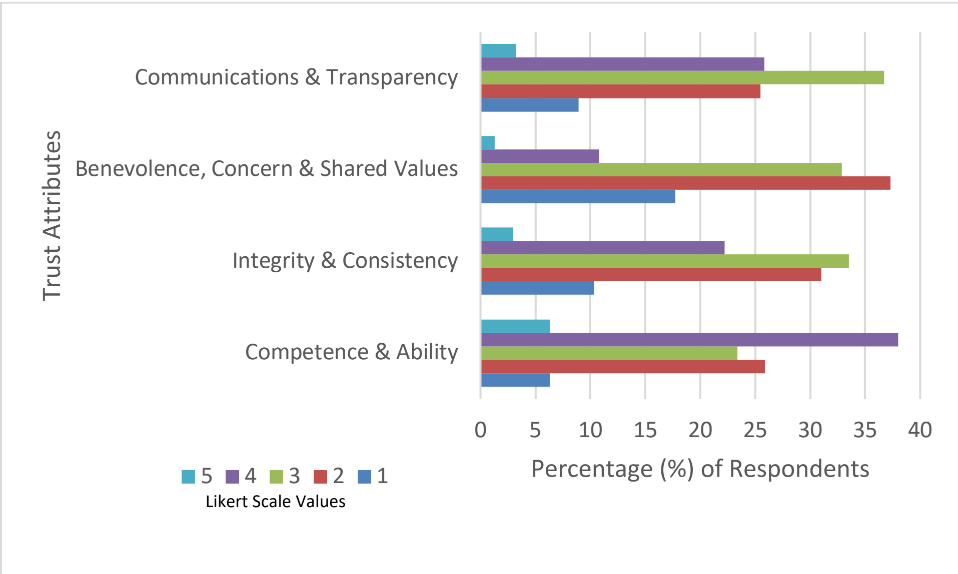

Figure 7. *The distribution of respondents' level of trust in the different Attributes of Trust within Bitcoin as a Financial Service.*

When comparing figures 6 and 7 to each other we can see that the general tendency to trust Bitcoin as a financial system is somewhat lower than the one to trust Blockchain as a financial service. This is also supported by the calculated mean of the attributes (also found in Table 3), Mean = (CA + IC + BCS + CT)/N = 2.83. This shows us, that on average people are less than '*neutral*' (point 3 on the Likert scale) when trusting Bitcoin as a financial system, potentially even a mistrust in it. When comparing the trust values between the four attributes, the attribute 'competence and ability' seems to carry the highest weight for respondents at an average value of

3.12, similar to trusting in Blockchain technology. However, the trust attribute with the second highest average is 'communications and transparency' with an average of 2.89. Only then comes 'integrity and consistency' with a mean of 2.76, and finally 'benevolence, concern and shared values' with its average trust lying at 2.41 on the Likert scale. These values show that trust in Bitcoin as a financial system is quite low, with the overall average lying under the 'neutral value'. When looking at the human-like 'translations' of the attributes of trust in technology (found in chapter two) the relatively higher level of trust in Bitcoins 'competence and ability' as a financial system could potentially suggest that respondents believe that it has the capability to execute its functional purpose, however its helpfulness and reliability is not as clear to them. Figure 7 also shows that the distribution of responses also seems to be fairly similar when comparing the four attributes of trust to each other, even if the general tendency is to trust is lower on average. This suggests, for example, that participants who are less trusting in one aspect of trust are also less trusting in another one, or even all four. Thus, the null hypothesis can be rejected at 0.05≥p because the relationship between all four trust attributes 'competence & ability', 'integrity & consistency', 'benevolence, concern & shared values' and 'communications & transparency', is considered statistically significant.

Hypothesis	Accepted/Rejected	Sig. value
H1: ***There is a significant difference in propensity to trust technology with respect to demographic groups (gender/ age/ employment status/ educational level/ nationality).***	Accepted (one-way ANOVA)	0.05≥p
H2: ***There is a significant difference between the four attributes of trust (C/I/B/T) in trusting Blockchain as a financial service.***	Accepted (one-way ANOVA)	0.05≥p

Table 5: *Determination of Confirmation or Rejection of Hypotheses (H1 and H2)*

4.2. Results and Analysis

After the general analysis and description of the constructs of trust in trusting both Blockchain and Bitcoin in terms of financial services and systems, this data can be used to further analyse the affects these may have on each other. Moreover, after determining the backbone of trust in both of these technologies they can now be compared to each other to determine a possible relationship which could lead to an answer to the main research question.

4.2.1. Demographic Groups and Propensity to Trust Technology

In this subsection the propensity to trust technology will be compared to all demographic groups of the sample. The statements on the five-point Likert scale were converted into numeric by recoding them into different variables using the SPSS program. The numeric values of the statements are shown in Table 1. When comparing the demographic groups, the percentage (%) of respondents was taken from within each group (e.g. in Figure 8, the orange bars on the histogram showing male respondents cumulate to 100%, and the blue bars representing female respondents equally add up to 100%).

i) <u>Gender</u>

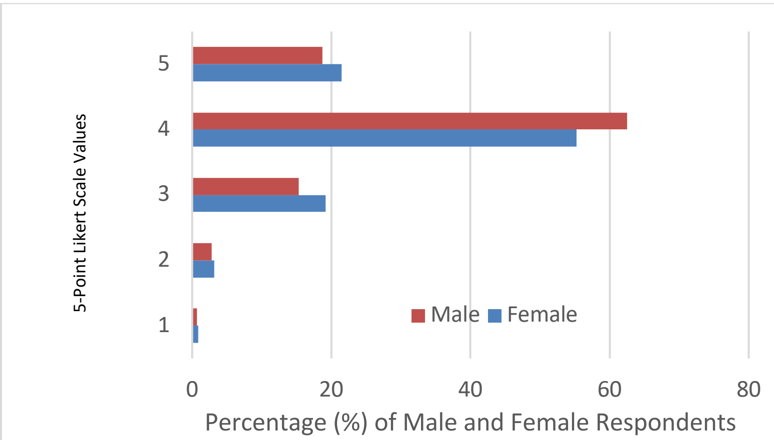

Figure 8. *Distribution (%) of male and female respondents' level of propensity to trust in technology.*

Figure 8 shows us that the highest percentage distribution of both male and female survey participants is at Likert scale point 4, meaning that they selected 'Agree' to most statements regarding their general trust in technology. Figure 5 shows that, on average, male respondents in the sample had a slightly higher propensity to trust in technology (Mean = 3.95) than females (Mean = 3.93). A t-test revealed that there is no significant difference in the scores for females and males (t(158) = -0.419, p =

0.675). Thus, the null hypothesis is retained, and it can be stated that the factor of gender may not create a significant difference in propensity to trust technology.

ii) <u>Age</u>

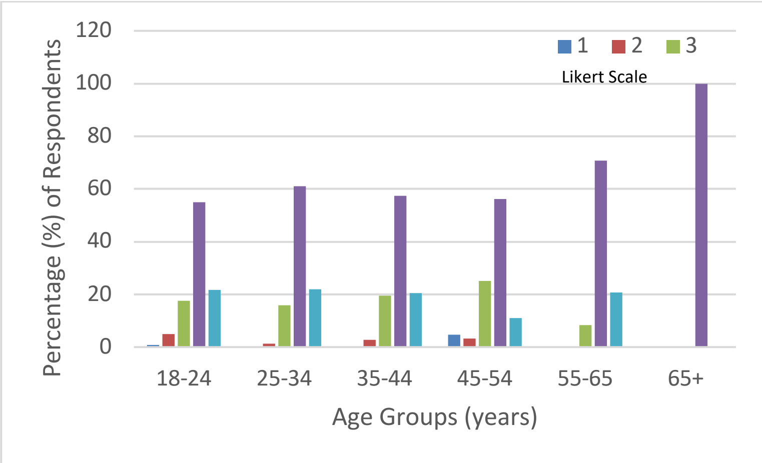

Figure 9. *Distribution (%) of level of propensity to trust in technology of respondents in different age groups.*

Age Group	*Mean Value*
18-24	*3.92*
25-34	*4.04*
35-44	*3.95*
45-54	*3.66*
55-65	*4.12*
65+	*4.00*

Table 6. *Mean values of respondents' propensity to trust technology with respect to different age groups.*

The mean values of propensity to trust in technology range between the 3.66 (age group 45-54) and 4,.2 (age group 55-65). Both of these values deviate quite a lot in relativity from the overall average in propensity to trust technology, of 3.94. Figure 9 shows when looking at the age group separately a difference in the skew of the graphs can be observed within the age group of 65+, as there is a symmetrical distribution, as all responders in the sample within this age group answered the same. The histogram is negatively skewed for all other age groups. The age group with seemingly the highest propensity to trust technology is 55-65 at an average of 4.2. Contrastingly the age group with the lowest propensity to trust in technology is the adjacent one (45-54 years old) with an average of 3,66. On average it seems that the trend of propensity to trust technology increases with age, however between the ages of 35-54 this trust seems to dwindle. Thus, respondents' age seems to be of significance when considering their propensity to trust in technology. As p = 0.010 (when F(5,626) = 3,040) from the one-way ANOVA, this supports the significance claim and the null hypothesis can be rejected at the 0.05 level. Previous research suggests that age plays a role in respondents' general attitude towards technology, in the form that younger people in more recent generations are considered to have grown up with it (Halmdienst, Radhuber and Winter-Edmer, 2019). However, this is also the reason that younger people tend to be more sceptical of technology when it comes to trusting it. Due to their, on average, higher level of knowledge and understanding they also see the problems and negative aspects that can come with technology. The results in figure 9 indicate that propensity to trust in technology varies across age groups, however, this may also be in slight accordance to other demographic groups, such as educational level or employment status, which also affects knowledge of technology, and by association also the trust in it.

iii) <u>Educational Level</u>

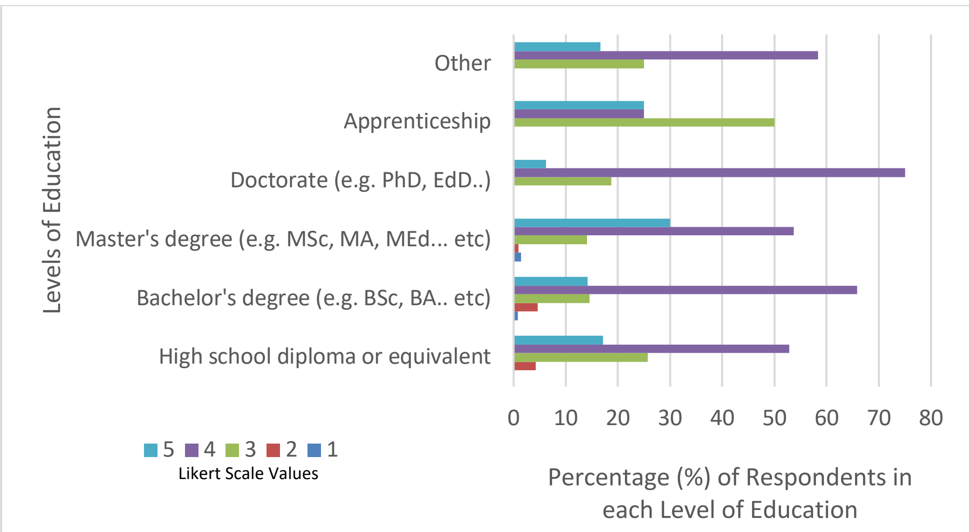

Figure 10. *Distribution (%) of level of propensity to trust in technology of respondents in different levels of education.*

Level of Education	*Mean Value*
High School diploma or equivalent	*3.83*
Bachelor's Degree (e.g. BSc, BA...)	*3.88*
Master's Degree (e.g. MSc, MA, Med...)	*4,10*
Doctorate (e.g. PhD, EdD...)	*3.88*
Apprenticeship	*3.75*
Other	*3.92*

Table 7. *Mean values for propensity to trust technology at different levels of education.*

Looking at figure 10, it can be determined that level of education has an effect on propensity to trust in technology. The distribution of mean values between the educational levels has a range of 0.35. The respondents who indicated to having a Master's degree have the highest propensity to trust in technology, whereas the respondents with a completed apprenticeship have the lowest, at 3.75 (See Table 5). When looking at the results, the mean values of propensity to trust increase as higher educational levels are reached but decrease at respondents with a Doctorate. When performing a one-way ANOVA test with SPSS the results also indicate a significant effect of educational level on propensity to trust technology at the $p<0.05$ level for all six different levels ($F(5,626) = 3.040$ and $p = 0.010$), resulting in the rejection of the null hypothesis of the various education levels not making a difference on the propensity to trust in technology. Figure 10 also shows that the highest percentage of respondents at all educational levels, except people with an apprenticeship, have selected '4' on the 5-point Likert scale, indicating a relatively high level of propensity to trust in technology.

iv) Employment Status

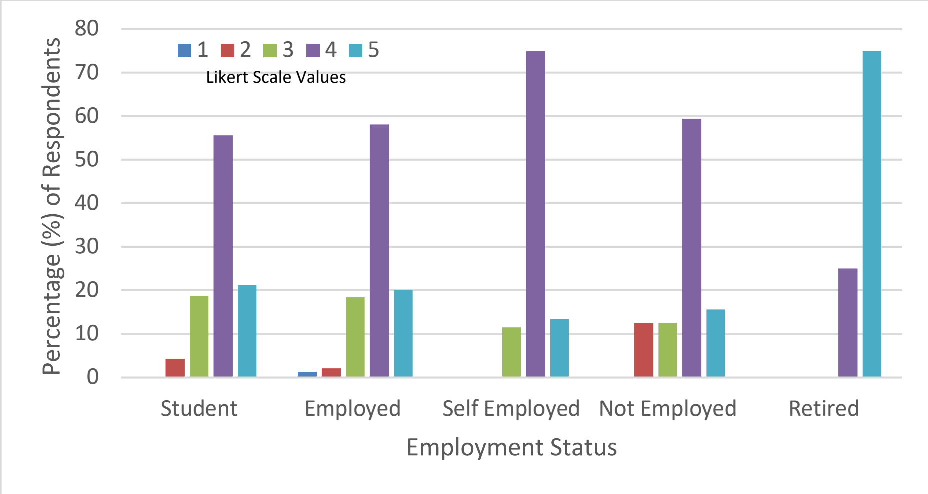

Figure 11. *Distribution (%) of level of propensity to trust in technology of respondents in different Employment Statuses*

Employment Status	***Mean Value***
Student	*3.94*
Employed	*3.93*
Self employed	*4.02*
Not employed	*3.78*
Retired	*4.75*

Table 8. *Mean values for propensity to trust in technology at different employment statuses.*

When considering employment status, table 6 shows that there is a difference in mean values across all employment statuses. The average propensity to trust technology of unemployed responders is the lowest at 3.78. This is however still over 'Neutral', showing that on average responders of all employment statuses have positive propensity to trust technology. The highest mean value is that of the retired responders, at 4.75. This indicates that retired responders have a very high tendency to trust in technology. Students come in second at mean=3.94, followed by self-employed people, and then employed people. These relatively large differences in average values imply that employment status may have a significant effect on propensity to trust technology, which is also supported by the one-way ANOVA test performed in which p<0.05 for the five different categories (F (4,627) = 2.853, p = 0.023). As the p value is below the 0.05 the null hypothesis, stating the absence of a significance of employment status on propensity to trust technology can be rejected.

v) Nationality (Regional – EU/Non-EU)

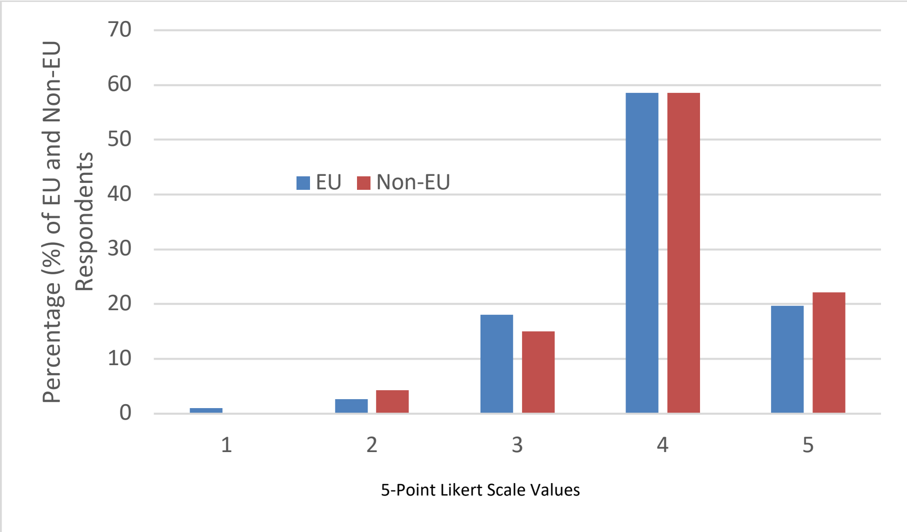

Figure 12. *Distribution (%) of respondents' level of propensity to trust in technology from EU and Non-EU Countries.*

Country of Origin	***Mean Value***
EU countries	*3.93*
Non-EU countries	*3.99*

Table 9. *Mean values of propensity to trust in technology for different countries of origin (grouped as EU and Non-EU countries)*

Figure 12 shows a clearly very similar distribution of results between responders from countries within or outside the EU. This signifies that country of origin does not have any visible effect on propensity to trust in technology. The mean values are also very close, as can be seen in table 7. A t-test was performed to test whether there was no significant difference in the scores for respondents from within the EU (Mean = 3.93, Standard deviation = 0.076) or outside the EU (Mean= 3.99 / Standard deviation = 0.074) at the conditions of t(158) = -0.732, p = 0.464. As p>0.05 the null hypothesis, stating that geographical origin has no significance when propensity to trust in technology is concerned is retained.

H3: There is a significant difference in propensity to trust technology with respect to demographic groups	Accepted/Rejected	Sig. value
Gender	Rejected (T-Test)	p>0.05
Age	Accepted (one-way ANOVA)	P<0.05
Educational Level	Accepted (one-way ANOVA)	P<0.05
Employment Status	Accepted (one-way ANOVA)	P<0.05
Country of Origin (EU/Non-EU)	Rejected (T-Test)	p>0.05

Table 10: *Determination of Confirmation or Rejection of Hypothesis (H3).*

4.2.2. Effects of Propensity to Trust in Technology

In this section the effect of propensity to trust in technology on both Bitcoin as a financial system and Blockchain as a financial service will be discussed, with the aim of answering research hypotheses (D) and (E), see chapter 3 for reference.

i) <u>Effect of propensity to trust in technology on trust blockchain as a financial service</u>

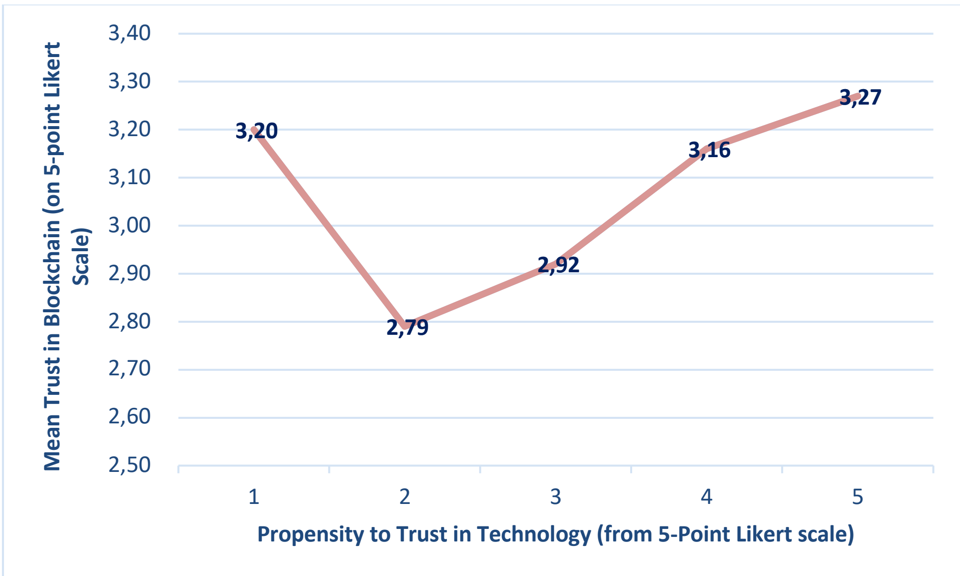

Figure 13. *Mean level of Trust in Blockchain as a Financial Service with respect to Propensity to Trust Technology.*

When looking at figure 13, a clear increase of trust in blockchain technology as a financial service can be observed for propensity to trust in technology, when starting at point 2 on the Likert scale. The high level of trust in blockchain when propensity to trust is at *1* on the Likert scale, can be explained by the lack of participants answering 'strongly disagree' in the questions regarding propensity to trust in relativity to the higher levels. On average about 59% of all respondents answered the propensity to trust technology questions in the survey with *'agree'* ('4' on the Likert scale), compared to the 0,8% who answered with '*strongly disagree'* ('1' on the Likert scale). However, this limitation does not hinder the clearly indicated positive correlation of the two variables. A linear regression was calculated to predict trust in Blockchain as a financial service based on propensity to trust in technology. A significant regression equation was found ($F(1,630) = 10.059$, $p<0.002$) with an R^2 value of 0.016. This small R^2 value could be a result of the low percentage of respondents at *1* in propensity to trust technology in relation to the other points. Nevertheless, as the p-value is below 0,05 the propensity to trust technology is implied as a significant factor when trusting Blockchain as a financial service.

ii) On Trust in Bitcoin as a Financial System

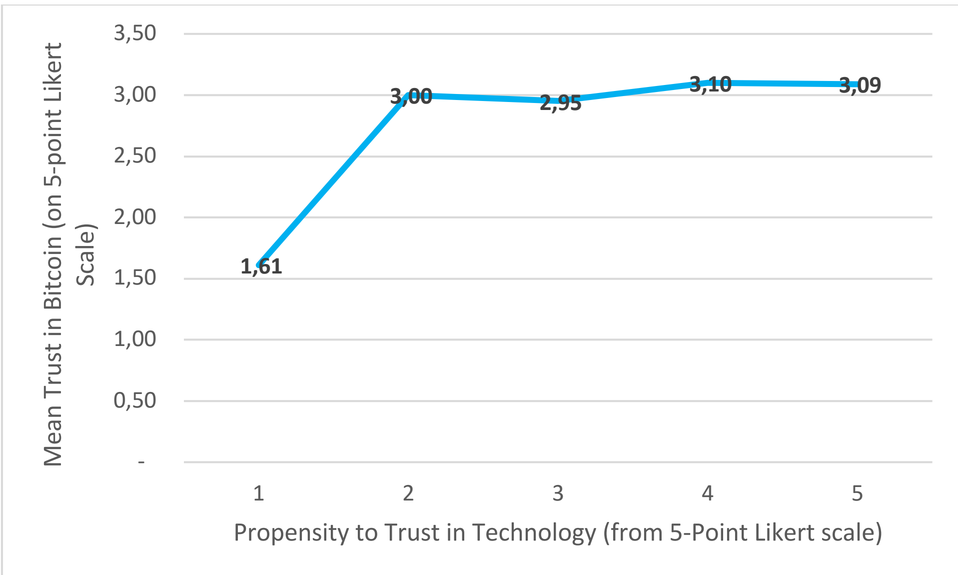

Figure 14. *Mean level of Trust in Bitcoin as a Financial System with respect to Propensity to Trust Technology.*

When looking at figure 14, a positive trend between propensity to trust technology and trust in Bitcoin as a financial system can be observed. The average value of trust in Bitcoin for responders who have a *'neutral'* (point 3 on the Likert scale) propensity to trust technology shows a slight decrease, however this may change to fit the general trend when a larger sample size would be considered. It also has to be kept in mind that the values in the 'trust in Bitcoin as a financial service' are merely the mean values. There may be an outlier in the raw data that skews the mean value. To support the statement considering the significance, using SPSS a linear regression was calculated to predict the trust in Bitcoin as a financial system based on propensity to trust in technology. The regression equation was found to be significant; ($F(1,630) = 4.129$ at $p<0.043$) with and R^2 value of 0.07. As $p<0.05$ the null hypothesis can be rejected.

4.2.3 Effect of Trust in Blockchain on Trust in Bitcoin

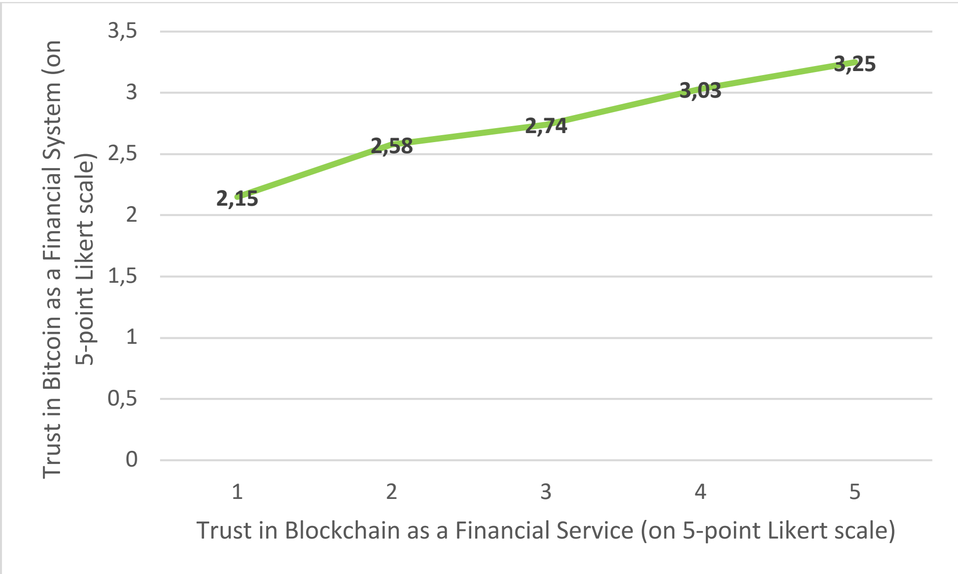

Figure 15. *Mean level of Trust in Bitcoin as a Financial System based on Trust level in Blockchain as a Financial Service.*

Looking at figure 15 a positive correlation can be observed between trust in Bitcoin as a financial system based on trust in Blockchain technology as a financial service. Trust in Bitcoin increases proportionately as trust in blockchain is higher in respondents. A linear regression was calculated to predict trust in Bitcoin as a financial system based on trust in blockchain as a financial service and a significant regression equation was found; (F (1.2052 = 96.626 at $p<0.000$) with an R^2 value of 0.045. Thus, the null hypothesis may be rejected as $p<0.05$.

Hypothesis	Accepted/Rejected	Sig. value
H4: *There is a positive correlation between trusting Blockchain as a financial service with respect to propensity to trust technology.*	Accepted (Linear Regression)	P<0.05
H5: *There is a positive correlation in trusting Bitcoin as a financial system with respect to propensity to trust technology.*	Accepted (Linear Regression)	P<0.05
H6: *There is a positive correlation in trusting Bitcoin as a financial system with respect to trusting Blockchain as a financial service.*	Accepted (Linear Regression)	P<0.05

Table 11: *Determination of Confirmation or Rejection of Hypotheses (H4-H6).*

5. Conclusion

5.1. Outcomes and Recommendations

In conclusion, it can be said that trust in both Bitcoin and blockchain technologies comes as a result of several factors and sublayers of trust. One of these factors is propensity to trust in technology in general. Results and analysis of the quantitative survey data collected, suggested that out of the five different demographic groups tested, respondents' age, educational level and employment status had a statistically significant effect on propensity to trust in technology, whereas gender and country of origin did not. When considering age as a variable, the results from the survey did not indicate any specific directional correlation to respondents' propensity to trust technology, however even though a significant effect was detected. Nevertheless, previous research suggests that age may have a direct effect on propensity to trust in technology, as younger generations have been significantly more exposed to it and in recent generations people are already being called 'digital natives' (Kesharwani, 2020). Research also suggests that the higher this technological exposure is, the more knowledgeable people are, and the tendency is that younger people are more exposed to technology on average and therefore, being more open to it and have a higher propensity to trust in it (ibid.).

Another factor considered significant towards propensity to trust in technology was educational level. This is also clearly resultant from having a higher knowledge base, which is most likely directly proportional towards having a higher propensity to trust, not only in technology but also in other fields (Jessup et al., 2019). Employment status was also determined to be a significant variable when considering propensity to trust in technology. Respondents who were either students, employed or self-employed had the highest average values, which similarly to the other influential demographic groups, suggests that constant or frequent exposure to technology has a positive impact on propensity to trust technology. These results indicate that businesses intending to use either blockchain or Bitcoin should also consider their customers propensity to trust in technology, and what this trust is based on. A clear trend in the significant demographic groups seems to be that a greater comprehension of technology, whichever way an individual may come to it, is an essential characteristic of a higher propensity to trust in technology.

Next, trust in both Bitcoin and Blockchain in financial systems was explored. The results show that in blockchain as well as Bitcoin, when considering finances, the trust attribute 'competence and ability' had the highest significance. A reason for this could be that when this attribute of trust in concerned, the overall functionality of the technologies is being examined by the respondents. This means that if the technology, in this case blockchain and Bitcoin, is not considered to be functional enough to execute its intended purpose then the trust in its competence and ability is low. On the other hand, if it is seen to be as a useful tool for a required financial function, then trust in its capabilities are respectively higher.

The second highest valued construct of trust in Blockchain as a financial service was found to be integrity and consistency. This can be explained from previous research, indicating that being able to rely on technology to perform its function in a consistent manner (Marella et al., 2019). However, the results of the data collection show this attribute to be only in third place, when taking trust in Bitcoin as a financial system into consideration. This, however, could be explained by the second highest weighted attribute in Bitcoin trust, which is 'transparency and communications'. As Bitcoin is associated with money and currencies this is an understandable result, because transparency in cash flows and transactions is a fundamentally crucial aspect in finance (Esterik-Plasmeijer and Raaij, 2017).

In both Blockchain as a financial service and Bitcoin as a financial system, the trust attribute 'benevolence, concern and shared values' had the lowest significance when considering trusting either of the technologies. A reason for this could be that when considering finances, the tendency is to put a higher weight on functionality and competence of a system, as well as certain amount of reliability. Likewise, as seen from the results of the effect of from propensity to trust in technology on trust in Bitcoin and Blockchain, a higher propensity to trust technology results in a higher level of trust in the specific technology, and as previously iterated a higher propensity to trust in technology, may be a direct result of knowledgeability of it. So, if knowledgeability is higher in a technology, then the need for it to be benevolent and helpful is somewhat reduced.

The direct effect of trust in Blockchain technology as a financial service on trust in Bitcoin as a financial system was also determined to have a positive correlation. This could be explained by blockchain being the underlying technology behind Bitcoin, and thus if the technology behind the system is not trusted, then the system can also not be trusted, and vice versa. In summary, these results give several indications towards an answer to the research question posed at the beginning of this thesis;

> *How does trust in Bitcoin relate to trust in the underlying Blockchain technology within financial systems and what factors lead to this relationship?*

Trust in Bitcoin relates to trust in blockchain in a positively correlational manner due to blockchain being the underlying technology behind Bitcoin. Thus, it can be stated that the trust existing in Blockchain is of greater importance as it is the technological function behind a system. As several industries and businesses are beginning to work with Blockchain, this deduction holds a significant standpoint.

The research result also found that the trust attribute of 'competence and ability' held the most significant value in trusting both Blockchain and Bitcoin as financial systems, which are directly related to increased levels of propensity to trust in technology. This high level was found to be a result of correspondingly having a high level of knowledge, understanding and exposure to technology. This is underlined by Alarcon et al.'s (2017) research on the development of relationships between trustors and trustees; if the trustor gains more knowledge and information on the trustee, in this case blockchain and Bitcoin, the higher the perception of trustworthiness in the trustee – which increases the overall trust the trustor has in the trustee. So, a considerable conclusion is that if comprehension and understanding of it is existent, then so is trust in both Blockchain as well as Bitcoin as a financial system. In this case it is recommendable for businesses intending to use blockchain in any application to encourage and provide their customers and users with an opportunity to increase their knowledge and understanding of blockchain, in order to inspire trust in them and therefore a higher willingness to use the application.

5.2. Evaluation of Limitations

There were several limitations of the thesis research that came to light throughout in the translation of the data into graphical and tabular formats. Another limitation is the format in which the data collection occurred. As data collection in the primary research occurred by means of a convenience sample, the conclusions coming from this research may potentially not be generalized on to a population. As the author originates from Austria, over half of the respondents were also of Austrian nationality, at 51,3%. Further demographic groups were also close to those of the author, which may not represent a generalized population. These factors could have affected the data and skewed some of the graphs. If the sample size were increased or the method of sampling was altered the data collection could be considered as more reliable.

A further limitation of the data is the time period in which it was collected. As this was a cross sectional survey, it only reflects results a certain period of time, and this happened to be during the emergence of the COVID-19 epidemic. The period in which the data was collected was one of economic insecurity which may have had an impact on responses, as the topic is one of relevance to the financial industry.

As mentioned in the methodology section, an additional final question was included in the survey to determine whether or not respondents would have answered differently had the data collection happened previous to the epidemic. Results showed that 86,1% of respondents answered with ‘no’. This means that the 22 respondents representing the remaining 13,9% may have skewed the results. As it was not asked how or why they would have answered differently, this factor cannot be discussed.

6. Bibliography

Acharya, V., Engle, R., and Pierret, D., (2014). Testing macroprudential stress tests: The risk of regulatory risk weights. *Journal of Monetary Economics*, Elsevier, vol. 65(C), pages 36-53.

Alarcon, G.M., Lyons, J.B., Christensen, J.C., Klosterman, S. L., Bowers, M. A., Ryan, T. J., Jessup, S. A., Wynne, K. T., (2017). The effect of propensity to trust and perceptions of trustworthiness on trust behaviors in dyads. *Behaviour Research Methods* 50, 1906–1920. https://doi.org/10.3758/s13428-017-0959-6

Alberti, A. M., Singh, M., & Da Rosa Righi, R. (2020). Blockchain Technology for Industry 4.0. 1-46. *Springer Nature Singapore.*

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143-174.

Atzori, M., (2015). Blockchain technology and decentralised governance: Is the state still necessary? *Journal of Governance and Regulation, 6(1), 45-62.* http://dx.doi.org/10.22495/jgr_v6_i1_p5

Babbie, E.R. (1990). *Survey Research Methods*. Wadsworth Publishing Co., Belmont.

Bernerth, J. B., & Walker, H. J. (2008). Propensity to Trust and the Impact on Social Exchange*. Journal of Leadership & Organizational Studies, 15(3), 217–226.* doi:10.1177/1548051808326594

Bornstein, M. H., Jager, J., & Putnick, D. L. (2013). Sampling in developmental science: Situations, shortcomings, solutions, and standards. *Developmental Review, 33*(4), 357-370. doi:10.1016/j.dr.2013.08.003

Bownes, R. for: Griggs, I., (2018). 'A Watershed Moment'. *PR Week.* Retrieved from Web: https://www.prweek.com/article/1460137/a-watershed-moment-people-woken-facebook-data-used-following-cambridge-analytica-scandal

Chiu, J., Koeppl, T. (2017). The economics of cryptocurrencies - Bitcoin and beyond., *Queen's Economic Department Working Paper* (1389). Queen's University Press.

Chung, M., & Kim, J. (2016). The Internet Information and Technology Research Directions based on the Fourth Industrial Revolution. *KSII Transactions on Internet and Information Systems, 10*(3). 1311-1320, doi:10.3837/tiis.2016.03.020

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, 92, 909-927.

Chakravorti, B., (2018). Trust in Digital Technology will be the Internet's Next Contractual Environment. *Cambridge Journal of Economics. 21 (2), 217-37.*

Chakravorti, B., (2018). Trust in Digital Technology will be the Internet's Next Frontier for 2018 and Beyond. *Scientific American Online.* Web.

Collins, R., (2018). Digital Transformation and New Ways of Thinking and Acting. *The Digital Transformation People.* Web.

Cooper, D. R., & Schindler, P. S. (2006). Business Research Methods (9th edition). 2-20. USA: Richard D. Irwin.

Creswell, John W. (2009). *Research design: qualitative, quantitative and mixed methods approaches* (3rd edition). USA: SAGE Publications

Emmanuel, N., (2019). Analysis of Saunders Onion. *Thesis Mind*.

Ennew, Christine, & Harjit Sekhon (2007). Measuring trust in financial services: the Trust Index *Consumer Policy Review*, 17, 62-68.

Ergungor, O. (2004). Market- vs. bank-based financial systems: Do rights and regulations really matter? *Journal of Banking & Finance, 28*(12), 2869-2887. doi:10.1016/j.jbankfin.2003.04.001

Esterik-Plasmeijer, P. W., & Raaij, W. F. (2017). Banking system trust, bank trust, and bank loyalty. *International Journal of Bank Marketing, 35*(1), 97-111. doi:10.1108/ijbm-12-2015-0195

Friedman, B., Khan, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM, 43*(12), 34-40. doi:10.1145/355112.355120*.*

Galar, D., Daponte, P., & Kumar, U. (2020). *Handbook of Industry 4.0 and SMART Systems*, 1-46. Boca Raton; London ; New York: CRC Press.

Glaser, F., (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis*.* In: *Proceedings of the 50th Hawaii International Conference on System Sciences,* 1543-1552 (HICSS 2017). Goethe Universität Frankfurt

Georgios, S., (2020). *A Granger Causality analysis between the bitcoin and the stock market returns of countries related to money laundering* (Published Master's Thesis). University of Macedonia

Halmdienst, N., Radhuber, M. & Winter-Ebmer, R. (2019). Attitudes of elderly Austrians towards new technologies: communication and entertainment versus health and support use. *Eur J Ageing* **16,** 513–523. https://doi.org/10.1007/s10433-019-00508-y

Hurley, R., Gong, X., & Waqar, A. (2014). Understanding the loss of trust in large banks. *International Journal of Bank Marketing, 32*(5), 348-366. doi:10.1108/ijbm-01-2014-0003

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review.* Web.

Jessup, S. A., Schneider, T. R., Alarcon, G. M., Ryan, T. J., & Capiola, A. (2019). The Measurement of the Propensity to Trust Automation. *Virtual, Augmented and Mixed Reality. Applications and Case Studies Lecture Notes in Computer Science,* 476-489. doi:10.1007/978-3-030-21565-1_32

Jones, S. L., & Shah, P. P. (2016). Diagnosing the locus of trust: A temporal perspective for trustor, trustee, and dyadic influences on perceived trustworthiness. *Journal of Applied Psychology, 101*, 392–414.

Kesharwani, A. (2020). Do (how) digital natives adopt a new technology differently than digital immigrants? A longitudinal study. *Information & Management, 57*(2), 103170., retrieved from Web: *Elsevier.* doi:10.1016/j.im.2019.103170

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into expectation disconfirmation theory. *The Journal of Strategic Information Systems*, 23(2), 128–145. https:// doi.org/10.1016/J.JSIS.2013.09.001.

Lankton, N. K., Mcknight, D. H., & Tripp, J. (2015). Technology, Humanness , and Trust : Rethinking Trust in Technology. *Journal of the Association for Information Systems*, 16(10), 880–918.

Lin, H. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International Journal of Information Management, 31*(3), 252-260. doi:10.1016/j.ijinfomgt.2010.07.006

Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Electronic Markets, 30*(2), 259-271. doi:10.1007/s12525-019-00392-5

Marr, B., (2018). A very brief History of Blockchain Technology everyone should read. *Forbes Online Magazine.*

Mayer, R. C., Davis, J. H., Schoorman, D. (1995). *An Integrative Model of Organisational Trust.* The Academy of Management Review, Vol. 20, No. 3, pp. 709-734.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). *Trust in a specific technology. ACM Transactions on Management Information Systems, 2(2), 1–25.* doi:10.1145/1985347.1985353

McNight, D. H., Cummings, L. L., and Chervny, N. L. 1998. Initial trust formation in new organizational relationships. *Academic Management.* Rev. 23, 3, 473-490.

Möhlmann, M. & Geissinger, A. (2018). Trust in the Sharing Economy: Platform Mediated Peer Trust. In: *The Cambridge Handbook on Law and Regulation of the Sharing Economy, 1-11*. Cambridge University Press.

Nakamoto, S., 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.

Narayanan, A., Bonneau J., Felten E., Miller, A., Goldfeder, S. (2016). *Bitcoin and Cryptocurrency technologies*. Princeton: Princeton University Press.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). *Blockchain. Business & Information Systems Engineering, 59(3), 183-187.* doi:10.1007/s12599-017-0467-3

Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in Qualitative Research. Journal of Nursing Scholarship, 33(1), 93–96. doi:10.1111/j.1547-5069.2001.00093.x

Pennington, R., Wilcox, H., & Grover, V. (2003). The Role of System Trust in Business-to-Consumer Transactions. *Journal of Management Information Systems, 20*(3), 197-226. Retrieved from www.jstor.org/stable/40398645

Raine, L., & Anderson, J. (2017). The Fate of Online Trust in the next Decade. *Pew Research Center.*

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. American Psychologist, 35, 1-7.

Sadhya, V., Sadhya, H., Hirschheim, R. and Watson, E. (2018). Exploring Technology Trust in Bitcoin: The Blockchain Exemplar*.* Research Papers *(*5). *ECIS 2018, Portsmouth UK.* doi:https://aisel.aisnet.org/ecis2018_rp/5

Sas, C., and Khairuddin, I. E. (2017). "Design for Trust: An exploration of the challenges and opportunities of bitcoin users.: In: *Procedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6499-6510). ACM.

Saunders. M., Lewis, P. & Thornhill, A. (2012). Research methods for business students, (6th ed.) London: Pearson.

Schneier, B. (2018). Security, Trust and Blockchain in: *Hyperledger Global Forum* keynote. Basel, Switzerland. Web. Retrieved from: https://www.linuxfoundation.org/blog/2019/01/how- blockchain-changes-the-nature-of-trust/

Schumann, J. H., von Wangenheim, F., Stringfellow, A., Yang, Z., Praxmarer, S., Jiménez, F. R., Blazevic, V., Shannon, R. M., Shainesh, G., and Komor, M.(2010). Drivers of trust in relational service exchange: Understanding the importance of cross-cultural differences. *Journal of Service Research*, 13, 453-468.

Sedgewick, K., (2019). Bitcoin History Part 10: The 184 Billion BTC Bug. *Bitcoin News*. Retrieved from: {https://www.news.bitcoin.com/bitcoin-history-part-10-the184-billion-btc-bug}

Sekhon, H., Ennew, C., Kharouf, H., & Devlin, J., (2014). Trustworthiness and trust: Influences and implications. *Journal of Marketing Management*, 30, 409-430.

Singh, S., & Chahal, D., Dr. (2020). A Survey on Bitcoin. *International Research Journal of Modernization in Engineering Technology and Science, 2*(4), 1014-1017. Retrieved July 11, 2020, from www.irjmets.com

Siva Durga Prasad Nayak, M., & Nayak, K. A. (2019). Strenghts and Weaknesses of Online Surveys. *IOSR Journal Of Humanities And Social Science,* 24 (5), 31-38.

Su, B. (2017). The evolution of consumer behavior in the digital age. *Medium.*

Swan, M. (2015). *Blockchain: Blueprint for a new Economy*. Beijing: O'Reilly.

Tabora, V., (2018). How the Blockchain Can Bring Trust and Transparency to the Advertsing Industry. *Medium.*

Tapscott, D., Tapscott, A., (2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Portfolio.

Tsang, S., Royse, C., & Terkawi, A. (2017). Guidelines for developing, translating, and validating a questionnaire in perioperative and pain medicine. *Saudi Journal of Anaesthesia, 11*(5), 80-89. doi:10.4103/sja.sja_203_17

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15-17. doi:10.1145/2994581

Vos, R. D., & Sawin, J. (2012). Drivers and Barriers. *READy: Renewable Energy Action on Deployment,* 49-62. doi:10.1016/b978-0-12-405519-3.00003-7

Walport, M., (2016). Distributed Ledger technology: Beyond Blockchain – A report by the UK government chief scientific advisor

Weisbaum, H., (2018). Trust in Facebook has dropped by 66 percent since the Cambridge Analytica Scandal. *National Broadcasting Company News.*

Werbach, K. (2017). Trust, but Verify: why Blockchain Needs the Law, 33. *Berkely Tech. Law Journal*. (487-549). UC Berkely.

Yahya, A., (2018). Web 3.0 and The Future of Trust [Keynote Address]. *A16Z Innovational Summit: Andreessen Horowitz*, Los Angeles, CA.

Zohar, A. (2015). "Bitcoin: under the hood." *Communications of the ACM*, 58(9), 104-113.

6.1. Sources with no identified authors

Blockchain Market by Component, Provider, Type, Organization Size, Application Area And Region - Global Forecast to 2025 (Rep. No. TC 4638). (May 2020). Retrieved July 2020, from Markets and Markets

Deep Shift: Technology: Tipping Points and Societal Impacts. (2015) Survey Report, *World Economic Forum*, Reference No. 310815.

Github, (2020). *Ethereum 2.0 Specifications.* Retrieved from: https://github.com/ethereum/eth2.0-specs?ref=hackernoon.com#design-goals

Statista – Bitcoin Price Index from July 2012 to June 2020 in U.S. dollars. Statista. July 7, 2020. - retrieved from https://www.statista.com/statistics/326707/bitcoin-price-index/