MODUL VIENNA UNIVERSITY
WKO WIEN PRIVATE UNIVERSITY

An assessment of trust in blockchain-based assets and technologies.

Bachelor Thesis for Obtaining the Degree

Bachelor of Science

in

International Management

Submitted to Horst Treiblmaier

Grigory Shkrbich

1521501

Vienna, 20th of May 2019

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.

20th of May 2019

Date

Signature

Abstract

This survey research examines the extent of public trust in blockchain-based assets and technologies, as this field develops rapidly, providing a wide scope of possibly disruptive implementation scenarios. It is established on the suggestion that it is reasonable to measure perceived trust in blockchain-based technologies and services separately, dividing them into two iterations. Such categorization reflects on conceptually different scopes of application: blockchain-based assets (First Iteration) and blockchain-based databases, registries, and provisioning systems (Second Iteration). Most interestingly, such categorization allowed for comparison of the trust extent between 2 iterations. In the literature review, a vast array of existing and potential challenges and concerns have been presented. Suitable trust measurement model and questionnaire were found and adapted for the purposes of this research. Generally, 2 dependent aspects of trust were derived from the model mentioned above. Those were Trusting Beliefs (perceived benevolence, competence, integrity), which influence Trusting Intentions (willingness to depend). Statistical analysis of data gathered from 100+ respondents confirmed the initial suggestion that the degree of trust differs between 2 iterations of blockchain-based technologies. It was statistically proven that degree of Trusting Intentions differs significantly between 2 iterations, with Second Iteration being more trusted, judging by mean values. Alongside that, it has been attempted to detect the most important aspect of Trusting Beliefs by means of linear regression analysis. It was found that competence aspect has a particularly predominant influence on Trusting Intentions, in comparison with benevolence and integrity. Possible areas for further analysis and examination by other researchers have been proposed.

Table of Contents

List of Tables

Table 1.

Combined mean scores of the main constructs.

	FI	**SI**	**Δ**
Benevolence (TBb)	4.11	5.11	1.00
Integrity (TBi)	4.23	4.93	0.70
Competence (TBc)	4.01	5.00	0.99
Willingness to Depend (TIwtd)	3.05	4.29	1.24

Table 2.

Count of successful predictions by the trusting beliefs aspects.

Total number of regressions	**60**
TB benevolence (# of valid predictions)	**2**
TB integrity (# of valid predictions)	**6**
TB competence (# of valid predictions)	**13**

List of Abbreviations

FI – First Iteration (Refers to Blockchain 1.0)

SI – Second Iteration (Refers to Blockchain 2.0)

TB – Trusting Beliefs

TI – Trusting Intentions

Dapps – Decentralized Applications

DAOs – Decentralized Autonomous Organizations

ICO – Initial Coin Offering

EBI – European Banking institute

FOREX – Foreign Exchange

ICT – Information and Computer Technologies

PoW – Proof of Work

PoS – Proof of Stake

G2B – Government to Business

G2C – Government to Consumer

B2C – Business to Consumer

RQ – Research Question

CIS – Commonwealth of Independent States

OECD – Organization for Economic Co-operation and Development

1 Introduction

The way how we perceive Internet is now changing. A disrupting element – blockchain is currently emerging from a niche-oriented technology aimed to be a base for crypto currencies (Bitcoin, in the first place) into a programmable, distributed and decentralized mechanism. That enables a possibility to use it in a wide range of value based services and applications. The term “blockchain” itself is defined as a decentralized data storage technology or, in simpler words, a chain of blocks connected sequentially. These blocks contain chronologically ordered data points and are stored in a decentralized manner across all the participating nodes of the network (Adarsh & Asharaf, 2017). The principles of the technology allow it to be implemented almost everywhere – in payment provision services, governmental and corporate databases, logistics provision services, etc. Not to mention, crypto currencies. Just as any new innovative technology it will have to pass 5 stages of an adoption process (Rogers, 2003): Awareness, Interest, Evaluation, Trial and eventually, Adoption or Rejection. Depending on the industry and specific way of application, it is now undergoing almost each and every one of them. For instance, in the field of crypto-based value assets, it is a de-facto standard with almost every crypto currency or smart contract being based on blockchain. Over last 5 years, a size of Bitcoin blockchain grew by over 50 times, while an overall number of blockchain wallet users grew from 3.2 to almost 25 million just in 3 years (Statista, 2018). Therefore, we may conclude that in this aspect blockchain has already reached the level of common adoption. Interesting trends may be detected in the supply chain industry. In a recently conducted market scan, it was found that 69% of all respondents stated that they list blockchain research programs as expenditure in the first half of 2018 (Statista, 2018 This fact proves that industry is currently evaluating and seeking for most optimal application of this technology. At the same time, due to a recent news report, CITI Group is seeking for crypto currency professionals who would be able to evaluate an ability to launder money with such currencies and search for ways to prevent it (Business Insider, 2018). It indicates an undoubted awareness with a high degree of concern, basically, a significant lack of trust. A vast array of industries and possible applications creates an enormous field for studies, making it very difficult to generalize information, which is gathered from industry-specific sources (e.g. professionals, executives, etc.). That is the reason why it would be rational to divide blockchain applications into two large, but mostly non-interconnected groups and evaluate them separately. These would be:

1) Blockchain technology based assets (e.g. crypto currencies, tokens) serving as a medium of exchange / store of value

2) Blockchain based decentralized registry and provision systems (land registries, identification services, corporate and governmental databases, voting systems, etc.)

Meaningfulness of the above-mentioned fragmentation may be explained by the subsequent factors. To begin with, the first type of application and also the oldest-existing one (since 2008), which is usually referred to as "Blockchain 1.0", is mainly focused on crypto currencies and micro-payments, providing less scope for business applications. In its turn, the second type of application is far more advanced, and is usually referred to as "Blockchain 2.0": it is programmable, includes support of smart contracts, Dapps, DAOs and therefore, provides far more opportunities and fields of utilization (S & S, 2017). Expectably, FI of blockchain technology, which is the most used one as for today, has been compromised in many ways. Main factors of trust (or distrust) were formulated in the following way: legislation influence, availability, anonymity, volatility, and awareness (Bucko, Pal'ová, Vejačka, 2015). At the same time, SI due to further ability to be customized and utilized in more proprietary ways might consolidate more trust in itself. Given the high probability that SI of blockchain is likely to play an important role in shaping the future, it is exceptionally interesting how general public differentiates above-mentioned ways of application in terms of trust and whether it is prepared to entrust money, personal and other important data to blockchain technology. This separation facilitates a literature gap, as in previous researches (Bucko, et al., 2015) blockchain technology was evaluated only as a medium of exchange.

1.1 Practical relevance

There is a very high chance that the outcomes of this research will be beneficial for all parties involved in the blockchain industry. First of all, businesses, which are aiming to apply blockchain in B2C services, will be able to gain deeper insights in what people consider useful and trustworthy: it can certainly help in making the products more likely to be perceived positively by consumers. Secondly, results from public perception analysis can help in deciding whether to use blockchain for internal purposes – especially if it somehow affects end customers (for instance, whether it will be considered trustworthy to entrust sensitive personal data of customers to a blockchain based registry or not). Eventually, G2C and G2B services like public land and company registries, which are currently either kept in paper format or in a centralized electronic database, are very likely to be transferred on blockchain-based decentralized registries due to their ease of tracking, sustainability, and overall convenience. The question is how citizens are going to perceive it. After the boom of ICOs (BBC News, 2018) and numerous cases of scam, often reaching some ridiculous amounts – like recent Pincoin fraud of 660.000.000 USD (TechCrunch, 2018), the public might have already tightened blockchain and risk together. The more important it is to raise the question of trust.

1.2 Main Research Questions are:

1. To what extent do people trust in blockchain-based systems?

   1a. To what extent do people trust in Blockchain 1.0-based systems (crypto currencies and micropayments)

   1b. To what extent do people trust in Blockchain 2.0-based systems (distributed registries, smart contracts, etc.)

2. Does the extent of trust differ between two iterations of blockchain technology?

   2a. Is there any significant difference in the extent of trust into FI and SI of blockchain between different demographical groups?

3. Which aspects of trust influence public opinion and readiness to use blockchain based technologies and services the most?

1.3 The purpose of the study is to quantitatively explore the nuances of the public's perceived trust into blockchain-based technologies, basing it on a separation principle introduced above. Get the most applicable information possible, basing it on certain carefully synthesized insights, which will reflect upon both perspectives of blockchain technology application options. The analysis will be based on hypothesis testing, which will clarify what is perceived trust in 2 conceptually different types of blockchain-based technologies and whether this perception differs between them or not. The data will be collected through a quantitative survey, with diverse population sample obtained via convenience sampling. It will most likely allow for quite a comprehensive data analysis, possibly leading to findings in trust level differentiation between demographical segments. Likert-type and semantic differential scales, along with rating questions would be used to evaluate the level of trust among the population.

2 Literature review

2.1 Crypto Currencies (FI)

In this segment, several blockchain implications and implementation scenarios will be overviewed from a scientific perspective. Alongside this, an analysis of fundamental trust aspects related to blockchain and e-commerce, in general, will be carried out, in an attempt to output a scientifically valid approach to the assessment and possible comparison of trust level between FI and SI implications. Such analysis will allow to reflect on examples of blockchain implementation and define the best-fitting areas to be survey researched. Alongside that, it will certainly be helpful for the hypothesis development process. All the articles and publications mentioned foregoing in this review have been accessed and may be sent directly to the supervising body.

Evaluating blockchain technology as a way to provide an alternative possibility of monetary transactions and a store of value generally, it is reasonable to address the research on the economics of crypto currencies. Chiu & Koeppl, 2017, argue that the main problem of e-commerce transactions, in general, is the double-spending problem, which can be solved in two conceptually different ways: via an intermediary (like PayPal) or using a decentralized network. For some transactions, the first way may not be trustworthy enough as it still involves a certain degree of distrust to an intermediary (Chiu & Koeppl, 2017). The second way is how Bitcoin works – and that is the most interesting and prominent thing about it. For any crypto currency system, 3 main issues have to be solved:

1. How to establish a consensus in a distributed network?
2. How to discourage double spending behaviors?
3. How to encourage proper transaction validation?

In the case of Bitcoin, this is mostly carried out via the mining process, which is generally called a proof-of-work (PoW) mechanism – it involves a huge physically working pool of computation machines. Another mechanism is proof-of-stake (PoS), which requires substantially fewer resources and is used in some other crypto currencies like ShadowCash or Peercoin. Noteworthy, Ethereum developers are intending to switch from PoW to PoS algorithms in 2019. Generally, successful attacks are still possible even though they require a lot of resources and this fact may still be a reason for reduced trust in such systems (Chiu & Koeppl, 2017). At the same time, Bitcoin and Ethereum are not the only possible types of crypto currencies. They are both unregulated and have open-source code. Given this fact, it may be reasonable to make a suggestion that such availability may lead to a reduced level of security. However, this is not the only possible case of developing a crypto currency or any other blockchain based system. In a research carried out by Saint-Petersburg State University it is distinguished between 3 types of blockchain: open, closed and combined/exclusive. The key difference is that the first type is completely unregulated and open source code is available, providing more opportunities for certain people to compromise them. Second and third, in their turn, possess some kind of supervisory authority, like Ripple (Babkin, Burkaltseva, Pshenichkov, & Tylin, 2017). This difference may certainly influence the degree of trust in crypto currencies and therefore it is quite reasonable to differentiate between them in the research. From another perspective, this fact may not be very significant due to one problem – general lack of deeper awareness about crypto currencies. For instance, a survey conducted by Opportunity organization (which functions are comparable with LinkedIn) which included almost 2.000.000 participants may serve quite a representative example. For a better understanding of a context it worth noting that data has been collected in late 2017, at the peak of Bitcoin's popularity. Results were quite expectable: even though 90% of respondents have heard about Bitcoin, only a relatively small percentage has ever owned it - the figure was around 7%, while only 0,5% has ever used it to make an actual purchase. The process of purchasing Bitcoin had been called rather challenging by 60% of respondents out of that 7%, who has ever owned it. Alongside this, Opportunity asked its respondents to estimate an approximate level of understanding of how Bitcoin (= blockchain) technology works on a scale from 0 to 10. An average answer was 5.28 ("Cryptocurrency Survey," 2017). The fact that by far the most famous crypto currency is still not very understandable for a vast majority of the public may lead to a suggestion that crypto currencies of other types, differentiated in a paper of Babkin et al. are still very far from common awareness phase.

It may be also easily checked if one addresses Google Trends analytical instrument – the number of searches by "bitcoin" query exceeds the same number of "ripple" and "ethereum" sevenfold. Therefore, even though there are already developed ways to make crypto currencies more controllable and, to some extent, stable and secure – this fact cannot yet influence the common perception significantly. From a general crypto market perspective, this fact may be rather depressing, but there are positive outliers. For instance, Ripple (XRP) which could greatly capitalize during late 2017 increasing its price tenfold ("XRP (XRP) price, charts, market cap, and other metrics,"2019), attempted to at least maintain its reputation during early 2018 meltdown via certain PR and marketing activities like an instant transfer of a donation amounted 4 million USD, which was then immediately converted in Rwandese dollars (Ogono, 2018). Conventionally, such transfer would take up to several working days. Even though this move was not anyhow helpful in maintaining the token's exchange rate which felt down to a pre-December 2017 level, from the marketing perspective it had been rather indicative in a sense that Ripple is still a major crypto market participant (ranked #3 by market capitalization in March 2019) which is still completely functional and fulfills its functional purpose successfully. Noteworthy, Ripple represents a "combined" type of crypto currency, according to Babkin's classification, and may serve as a good example for the market.

At this point, it might be reasonable to address to and review other types of crypto currencies appeared on the market after Bitcoin. It is easier to refer to them as to “altcoins” – modification of Bitcoins source code in one or another way in order to surpass its initial limitations or adapt it to some specific purpose (Ong, Lee, Li, & Chuen, 2015). This overview would be based mostly on the article of Ong et al. (2015), which provided an in-deep analysis of altcoins potential on the market. To represent a reason why altcoins have emerged at all, we may address the most evident examples presented in an above-mentioned article. For instance, Bitcoins infrastructure and design in combination with exploding rates of growth throughout late 2017 has resulted in at least 2 serious mutually dependent limitations / issues:

1) Time of transaction may increase very significantly when a large number of them is in progress – the bottleneck is created due to necessity for all the transactions to pass through validation process called “proof of work (PoW)”
2) The above-mentioned validation process, in contrary to proof of stake process leads to a massive power consumption throughout the network as it requires hardware-powered calculations in order to create and validate the block. For instance, Bitcoins annual network consumption is even exceeding a power consumption of Bangladesh (“Bitcoin Energy Consumption Index,” n.d.) – a country with a population amounting to 164 million people, according to the World Bank.

Generally, Ong proposes a categorization system of Altcoins which is based on a degree of deviation compared to initial Bitcoin code, which is publicly accessible on the GitHub platform, and their ultimate purpose. They are divided into 5 categories (Ong, Lee, Li, & Chuen, 2015):

1) Coins with minor changes of parameter (Terracoin, 1xCoin)
2) Coins with technical innovation (Litecoin, Namecoin, Peercoin)
3) Coins coded in a different coding language (NXT based on Java)
4) Coins with new ideas (Counterparty, Ethereum, Mastercoin)
5) Appcoins (SWARM Coin, MaidSafe Coin).

At the point of the study addressed was conducted, there were 440 active altcoins on the market. Many of altcoins are designed to implement and thus test solutions which seem prominent in theory but are too radical or impossible to implement them as a modification of Bitcoin, due to an enormous amount of transactions and value concluded in it. For instance, Litecoin proposes even further decentralization of mining, introducing Scrypt instead of Bitcoins SHA256 hashing algorithm. Peercoin in its turn addresses the energy consumption problem replacing Proof of Work with a Proof of Stake validation method. ZCash and Darkcoin can be used in order to execute truly anonymous and traceless transactions. Appcoins could be the category of particular interest for our research, as they represent something in the middle between 2 categories of consideration, not being a payment method nor database, but combining some certain properties of both worlds, representing a method of collective owning of property, a kind of a digital stock in a "DAO" (Decentralized Autonomous Organization). Appcoins are sometimes sold in a crowdfunding manner on platforms like Kickstarter (Ong, Lee, Li, & Chuen, 2015). Unfortunately, their current market penetration and the level of general public awareness is rather low, and thus Appcoins are just a good phenomenon to know about and to examine in future researches, but they are not yet the application method trust in which may be measured and examined effectively. Regarding the safety & trust aspects, Ong et al. came to the following conclusions (Ong, Lee, Li, & Chuen, 2015):

1) The fact that creator (creators) of Bitcoin are still preferring to stay anonymous and are not disclosing their personality will remain very troubling to investors as they can not be certain in effective crisis management in extreme situations (e.g. 51% attack)
2) Standard econometrics methods are mostly inapplicable to Altcoins, as they are "at best explanatory and are hardly useful for ones investing large amounts in Altcoins" and thus "one should never bet anything that one cannot lose on altcoins until the issue of crisis management is addressed as that remains the biggest risk of this Bitcoin and altcoins experiment"

Such wording may seem effectively radical, but generally, it represents the common attitude towards crypto currency accurately, as it can be met across almost any source of information about crypto investing – from specialized websites to Telegram channels. Thus, for this research, it is crucial to find out whether that holds true for Blockchain 2.0 type of applications and whether this negative perception regarding crypto currencies holds true in 2019, 4 years after the addressed study was published. There are reasons and events which could have changed the situation – a boom of late 2017, ended up with a quick decapitalization and followed with a relative stabilization and moderate rise throughout late 2018 and early 2019. To examine if there had been any changes in the situation described above, it is reasonable to address comparable research carried out by Wang Chun Wei in the University of Queensland recently – in June 2018. Wei attempted to examine market efficiency and liquidity among 456 altcoins, comparing his results with a comparable study from 2016 carried out by Urquhart in 2016 and managed to draw several important conclusions from his study (Wei, 2018):

1) Overall market efficiency increased since 2016
2) Higher liquidity leads to more confidence across investors and thus lower volatility
3) Smaller altcoins exhibit mini "boom-boost" cycles, attracting speculators who are either overly pessimistic or optimistic
4) Generally, in higher liquidity quartiles of crypto currencies examined stability and confidence increased overall, while smaller altcoins still struggle to deliver an investment-appropriate behavior.

This research represents the consequences of global trends and tendencies towards stabilization and regulation of the crypto currency market – for instance, listing Bitcoin futures on CME (Chicago Metal Exchange) and CBOE (Chicago Board of Option Exchange), which not only attracts new institutional investors, but also enhances the confidence of existing ones (Foley, Karlsen, & Putniii, 2018). Relative stabilization of the exchange rate for major crypto currencies and less interest from the speculative part of investors may be also put on this list. Given that, it is possible to state that dynamics and trends are relatively positive for investors and therefore possible outcomes of this study are not as predictable as it might initially seem.

One of the biggest challenges crypto currencies have yet to overcome is a public image of technology which is often misused. This is a very significant barrier towards trust, but these are also two sides of the same coin – privacy with all of its benefits on one hand, and criminal use opportunities it provides on the other. One of the examples already mentioned in this paper are ICO scams, which may result in losses of enormous amounts of investors' money – and they are incredibly difficult to regulate according to recent European Banking Institute study (Zetzsche, Buckley, Arner, & FFhr, 2017). At this point it has to be mentioned that even though ICOs' underlying technology, a smart contract (to be discussed later in further detail) is definitely a Second Iteration technology, its most frequent use as a financial instrument with an intention to secure or multiply funds makes it necessary to relate it to FI of blockchain throughout this research.

From one perspective, ICOs are a very prominent mechanism for financing of innovative initiatives in countries where businesses lack free access to capital, or it is unaffordable. Furthermore, it is also representing a considerable percentage of start-up financing in US and EU amounting to 0,45% and 3,83% respectively, not to mention less developed countries where in many cases, as it has already been mentioned, there is barely any other way to access capital but crowdfunding of one or another form. From another – there are studies that indicated clearly: an amount of ICO scams is still very significant, amounting to 80% in nominal numbers (although "only" 30% in real money) in 2017 (Alexandre, 2018). Nevertheless, positive development dynamics may be noticed in this field – according to more recent 2018 study, only 1 out of 5 ICO had clear scam "red flags", e.g. fake executive teams, plagiarized investor documents or guaranteed returns ("ICO Scam," 2018). Therefore, appropriate regulation is currently a major milestone to achieve, in order to this mean of funding to institutionalize and become more opened and rather conventional for a majority of investors. Referring back to the EBI article, major regulation issues are indicated as following (Zetzsche, Buckley, Arner, & FFhr, 2017):

1) Difficulty to determine the responsible financial controlling authority due to international cross-border nature of ICO-related transactions
2) Difficulty in establishing a relevant jurisdiction as it is frequently uncertain where is the beneficiary of an ICO is domiciled
3) Only in a limited amount of countries, ICOs are covered by an existing regulatory framework.

In the concluding part of an above-referred study there is a very important conclusion drawn, which represents a quite significant factor for this paper: in case regulation measures are not introduced and aligned, investors' money will continue to flow in ICOs with highly uncertain prospects which feature very high risk of investors' money being lost. This, in its turn, will make investors less willing to participate in such ventures generally and thus actually responsible teams with great ideas which could have achieved financing via ICO only will have much fewer opportunities to get one (Zetzsche, Buckley, Arner, & FFhr, 2017). Up until middle 2019 when this paper is prepared, no any significant changes had happened regarding the regulations. Only significant attempt was made by Security Exchange Commission (SEC) of the US, which had implemented general guidelines on ICOs for investors and professional market participants, clarifying how the process had to be carried out in order to comply with the US legislation, effectively putting ICO tokens under the power of the Securities Act of 1933 ("SEC.gov | Spotlight on Initial Coin Offerings (ICOs)," n.d.). Still, these attempts do not solve the problem globally, as a vast majority of scam ICO activities had their beneficiaries outside of the countries with developed corresponding legislation.

Taking these factors into consideration it is possible to argue that compromised and to some extent, the flawed image of ICO will probably continue to harm such of crypto currencies in general, as for a significant amount of people these terms are closely associated. However, it is reasonable to hope that the situation will change over time as ICO investors and other market participants gain experience, while crypto investment field stabilizes and attracts fewer speculators resulting, as it had been evidenced above, in a lower amount of ICO scams in general. Furthermore, less hype-attracted and poorly educated investors with wrong motivation and little understanding of the market are taking part in ICOs, as it is now barely possible to achieve the same returns there had been in late 2017. This may be considered a positive factor as:

1) Less uneducated investors result in lower to none funding of the most controversial and scam-probable ICOs
2) The less money such investors lose, the less the amount of negative hype caused by WoM around the industry
3) More mature investors are likely to choose carefully when evaluating an investing decision, which again lowers the number of opportunities for ICO scam events to occur.

In process of assessing and analyzing crypto currency misuse issues which may negatively influence their public perception and approval, it is impossible to avoid the topic of digital currencies becoming an integral part of any modern black marketplace providing illegal goods and/or services. For the beginning it would make sense to present certain figures, reflecting on which role does Bitcoin play in black market transactions. An in-deep analysis of such role has been carried out by Foley et al. (2018), applying the knowledge about certainly illegal trade networks, building detection controlled estimation models on their basis. First of all, illegal activity was found to comprise a substantial proportion of all Bitcoin trading activity. To get more precise, around one-quarter of all users and almost half (44%) of all Bitcoin transactions are probably associated with illegal activity. In real terms, as of Spring 2017, around 24 million Bitcoin market participants were using it for primarily illegal purposes, executing around 36 million transactions with a turnover amounting 72 billion dollars (Foley, Karlsen, & Putniii, 2018). In total, these participants hold around 8 billion dollars' worth of Bitcoin. Nevertheless, for better understanding of the context is worth noting that the figures above represent the amount of Bitcoin holding addresses involved in suspicious and likely illegal transactions, not real humans. In order for these numbers to be relative to general black market figures, it is possible to address worldwide statistics on the drug market. For instance, a report to the US White House Office of National Drug Control Policy estimates that drug users in the United States in 2010 spend around 100 billion dollars on illicit drugs annually. For the EU, using a different methodology, analytics from the European Monitoring Center for Drugs and Drug Addiction came to the conclusion that the respective amount is close to 24 billion euro.

According to certain researchers and common sense, a very significant amount of illegal Bitcoin use is related to drug purchase or trafficking which may lead to a conclusion that the share of Bitcoin in illegal transactions concerning drugs varies somewhere below 5 to 20 percent of the drug market transactions are processed with Bitcoin. That is a very rough estimate, but in any case, those numbers are quite solid for such new technology (Janze, Christian, 2015). Still, there is one tricky thing associated with this calculation – Bitcoin is far from being the only cryptocurrency for black market transactions, especially If a user involved in the black market is interested in some more "exclusive" good or service, as Bitcoin transactions are perfectly traceable, yet somewhat anonymized. It means that Bitcoin wallet can contain several Bitcoin holding addresses, which are not traceable. Still, it is possible to link addresses belonging to the same wallet, especially when more than one address of the same wallet is used to make a purchase. Moreover, it is probable that the more popular Bitcoin becomes, formalizes and institutionalizes, the less will there is for criminals to use it. This phenomenon became more or less apparent when the researchers were able to detect an inverse relationship between the proportion of illegal activity in Bitcoin and the Google Search intensity of the "bitcoin" query. However, even though the misuse proportion had declined, in the absolute amount it has increased (Foley, Karlsen, & Putniii, 2018). Such effect may be compared with an effect of share delusion when a new volume of stocks is issued in a successful PLC, meaning that even though the proportion declined, the absolute number has been increasing – it happened due to massive growth in late 2017 and hype associated with it. In the same research, it had also been pointed out that Bitcoin has his "competitors" in this darker side of application scope. Competitors, that are far better at concealing privacy and user activity associated with them, e.g. Zcash, Dash, Monero – so-called shadow coins. Those are much closer to an image of a completely private and traceless way to process money flow executing not-so-legal activities. According to Foley, Bitcoin and other digital currencies are currently facilitating the same disruption in black commerce industry as the one PayPal has long ago facilitated in conventional e-commerce industry: it provides secure, to a large extent anonymous and relatively quick flow of money outside of legal system's scope. Unfortunately, it is not yet scientifically determined whether illegal use of crypto currencies on such a broad scale may anyhow influence perceived trust in them among the general public.

Still, even though numbers which are presented in the researches mentioned above are nominal – for instance, there actually is a 50% figure in estimation of total illegal activity related transaction proportion, but such transactions are usually much lower in value in comparison to a normal market transaction, etc., there is a high chance that an image of some utility to execute certain illegal activities will be associated with crypto currencies, decreasing the willingness to trust this technology, especially among ethically conscious people. Even from a pure investment grade perspective one may wonder about what happens if for some reason illegal business-related actors will abandon its use, and how strong will the influence of such an event be in respect to Bitcoins liquidity and market value. Lack of general regulation is a two-sided medal in this case just as it is with ICOs. From one hand, the low ability of the government to track crypto-currency related transactions leads to their misuse and facilitation of illegal activity, but on the other may still be the only chance to people suffered from some sort of governmental failure – whether it is economic or political (e.g. hyperinflation or political activism oppression via financial pressure). Fortunately, there are several suggestions regarding crypto currency illegal use which are rather beneficial for their image. The following theses are excerpts from an interview with a DEA (Drug Enforcement Agency) agent conducted in late 2018 ("Illegal Activity No Longer Dominant Use of Bitcoin," 2018):

- Use of Bitcoin in illegal activities had significantly shrunk and now does not exceed 10% of transactions thanks to increasing popularity of technology among the general public and therefore predominantly legal use
- Total transaction volume surged since 2013
- Liquidity of "shadow coins" is too low for significant black-market operations and therefore Bitcoin use is inevitable
- DEA claims that even though shadow coins feature enhanced privacy in comparison to Bitcoin, there still are feasible ways to trace their illegal use.

However, given the certain interest of the interviewed party in the subject discussed and a non-scientific essence of the source, these facts cannot be taken for granted. The only thing which is clear now is that future development and formalization of Bitcoin and crypto currencies, in general, will be rather beneficial for perceived trust in this technology, putting aside the factor of illicit use.

Another serious concern, which negatively influences the image of crypto currencies and their overall perception, is possible terrorist use of them. Quite a high degree of anonymity provided by "shadow coin" crypto currencies like ZCash makes it very tempting to use them unlawfully. A big report on this conducted recently by the Center for a New American Security (CNAS) states that virtual currencies are mostly used for the following purposes: buying and selling stolen data, exploits in dark web markets, drug and weapon trafficking and other similar illegal commercial activities (Goldman, Maruyama, Rosenberg, Saravalle, & Solomon-Strauss, 2017). That has already been examined in detail above. However, some researchers argue that in general, virtual currency terrorist use is very limited, mostly due to very poor telecom infrastructure in areas where terrorists are operating. Therefore, it is possible to conclude that terrorist use threat is rather reputational than real for crypto currencies, at least as for the moment of conducting this study. Still, one of the main aims of regulators and other governmental institutions is to prevent terrorists from using virtual currencies on a large scale (Goldman et. al., 2017), for such reputationally harmful precedents not to occur.

Having the above-presented information in mind, it is also useful to address an issue which is a part of every misuse case already discussed in this paper. To be precise, it is money laundering which is almost always a part of any criminal offense including a financial transaction in it. Certainly, due to many factors and aspects of functionality crypto currencies brings certain new features to this field. In order to examine them in a systematic way, and attempt to find any trust-related aspects it is reasonable to address a corresponding article from the book by Choo which included quite a comprehensive analysis of money laundering and benefits of applying crypto currencies in such an activity. First of all, it is important to understand the money laundering process itself. Choo made a division in 3 general and common steps in order to categorize it (Choo, 2015):

1) Placement Stage: money laundered introduces the corruption proceed into the financial system or acquires another form of value-containing assets like pieces of art, precious metals or, in case of our interest, digital currencies
2) Layering Stage: after the launderer has successfully placed the money in form of contributing them into the financial system or via purchasing of some other form of value-containing asset, one has to engage in a series of transactions in order to distance corruption proceeds from their original source. Conventionally, it is done via setting up companies registered for recruited individuals and forwarding money between a vast amount of them using contracts for non-existing goods or services as a reason for transactions. This forwarding may proceed until the

moment when the laundered funds become almost untraceable. Basically, the identical process happens in the case of crypto currencies, but it is even slightly easier: specially recruited people open up companies and purchase crypto currencies in an amount below the reporting threshold for given country, then forwarding them between digital wallets (accounts) up until it is, again, impossible to trace where did this money come from.

3) Integration Stage: Disguised (cleaned) funds appear in the financial system as if they had been legally earned. From this moment onwards, it is almost impossible to distinguish whether between legal and illegal wealth

Alongside categorization of main money laundering stages, Choo introduces a categorization of risks (for current regulators' procedures) which are associated with crypto currency use for money laundering in particular. Risks are categorized by steps (Choo, 2015):

1) *Near anonymity* of crypto currencies and absence of KYC procedures on certain exchanges means that literately anybody can open a crypto currency wallet despite being accused in frauds or terrorism – this is an issue concerning regulators the placement stage. During layering stage, it is not anyhow feasible to use special "black lists" of the financial system containing information about highly suspicious people, criminals or terrorists, making digital wallet transactions a safe zone for such user categories. At the integration stage, near-anonymity turns into a feature which allows to cash out the laundry proceeds anonymously and basically anywhere where the Bitcoin ATMs are placed.
2) *Elusiveness and high negotiability* enable launders to structure the proceeds of illegal activity into different accounts, avoiding triggering the reporting requirement if such exist at all – such opportunities ease the passing of placement stage a lot. Layering attempts also have much more chance to succeed as basically an unlimited number of wallets can be registered and therefore an endless amount of transactions can be executed as no any justification needed in order to initiate one. As of the integration part, there

is also an opportunity to withdraw fund from multiple wallets and accounts at the same time, which brings a lot of ease to a cashing-out process.

3) *Real time transaction and utility and withdrawal of funds* allows launderers to quickly deposit proceeds of crime and then transfer it to another account or currency in a different country. Again, it means that the placement stage of the laundering process is significantly simplified. At the same time, transactions occur mostly uncontrollably in real time, without a manual check of transactions, weekends and holidays, allowing little or no time to stop them in case there is a suspicion in money laundering, financing of terrorism or any other crime – this factor assists launderers a lot during the layering stage. Integration stage risks involve the ability of illegally obtained funds to be transferred rapidly across the system and be withdrawn from another account in a different country.

Information from the research examined above may serve a basis for the following assumptions. First of all, crypto currencies are very helpful for the public which seeks the unregulated financial system. Still, it does not automatically qualify them as criminals – there are many cases and situations, both social, political and economic, when a deregulated financial environment may help to overcome the unfair and anti-humane limitations imposed by a “legal” one. On the other hand – there is a variety of misuse scenarios which are influencing the image and public perception in a very negative way, are yet to be overcome. Moreover, overcoming these issues may appear to be almost impossible without a straight out ban of all decentralized currencies as monitoring and tracking the movement of funds which can be used for any inhumane and unethical business is still very difficult, if even possible. Certainly, the recent implication of obligatory Know Your Client (KYC) and Customer Due Diligence (CDD) in almost every major crypto exchange brings some order and an illusion of regulation, but there will always be a dozen of deregulated exchanges without those policies. It is practically inevitable without worldwide regulation. One factor can bring certain optimism to this discussion – the maturity of the technology and the digital currency market overall. The absence of this maturity, to be more precise. And of course, it would be rather biased not to add that massive regulation of conventional financial system on a worldwide scale was far from being a given thing until the beginning of 21st century which is, given its age, a very recent event. It is also worth noting, that major banking corporations have also been incriminated participation in worldwide money laundering and even terrorism financing schemes. HSBC example is one of the most recent ones with events taking place in 2012 when the bank was found guilty in money laundering of drug cartels, oppressive political regimes and even processing terrorism financing related transactions (Rushe, 2012).

2.2 Distributed registries / Decentralized Data Storage (SI)

At this point, the SI of blockchain technology is going to be examined. Blockchain 2.0 is going far beyond transaction providing systems/crypto currencies and there are many successful implications which are already in operation. In a recent journal article, Steve Mansfield-Devine defined blockchain as a “decentralized, cryptographically authenticated record of transactions” which perfectly demonstrates how broad the scope of application may be; furthermore, he argued that “It’s a bit unfortunate that it is so tightly bound with Bitcoin and financial services. Once upon a time, there was a reason for that. But its value really lies outside of financial services” (Mansfield-Devine, 2017). Still, before proceeding further it is important to introduce one more term which is integral for an understanding of some principle related SI of blockchain – a smart contract. According to the classic definition made by Vitaliy Buterin, one of the “founding fathers” of SI blockchain V who created Ethereum, a smart contract is “a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated” (Buterin, 2014). To put it in more simple words, a smart contract defines the rules and obligation which involved parties must follow and according to which the contract executes automatically. The easiest example of a smart-contract in real life practice may be some crowdfunding activity. Conventionally, crowdfunding has been carried out by trusting the funds to certain 3rd party intermediaries, like Kickstarter. Money is collected by an intermediary until:

a) The target amount is reached → funds are transferred to fund seekers
b) The maximum time of reaching the target amount passes by, while the target amount is not reached → funds are transferred back to funders.

Smart contracts can be used (and are already used successfully) to replace that intermediary via operating two variables – target amount of funding (X) and the maximum time allowed (Y) to collect the target amount, in our case. In theory, the number of variables is unlimited which allows using smart contract even in highly complex scenarios. Another term it would be useful to introduce is a distributed ledger, usually referred to as just "ledger" in blockchain related discussions. Ledger is "a database that is consensually shared and synchronized across multiple sites, institutions or geographies. It allows transactions to have public "witnesses," thereby making a cyberattack more difficult. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it" ("Distributed Ledgers Definition," 2019).

In the article by Mansfield-Devine which was already mentioned above, a remarkably advantageous use case is investigated – technical maintenance of an aircraft. It is much easier and more secure to use blockchain to register all the repairs and maintenance operations for thousands of details of an aircraft, rather than trust it to standard maintenance journals. It is impossible to re-write anything or to simply lose such a registry during a sale of an aircraft, for example. It ensures that all parts are treated on time and everything is in order – which is crucial for aircraft operation. For instance, it is quite normal for a major airline to have literally billions of parts, which they have to track and easily access in case of some maintenance need or if the malfunction is detected. They are usually stored or installed in a different location, while many of them (e.g. some fundamental parts like fuselage structure parts or sophisticated plane-specific systems) are to stay with an airline for decades, yet have to be monitored and serviced. Inevitably, that need results in a huge amount of paperwork and massive databases. Everything complicates even further given an airlines incentive to offshore the maintenance of certain parts and even modules (e.g. landing gears). Overall, that involves a lot of certified parties which have the authorization to manipulate such sensitive things as aircraft parts, plenty of signatures and trust. Patrick Hubbard, an aviation industry specialist shared an interesting perspective on the given topic: "Blockchain gets particularly interesting when you look at multiple assets that are interacting, each of which needs to be assured. If you think about the complexity of not just maintaining a part but a whole series of parts for an aircraft … well, that is ripe for blockchain technology", he concluded (Mansfield-Devine, 2017).

To consider the governmental operation of blockchain based technologies, it is indeed interesting to address research of Ølnes et al., examining its possible implications, benefits, and challenges. The researchers have concentrated mostly on the issues which are likely to be faced when the mass implementation of blockchain is started. In particular, they have focused on governmental agencies implementation scenarios as the article was designed to be published in the Governmental Information Quarterly journal. It is mentioned that governmental blockchain application scope is very diverse, among them are digital identity, the storing of judicial decisions, financing of school buildings and tracing money, marital status, e-voting, business licenses, passports, criminal and tax records (Ølnes, Ubacht, & Janssen, 2017). At this point, it could be reasonable to address some scenarios which are described in detail. As it has been mentioned above, smart contracts can be used in cases where there are many variables and contract participants. Such implications are presented beyond (Ølnes, Ubacht, & Janssen, 2017):

- *Granting permits of organizers of mass events* (e.g. concerts, demonstrations, etc.). In this case, all the possible parties involved have to clarify and approve that they are ready for an organization of the event. It may include approval from fire brigades, municipality, respective police station, a relevant health organization.
- *Transfer of car ownership* is a relatively simple example, as it refers to only 3 parties: car owner, who was to authorize permission to sell a car, car buyer, who has to confirm he intends to buy it and a bank who shall confirm that the transaction of funds has been executed successfully.
- *Blockchain Technology use for land title ownership* is also a very tricky use case as it includes many parties and authorized date involved. First of all, it is supposed that all the transactions have to be already recorded in the blockchain based system. Besides the confirmation from lawful seller and buyer, an authorization from a relevant layer is required, and beyond that, an authorization from a land registry that there is no mortgage rest on the

property. Of course, transaction confirmation from a bank is required as well.

For sure, each of the implications has to be treated separately, and lack of uniformity is considered as a certain disadvantage. That means, it is almost impossible to make a uniform blockchain based system which will address all the government needs and requirements. In order to transfer all such operations and procedures on a blockchain, an integration of multiple blockchain based registries, addressing different needs (e.g. land registry, citizen database, etc.) has to be implemented. According to Ølnes et al., for successful implementation, two perspectives have to be considered (Ølnes et al., 2017):

- *Governance by Blockchain* – which is basically a process of conscious blockchain adoption in public institutions. It proclaims that when governments are to develop a blockchain based system, it requires knowledge of design options in order to apply the appropriate type of blockchain architecture.
- *Governance of Blockchain* – which determines how the technology operates, and how end users are supposed to interact with it. Normally, there should be a few experts who determine and enforce the rules according to which the application governs the user, while policy-makers are supposed to play integral role in ensuring that public values, ethical standards, and social needs are fulfilled and are taken into account during the process of design and implementation of blockchain based architectures and applications.

Certain governments have already implemented blockchain for their commercial and some other registries; those have already been mentioned in the introduction. The more governmental solutions appear, the more trustworthy blockchain is expected to be, in public perception. Such awareness in case of system's successful operations has to be beneficial for the technology as a whole. Research conducted by a group of China-based scientists confirms the large scope of possible blockchain based application scenarios and indicates the following categorization of them (Wang, Zheng, Xie, Dai, & Chen, 2018):

- *Finance*, including enterprise transformation, financial services, p2p financial markets, and risk management
- *IoT*, which is going to be discussed later in more detail
- *Public and Social Services,* including already familiar land registration, education, energy saving, and free-speech right
- *Reputation measurement system,* which might be very useful for the web community in general and academics in particular.

One of the prominent and important scenarios is the successful integration of blockchain based services with IoT. Examining it is particularly important for this study, as both technologies are relatively new, while the IoT is considered to be the next "big thing". If integrated and applied successfully, blockchain based technologies may gain a considerable increase in credit and trust. Internet of Things – a concept steadily becoming a reality is expected to generate huge flows of additional data, just as 5G-networks are already starting to develop on the consumer level, and in not so distant future are expected to become an industry standard. A study conducted by the University of Malaga points out several significant improvements, which can be implemented via such technological collaboration. In the foregoing section, the most important ones are presented with a brief description of each (Reyna, Martín, Chen, Soler, & Díaz, 2018):

1) *Decentralization and scalability* – allow to remove central points and bottlenecks, prevent excessive corporate control over data
2) *Identity* – ability to identify every single device participating in a system
3) *Autonomy* – the ability of devices to operate without the involvement of any servers
4) *Reliability* – participants of the system are capable to verify the authenticity and validity of the data
5) *Security* – information and communications are highly secured when the transactions are stored in a blockchain.

Furthermore, according to another study, Blockchain technology provides better flexibility in accessing the data and is identified as one of the solutions for addressing the issues and challenges in IoT. Essentially, blockchain was called "one of the "remedies" for addressing security and privacy issues in IoT, as it disintermediated the most potentially vulnerable security point – the data interchange between the device and a centralized server. Blockchain integration with IoT will allow for seamless flow of data through blockchain distributed ledger ensuring each transaction an appropriate authentication (Kumar & Mallick, 2018). That aspect might be particularly important, as public sight has once already been concentrated on a huge IoT-related security flaw when millions of webcams worldwide appeared to transmit data not involving any kind of security protocol and therefore were possible to be accessed by virtually everyone on the Internet. It may be relevant to address some prominent implementation scenarios of blockchain technology being integrated with IoT, applied mostly in shared economy setting. For this purpose, a study conducted at the University of Sussex will be addressed. It provides 3 quite interesting examples (Huckle, Bhattacharya, White, & Beloff, 2016):

1) *AutoPay* – a service which integrates with car onboard computer, parking service providers, gas stations, and other road-related services in order to seamlessly help the user make the autonomous and secure payments for everything which the system recognizes the need of.
2) *Peer-to-peer FOREX application* for left-over foreign currency (LFC). It is estimated, that in the UK only, almost 3 billion pounds of foreign currency remaining unused due to post-travel leftovers. Usually, exchange offices do not provide a fair exchange rate for a relatively low amount of money – so unfair, that many people prefer just to put it in the cupboard. Blockchain based system enabling special ATMs, where you initiate a smart contract, indicating the preferred exchange rate and depositing the money, and mobile application, which will allow users to provide smart-contract ensured FOREX transactions at a mutually-acceptable exchange rate.
3) *Digital Rights Management System* which would allow musicians and other content-producers to determine the conditions under which they allow to use their content. It will allow overcoming the somewhat flawed current content distribution system which makes it barely possible for musicians not signed by major studios to earn money via distributing their content online. An interesting example was outlined in the study – a musician who is listed on Spotify has to reach 1.1 million streams of his records in order to earn a minimum salary in the US amounting 1,240$.

These aspects and ways of application may appear to be trust enabling for public and become quite crucial for the general perception of the technology. IoT-related scope of applications, which are already created in the form of certain platforms and services, is also presented in the study by the University of Malaga, among them: identity verification, e-government, verification of ownership, e-health, product-traceability, cloud storage, renting sharing and selling, etc. (Reyna et al. 2018).

However, the current level of development of IoT to Blockchain integration includes a significant level of risk and a vast amount of challenges. Security risks have been examined in detail in a research conducted by scientists from the Khalifa University of Science, UAE. In that study, a detailed categorization of risks has been introduced – it is even too sophisticated to be examined in this paper. To get at least general perception it is reasonable to mention that there were more than 5 dozen of possible risks indicated including critical ones, and none of the current platforms is able to address all of them. Regrettably, it remains a barely solvable challenge to design a system which would be reliable, efficient and most importantly saleable to address all the requirements of IoT infrastructure (Khan & Salah, 2018). Another study examining blockchain based IoT services carried out by researchers from the University of Malaysia also provides a very wide perspective on main implementation challenges. Positively, this research could categorize these challenges in a simpler way, therefore it makes sense to present the key finding relevant to us here, in order for better understanding (Kumar & Mallick, 2018):

- *Limitation with storage facility:* in the IoT ecosystem, the storage capacity required for sensors and other appliances is very much less than the one required for the ledger based blockchain technology. Conventionally in IoT, single central storage is facilitated, while in blockchain based systems each ledger must be stored at its own node. That increases the required storage size significantly
- *Lack of skilled workforce in the fields:* Skilled workforce is very limited in the field of conventional IoT. If it is combined with a requirement to be proficient in the field of blockchain, the already limited number of professionals shrinks dramatically

- *Legal issues:* The technology, in general, is still very modern, there are no legal codes to follow yet. In the discussed research, this is distinguished as the most important barrier to overcome
- *Variation in computing capabilities:* the technical specifications and thus computational capabilities are very diverse across current IoT solutions. At the same time, the need for running the encryption is essential for all the things that are going to be connected to the blockchain based IoT system, which can result in incapability and incompatibility issues.
- *Processing time:* results from the previous point. As computational capabilities vary significantly, the time to perform the encryptions would vary leading to variations in processing time
- *Scalability:* According to researchers' opinion, scalability may lead to centralization, and in this case, the very point of using blockchain technology would be compromised.

Still, not to be overwhelmed with the above-mentioned limitations, it worth noting that blockchain, in general, is an innovative general-purpose technology, offering fundamentally new ways for recording transactions in almost any industry or organization the one reading can imagine. Certainly, due to a very immature stance of technology, it is only possible to observe an abundance of the application scenarios in private sectors, but as it has already been indicated above, e-government applications even in very sensitive fields are possible (Ølnes, Ubacht, & Janssen, 2017). Due to many reasons, the relative difficulty of implementation, in particular, the possible gains are not easy to realize but the overall societal benefit from it is far too promising to be avoided.

In conclusion of this section, it is reasonable to address to a paper directly dealing with limits of trust-free systems, published in the Journal of Electronic Commerce Research and Applications. It is suggested to measure trust as an individual's belief that a platform is honest, reliable and competent based (Ba and Pavlou, 2002 cited in Hawlitschek et al., 2018). Given many concerns (Veuger, 2018) regarding use of blockchain expressed by authors of the majority of above-mentioned papers and articles, same dimensions will be used in this paper to evaluate perceived trust in FI and SI blockchain technology application scope. Taking into account the conceptual difference between FI and SI blockchain applications presented above it is still considered reasonable to divide them during the trust evaluation process in this research. Evaluating trust in such a modern and not yet generally familiar technologies may be rather tricky, but just as with crypto currencies and FI of blockchain, the two-sided bias may be monitored at the SI of blockchain which can lead to particularly interesting outcomes of the given study. Certainly, those are not the same reasons which underlie the difference in attitudes towards FI and SI of blockchain, but measuring the variation of perceived trust in them may be crucial for understanding the public opinion and very much helpful in deciding on further development direction for blockchain-based technologies in general. Ironically enough, trust-free systems are very unlikely to develop without public trust in them.

3 Research Method and Design

3.1 Data collection and analysis procedures

Survey research has been chosen as a method of data collection. The purpose of survey research is to "generalize from a sample to population so that inferences can be made about some characteristic, attitude or behavior of this population" (Babbie, 1990). In the case of the proposed research, we would evaluate an attitude, e.g. trust. Cost-effectiveness and a rapid turnaround are major arguments that make this instrument most preferable for this research, alongside that it ensures that all data gathered from participants is coherent and has uniform dimensions (Fowler, 2002). The survey will be cross-sectional with data intended to be collected at one point in time. The period of collection is March/April 2019. A closed-ended questionnaire includes several types of questions – that will allow more flexible analysis. They will include dichotomous, bipolar and rating / Likert-scale questions. Questions will be divided into two sections. First of them will survey on trust matters in regards to blockchain technology as a mean of payment and value based assets. The second one will survey on other, SI implications of blockchain, mainly on its capability to serve as a decentralized / distributed database. Results will be assessed and compared. More precise information on the format and theoretical justification of questions and methodology are to be provided further in the paper, in part 3.3.

Convenience sampling is considered to be the most reasonable for this research as it will allow obtaining a greater number of respondents in a limited timeframe. Limitation of a timeframe for gathering responses is considered reasonable in order to minimize the possible influence of media coverage on the respondents' attitude to the research topic. Convenience sampling is likely to provide a sample which would be sufficient to analyze data and gain remarkable insights in spite of differences in perceived trust among the population. The number of respondents reached in order to consider the sample size sufficient for this research is set at 100+. Generally, it should be possible to refer to different age and gender groups, differentiate survey participants by their level of education and place of residence. Data will be analyzed with SPSS Statistical Software using the following tests: parametric t-test and non-parametric Wilcoxon. Descriptive statistics and linear regression are to be applied as well.

3.2 Theoretical framework

In this research, from the theoretical perspective, it is firstly crucial to point out what type of trust we are considering. In Mr. Rompf's paper on The Concept of Trust, the trust itself has been divided into two broad fundamental categories: the objective structure and subjective experience of it (Rompf, 2015). Due to a fact that this research is going to be concentrated on perceived public trust in the blockchain-based technologies, it would make little sense to measure the objective structure of trust in the blockchain. That would involve excellent technological expertise and deep analysis with paying little or no attention to actual public perception. Therefore, the paper's theoretical background will be based on the subjective experience of trust, which is defined as "the internal mental state associated with trust" (Rompf, 2015). Another, more precise definition of trust may be presented in following way: "It is a multilayered and complex research topic, difficult to delineate and divergently addressed across disciplines (Rousseau, Sitkin and Burt, 1998, cited in Hawlitschek, Notheisen, & Teubner, 2018). However, a common element in various trust definitions is "[...] the intention to accept vulnerability based upon positive expectations [...]" (Rousseau, Sitkin and Burt, 1998, cited in Hawlitschek et al., 2018)." Alongside that, it would be interesting to address studies which can widen the perspective on trust being related to ICT, e-commerce in particular. Here two studies are going to be examined as they were deemed to be rather relatable to the topic of the given research. A. Duane et al. discussed the aspect of trust in detail in the study on development perspectives of mobile payments using handset devices, what can be considered closely related to blockchain use as a medium of exchange, e.g. crypto currencies. Initially, it has been pointed out that perceived trust towards an online service is an important determinant in considering its usage (Chau et al. 2007, Roca et al. 2008, cited in Duane, O'Reilly, & Andreev, 2014) and is a fundamental and most important prerequisite for the technologies adoption (Sanchez-Franco and Rondan-Cataluna, 2011, cited in Duane, O'Reilly, & Andreev, 2014). Several possible reasons for that have been indicated in the above-mentioned article, however, one of them is noteworthy for this research. Lie et al. has proven that trust is crucial in mobile commerce, given that buyer-seller transactions are often anonymous and lack formal contractual agreements (Lie et al., 2010, cited in Duane, O'Reilly, & Andreev, 2014). Such concerns are very significant for crypto currencies, and the FI of blockchain technologies altogether, when they are intended to be used as value containing assets or a medium of exchange. In the above-cited research, seven "manifest" variables of trust were indicated (Duane, O'Reilly, & Andreev, 2014):

- *Perceived Security Control:* shortcomings in security control reduce consumers trust and slows down the emergence of existing systems
- *Perceived Privacy Control:* also, a very important factor, as consumers tend not to share any personal or financial information
- *Perceived Integrity:* if a user perceives a vendor or service as honest and of high integrity, their intention to use will be stronger
- *Perceived Ethical Commitment:* perceived levels of this trust dimension heavily influence an online purchasing decision
- *Perceived Compliance:* it is suggested that online vendors are able to minimize uncertainties in case they comply with all the required regulations
- *Perceived Governance*
- *Perceived Independence of Regulatory Authority.*

As a matter of fact, all the dimensions listed above are perfectly applicable for the subject of this research and indeed address the concerns which had been pointed out in the literature review. To be more precise, security control, perceived ethical commitments, perceived compliance and the perceived governance represent the major possible trust disablers, while perceived privacy and perceived independence from regulatory authority may, on the other hand, ensure the perceived trust in crypto currencies. The factor set differs significantly for the SI of blockchain, but generally, an evaluation of trust based on the above-mentioned dimensions may be quite appropriate for purposes of this research.

3.3 Theoretical background of survey

Theoretical outlines discussed above in detail, and considered appropriate for the purpose of this research, have in a very similar way been transformed and synthesized in a complete and self-sustaining methodology in a study by McKnight et al., 2002. This study, which proposes a sophisticated model of examining trust in web-services, will serve a backbone for the design of the questionnaire for this survey research. Even though web-services are in fact a part of e-commerce concept, it is noticeable that motivation underlying the development of a trust-measurement scale is rather similar to the research by Duane et al., addressed in part 3.2. To be more precise, it has also indicated security, privacy, and ethical concerns, lack of trust to vendors who collect data and pointed out the fact that lack of trust can be an issue, preventing the technology from further development (McKnight, Choudhury, & Kacmar, 2002). In this research, the questionnaire will be based on an adapted version of "Web Trust Model" and a corresponding questionnaire developed in the study by McKnight. It included 5 main factors: Disposition to Trust (I), Institution-Based Trust (II), Trusting Beliefs (III), Trusting Intentions (IV), and Trust related behaviors (V); factors I and II are interconnected with each other and are directly influencing factor III, which in its turn directly influences factor IV, also partially dependent on factors I and II. Factor V is solely dependent on factor IV (McKnight, Choudhury, & Kacmar, 2002). It has been considered rational to concentrate on factors III and IV, as they represent aspects of subjective trust this research is focusing on, e.g. "perceptions of specific Web vendor attributes" and "intention to engage in trust-related behaviours with a specific Web vendor" respectively (McKnight, Choudhury, & Kacmar, 2002). Other reasons under lied the decision to take only these factors into account were (McKnight, Choudhury, & Kacmar, 2002):

- Simplification of the final questionnaire from the respondent perspective
- The relative ease of partial adoption of existing valid questionnaire present in McKnight's research, by adding contextual and minor linguistical changes
- Thus, eliminating the need in re-validation of the questionnaire.

Factors which are to be examined, e.g. Trusting Beliefs and Trusting Intentions, have been divided by McKnight into further sub-factors:

- *Trusting Beliefs*: Competence Belief, Benevolence Belief, Integrity Belief
- *Trusting Intentions*: Willingness to Depend and Subjective Probability of Depending

A further step was to adopt the model questionnaire from McKnight's study in order to make it applicable for the purpose of this research. Main adjustments were made mostly in an expressional sense, while 3 questions were removed due to lack of possibility to adopt them accordingly to this research, without implementing significant modifications. The questionnaire was duplicated with 2 sets of adjustments to serve the purpose of surveying trust in FI and SI of blockchain. The wording was simplified as significantly as it has been possible so it would be quite easy to understand for the general public. Introduction message was also added to present the survey topic to respondents. In the conclusion of a questionnaire, a demographic section was set up to allow for further stratification. Below one can find the structure of a questionnaire, table of changes made to the model questionnaire, alongside with content of the introductory and demographical section.

I) Introductory part

"Hello! My name is Grigory Shkrbich and I am a Bachelor student at MODUL University Vienna. This questionnaire is part of my Bachelor thesis. It is about trust in different forms of blockchain applications and it will take 7 to 10 minutes to fill it out.

In this questionnaire I refer to two common applications of Blockchain – crypto currencies and decentralized data storage.

The best example for the former is Bitcoin, which can be used as a payment service or to store value.

Decentralization allows to store data in many places at the same time and makes the data immutable. This means that it is almost impossible to modify the data.

All the data collected is used for research purposes only and will only be published in an aggregated form. Thank you very much for your support!"

II) Model Questionnaire Modifications

Trusting beliefs (benevolence); Blockchain 1.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_1.1.1	I believe that LegalAdvice.com would act in my best interest.	I believe that cryptocurrencies would act in my best interests.
~~Var_1.1.2~~	~~If I required help, LegalAdvice.com would do its best to help me.~~	~~If I required assistance, cryptocurrencies would do their best to help me.~~
Var_1.1.2	LegalAdvice.com is interested in my well-being, not just its own.	Cryptocurrencies are beneficial for the whole society, not just their own creators.
Trusting beliefs (integrity); Blockchain 1.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_1.2.1	LegalAdvice.com is truthful in its dealings with me.	Cryptocurrencies are truthful applications.
Var_1.2.2	. I would characterize LegalAdvice.com as honest.	I would describe cryptocurrencies as honest.
~~Var_1.2.3~~	~~LegalAdvice.com would keep its commitments.~~	~~Cryptocurrencies would keep their commitments.~~
Var_1.2.3	LegalAdvice.com is sincere and genuine.	Cryptocurrencies are sincere and genuine.
Trusting beliefs (competence); Blockchain 1.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		

Var_1.3.1	LegalAdvice.com is competent and effective in providing legal advice.	Cryptocurrencies are effective in providing payment services and storing value.
Var_1.3.2	LegalAdvice.com performs its role of giving legal advice very well.	Cryptocurrencies are providing effective payment services and value storage.
Var_1.3.3	Overall, LegalAdvice.com is a capable and proficient Internet legal advice provider.	Overall, cryptocurrencies are capable and proficient in providing payment services and storing value.
Var_1.3.4	In general, LegalAdvice.com is very knowledgeable about the law	In general, creators of cryptocurrencies are very knowledgeable about finance.
Trusting intentions (willingness to depend); Blockchain 1.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_C1.1	When an important legal issue or problem arises, I would feel comfortable depending on the information provided by LegalAdvice.com.	When an important financial transaction has to be executed, I would feel comfortable depending on cryptocurrencies.
Var_C1.2	I can always rely on LegalAdvice.com in a tough legal situation.	I can always rely on cryptocurrencies in a tough financial environment.
Var_C1.3	I feel that I could count on LegalAdvice.com to help with a crucial legal problem.	I feel that I could count on cryptocurrencies executing crucial financial transactions.
	~~Faced with a difficult legal situation that required me to hire a lawyer (for a fee), I would use the firm backing LegalAdvice.com.~~	~~N/A~~
Trusting beliefs (benevolence); Blockchain 2.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_2.1.1	I believe that LegalAdvice.com would act in my best interest.	Decentralization would act in my best interest.
~~Var_2.1.2~~	~~If I required help, LegalAdvice.com would do its best to help me.~~	~~If I required assistance, decentralized services would do their best to help me.~~
Var_2.1.2	LegalAdvice.com is interested in my well-being, not just its own.	Decentralized services are beneficial for the whole society, not just their own creators.
Trusting beliefs (integrity); Blockchain 2.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_2.2.1	LegalAdvice.com is truthful in its dealings with me.	Decentralized services are truthful applications.
Var_2.2.2	. I would characterize LegalAdvice.com as honest.	I would describe decentralized services as honest.

~~Var_2.2.3~~	~~LegalAdvice.com would keep its commitments.~~	~~Decentralized services will keep their commitments.~~
Var_2.2.3	LegalAdvice.com is sincere and genuine.	Decentralized services are sincere and genuine.
Trusting beliefs (competence); Blockchain 2.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_2.3.1	LegalAdvice.com is competent and effective in providing legal advice.	Decentralized services are effective in storing information securely and reliably.
Var_2.3.2	LegalAdvice.com performs its role of giving legal advice very well.	Decentralized services perform their role of secure and reliable information systems very well.
Var_2.3.3	Overall, LegalAdvice.com is a capable and proficient Internet legal advice provider.	Overall, decentralized services are capable and proficient information systems.
Var_2.3.4	In general, LegalAdvice.com is very knowledgeable about the law	In general, decentralized services creators are very knowledgeable about information systems.
Trusting intentions (willingness to depend); Blockchain 2.0	**Original Item**	**Modified Item**
(McKnight, Choudhury, & Kacmar, 2002), p. 355		
Var_C2.1	When an important legal issue or problem arises, I would feel comfortable depending on the information provided by LegalAdvice.com.	When it is required to store or access sensitive data, I feel comfortable depending on decentralized services.
Var_C2.2	I can always rely on LegalAdvice.com in a tough legal situation.	I can always rely on information stored in decentralized services, even in making tough decisions.
Var_C2.3	I feel that I could count on LegalAdvice.com to help with a crucial legal problem.	I feel that I could count on decentralized services to help me with storing crucial information.
	~~Faced with a difficult legal situation that required me to hire a lawyer (for a fee), I would use the firm backing LegalAdvice.com.~~	~~N/A~~

III) Demographical Section

Variable Name	**Question**	**Question type**
Var_AGE	Please, specify your age.	Short Answer
Var_GENDER	Please, specify your gender.	Multiple Choice (M/F/NS)

Var_RESIDENCE	Please, specify your place of residence.	Short Answer
Var_EDUCATION	Level of education:	Multiple choice (BSc/BBA/MSc/PhD/High school diploma

Above presented version of a final questionnaire has been approved by the supervising body and distributed to respondents. According to the feedback of certain respondents, no any significant difficulties or inconveniences were reported, even from respondents who are not well informed about the topic.

4 Data Analysis

At the beginning of this part, a brief overview of the sample will be presented. The data has been collected through Google Forms in the period from 21st of March until 5th of April. The overall number of respondents took part in the survey is 109, which has fulfilled the requirements stated by the supervising body. SPSS Statistics ver. 24 software was used to run the tests. Certain replies in the demographic section have been combined to more general variables in order to allow for running tests which require a significant number of group members in order to be more representative and valid. The generalization has been carried out in the following way:

- Age: 2 groups were formed: respondents above 30 years old and respondents below 30 years old
- Residency: countries of residence of respondents were divided into 2 categories: CIS countries (Armenia, Belarus, Kazakhstan, Kirgizia, Moldavia, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan) and OECD countries
- Education: respondents were grouped and divided into 3 categories, according to a level of education they have obtained: High school, BBA/BSc, MSc/Ph.D.

Demographically, the sample represents the following public:

- 71 females (65%), 35 males (32.1%), 3 people preferred not to specify their gender (2.8%)
- 85 of them were below 30 years old (78%), 24 were above (22%)
- 71 of them were residents of CIS countries, and 38 has been from OECD countries. In relative numbers, it has been 65.1% and 34.9% respectively.
- 65 people had either BSc or BBA degree (59.6%), 26 were either MSc or Ph.D. (23.9%), while 12 had only High School degrees in possession (11%). 6 people preferred not to specify their level of education (5.5%).

Alongside above-discussed modifications, a grouping of replies was conducted according to aspects of trust the reply represents. The detailed grouping methodology is explained beyond:

- Var_1.1.1 and Var_1.1.2 were combined into variable Var_FI_TBb in order for it to represent benevolence aspect of trusting beliefs into FI of blockchain.
- Var_1.2.1, Var_1.2.2 and Var_1.2.3 were combined into variable Var_FI_TBi in order for it to represent integrity aspect of trusting beliefs into FI of blockchain.
- Var_1.3.1, Var_1.3.2, 1.3.3 and Var_1.3.4 were combined into variable Var_FI_TBc in order for it to represent competence aspect of trusting beliefs into FI of blockchain.
- Var_C1.1, Var_C1.2 and Var_C1.3 4 were combined into variable Var_FI_TIwtd in order for it to represent willingness to depend aspect of trusting intentions into FI of blockchain.

Combination has been executed using the following formula: *(Var_X.X.X + Var_X.X.Y + …) / number of variables.* An identical manipulation has been carried out for variables measuring the level of trust into the SI of blockchain (ones written in format 2.X.X). All the data in raw format, alongside with easily readable tables can be found in the Appendix section of this research (Appendix A). Such grouping allowed to analyze whole aspects of trust, instead of digging into each and every question. In further analysis, this will allow understanding which aspect of trusting beliefs is the most influential on certain demographic groups and the sample in general. The finalized version of the dataset can be found in the Appendix under

“GSBT002” supplement ID (Appendix B). In order to structure the data analysis part logically, it will be arranged in a way to answer the Research Questions consecutively. In section 4.2, advanced testing procedures are examined.

4.1 To what extent do people trust in blockchain-based systems?

In order to answer the first question, combined variables of trust aspects to the FI and SI of blockchain, e.g. Var_FI_TBb, Var_FI_TBi, Var_FI_TBc, Var_FI_TIwtd were addressed. Special attention has to be paid to the latter one, as it is designed to represent an actual readiness of people to use the technology. On a scale from 1 (negative) to 7 (positive), mean score results were the following:

	FI	SI	Δ
Benevolence (TBb)	4.11	5.11	1.00
Integrity (TBi)	4.23	4.93	0.70
Competence (TBc)	4.01	5.00	0.99
Willingness to Depend (TIwtd)	3.05	4.29	1.24

(Table 1. Combined mean scores on a Likert scale derived from a survey research. Categorized by blockchain technology iterations and aspects of Trusting Beliefs and Trusting Intentions.)

Even though Trusting Beliefs related aspects in the FI have been evaluated in a cautiously-positive way, Trusting Intentions related aspect was evaluated quite negatively, as to a score below average (3.05). This can be interpreted as a generally cautious attitude towards crypto currencies which are the most conventional example of the FI of blockchain. In case of the SI, it is noteworthy that the relation of Trusting Beliefs to Trusting Intentions is basically the same as in the case of FI of blockchain – benevolence, integrity and competence aspects are all around 1 point higher (0.7, 0.99, 1.00) than the resulting willingness to depend aspect. Nevertheless, it can be concluded that perceived trust toward SI of blockchain is on the positive side of a scale. Overall, trust in the SI can be considered of a moderate extent.

4.2 Advanced Testing Procedures

Detailed answer on the following RQs requires significantly deeper analysis. In order to evaluate the significance of the difference in the extent of trust and its aspects among overall sample and demographically stratified groups, it was decided on running parametric/non-parametric tests (depending on the normality of distribution), designed for 2 related groups. These are non-parametric Wilcoxon (in case of normal distribution violation) and parametric Paired-Samples t-test (in case of normal distribution). Normality of the distribution was evaluated with a visual inspection of histograms combined with Kolmogorov-Smirnov tests. In order to determine the most influential aspects of Trusting Beliefs in regards to Trusting Intentions, regression analysis has been applied. Detailed results of all the analysis procedures described can be examined in the spreadsheet attached in the Appendix section (Appendix A). It is marked as "Supplement ID: GSBT001". Generally, tests were divided into the following categories:

I) *Group Difference Testing*, where the significance of the difference between paired samples was examined by running Wilcoxon test / Paired Samples t-test. It included determining:

- difference in TB (benevolence, integrity, and competence) and TI (willingness to depend) aspects towards FI and SI of blockchain among the whole sample
- difference in TB (benevolence, integrity, and competence) and TI (willingness to depend) towards FI and SI of blockchain, distinguishing between the stratified categories of a sample (e.g. age, gender, etc.).

II) *Linear Regression Analysis,* attempted to distinguish the most important predictor variable among TB aspects (benevolence, integrity and competence), which influences respondents TI aspect (willingness to depend) the most. It included an analysis of:

- influence of predictor variables on TI (willingness to depend) aspect towards FI and SI of blockchain among the whole sample
- influence of predictor variables on TI (willingness to depend) aspect towards FI and SI of blockchain, distinguishing between the stratified categories of a sample (e.g. age, gender, etc.).

4.3 Does the extent of public trust differ between two iterations of blockchain technology?

Group Difference Testing basically assured a logical suggestion from the answer on the first RQ, which is easily deducible due to a high delta of TIwtd (1.24) between FI and SI. It determined that Trusting Beliefs and Trusting Intentions differ significantly between FI and SI of blockchain when the whole sample is evaluated without stratification (p-values for all TB and TI aspects were <0.01 in these tests). The model hypothesis* for these tests was:

> H1: There is a significant difference in TB(b/i/c) / TI(wtd) aspect of trust between FI and SI of Blockchain among the given [age/gender/residency/education] group.

*actual hypoteses for each separate test can be found in the spreadsheet labeled "GSBT001" delievered alongside this thesis.

However, H1 was corroborated in almost any possible stratified testing, besides several groups and certain aspects, for which no significant difference was determined. Those are:

- Trusting Beliefs competence aspect among respondent above 30 years old (p-value = 0.09)
- All TB and TI aspects among respondents with High School diploma. P-values equaled 0.36, 0.29, 0.24, 0.14 for TB benevolence, TB integrity, TB competence and TI willingness to depend aspects respectively.

It is rather difficult to explain the absence of a significant difference in the first exemption case. However, p-values of 0.48 and 0.49 in TB benevolence and TB integrity aspects respectively may indicate that even though the difference in these trusting beliefs aspects is theoretically significant among the given category of respondents, it is not actually dramatic. Regarding the second exemption case, the lack of difference in perceived trust towards FI and SI of blockchain may be explained by the fact that respondents in this category were mostly below the age of 18, and thus may have not yet formed the distinctive attitude towards blockchain. On the other hand, the case may be that the younger generation is equally optimistic about the perspectives of these prominent technologies. This suggestion is supported by their average answers in the questionnaire: for FI of blockchain, means of TB aspects are 4.54, 4.38, 4,1 for benevolence, integrity, and competence respectively, while for SI of blockchain they were 5.1, 4.9 and 4.75. All these results are considered relatively solid. Still, in case of any other possible stratification, whether it is gender, age, or residency based, the significance of the difference between trust towards FI and SI of blockchain is present, and therefore H1 was corroborated.

4.4 Which aspects of trust influence public opinion and readiness to use blockchain based technologies and services the most?

Linear regression analysis led to some important insights which were very useful in answering the last RQ. Prior to a discussion of results, the model hypothesis* used in testing will be provided:

*actual hypoteses for each separate test can be found in the spreadsheet labeled "GSBT001" delievered alongside this thesis.

H1: Trusting Intentions (willingness to depend aspect) in FI of blockchain can be predicted by the independent variables in the model.

Independent variables (all related to FI of blockchain):

- Trusting Beliefs benevolence aspect

- Trusting Beliefs integrity aspect

- Trusting Beliefs competence aspect

Initially, it has been attempted to detect the interdependency and possibility to predict TI (willingness to depend) aspect between FI and SI of blockchain. Putting it in simpler words, a possibility to predict the respondents' TI (willingness to depend) in FI basing on their attitude towards SI of blockchain and vice versa. A regression analysis without any stratification has indicated that it is actually possible, proving H0 is to be rejected with significance value <0.01. However, with stratification introduced, it appeared that for certain demographical categories that do not hold true, and prediction is impossible. Among the cases where H0 is retained are:

- respondents with a High School diploma or MSc/Ph.D. degree (significance value equals 0.75 and 0.4 respectively)
- female respondents (significance value equals 0.18)
- respondents residing in OECD countries (significance value equals 0.08).

A reasonable and scientifically valid explanation for such results are likely out of the scope of this research – it is rather a question of sociology. Still, it is very interesting to examine and put more attention to the importance and significance of TB variables (benevolence, competence, and integrity) in predicting Trusting Intentions (willingness to depend). This analysis is able to quantitatively determine which aspect of Trusting Beliefs is more important for different demographic groups in determining whether to trust blockchain-based technologies or no.

The examination will start with discussing the analysis results for FI of blockchain. Remarkably, only competence belief variable appeared to be capable of being the predictor for willingness to depend, if the non-stratified sample is examined. H1 has been retained with significance value <0.01. Same results held true for age-stratified sample, where analysis of respondents both below and above 30 years old resulted in identical significance values for competence belief. Interestingly, integrity belief also appeared to be a valid predicting variable for respondents below 30, with a significance value of 0.04. In the case of sample stratified by gender, results are almost equal. For FI of blockchain, competence belief remains the only valid predictor variable of trusting intentions, both for male and female. Even significance values are almost identical: <0.01 for both groups. Stratification of the analyzed sample by the education provided slightly different findings. None of trusting beliefs variables appeared to be a valid predictor of trusting intentions for respondents who have MSc or Ph.D. degree. Among High School and BSc/BBA graduates, competence belief remained a valid predictor of trusting intentions – significance values were both below 0.01. Noteworthy, integrity belief also appeared to be a valid predictor among respondents with BSc/BBA degree (significance value equaled 0.05). Analysis of FI of blockchain is to be concluded with an examination of sample stratified by residency. In this case, the situation is very similar to a sample stratified by age: integrity and competence belief are predictors of trusting intentions among residents of CIS counties (respective significance values are 0.02 and <0.01), while only competence belief is a valid predictor in regards to residents of OECD countries (significance value <0.01).

The second part of linear regression analysis will consider the predictors of Trusting Intentions in SI of blockchain. Mostly, it does not follow the patterns distinguished in the analysis of FI presented above, where competence aspect of trusting beliefs has demonstrated predominant prediction capabilities. In the analysis of the non-stratified sample, competence and integrity trusting beliefs have been determined as valid predictors of trusting intentions (significance values equal 0.01 and 0.03 respectively). If stratified by gender, competence belief is the only valid predictor variable among respondents who are below 30 years old (significance value <0.01), while integrity belief is also the only predictor among the respondents who are above 30 years old (significance value 0.05). Gender-based stratification has led to rather interesting outcomes: the only predictor variable for the male part of the sample is benevolence belief, while among female just competence belief remained the predictor variable, same as in the case with FI of blockchain. Significance values for those regressions are 0.03 and <0.01 respectively. Unexpectedly, detection of predictor variables in the sample stratified by the level of education has been rather unsuccessful. For High School graduates and MSc/Ph.D. degree holders, there were no valid predictor variables found. Significance values in every case are above 0.2. For BSc/BBA part of the sample, competence belief is the sole valid predictor variable (significance value 0.02). Noteworthy, there are similarities with FI of blockchain in this case: competence belief was also one of two valid predictor variables among BSc/BBA degree holders. Residency-based stratification has led to the following results: benevolence belief is the single determinant variable among residents of CIS countries (significance value <0.01), while integrity belief was also the single valid predictor for residents of OECD countries.

In order to conclude the regression analysis part, it has been considered meaningful to compose a table quantifying how many times each of the predictor variables were found valid and significant. The following table allows to determine which aspect of the Trusting Beliefs is the most "influential" one.

Total number of regressions	**60**
TB benevolence (# of valid predictions)	**2**

TB integrity (# of valid predictions)	**6**
TB competence (# of valid predictions)	**13**

(Table 2. Quantified representation of successful prediction capabilities detected during regression analysis, by Trusting Beliefs aspects, in comparison with total amount of linear regression test ran.)

From this information it may be concluded that competence belief is of crucial importance when determining the probable trusting intentions, being in many cases the only valid predictor variable. Alongside that, the fact that trusting intentions in both iterations of blockchain technology are closely related and interdependent is quite noteworthy.

5 Conclusion and Recommendations

A significant amount of important predictions and conclusions can be extracted from this research. Firstly, an issue regarding the possible lack of trust in blockchain based assets and technologies has been discovered and examined. In order to examine the subjective trust and public perception more effectively, 2 distinct categories of possible blockchain implementation and application were defined in detail – First and Second Iterations of blockchain technology. This categorization has been carried out thoughtfully with a suggestion that general public addresses different issues and challenges to conceptually different implementation scenarios. A review of available scientific literature and other publicly accessible sources had proven that above-mentioned differentiation is actually sustainable, as FI related ways of blockchain application are mostly considered as part of an alternative financial system (coins and respective payment systems, ICO tokens) whereas SI of blockchain mostly attempts to address the need for secure, reliable, and immutable data exchange and storage (corporate and governmental registries, databases, IoT data exchange providers, smart-contracts). Moreover, an analysis of literature on implementation scenarios has provided useful information on a variety of concerns and challenges which are already present or are yet to overcome. The ones considered of higher importance are indicated further. For the first iteration of blockchain technologies, these were very frequent ICO scams, misuse in various forms (money laundering, use of crypto currencies in the black market, etc.), lack of ability to predict the behavior of non-major crypto currencies, lack of liquidity. One very important factor has to be mentioned separately – it is rather unlikely that people will trust to crypto currencies with anonymous creators, as knowing and trusting the issuing body is a crucial element of a conventional financial system. In the case of the second iteration, it has been more difficult to extract existing trust-related concerns, as their current scope of application is rather limited due to relative immaturity. Furthermore, there were no events of major public attention attracted to SI of blockchain technology, as it was with crypto currencies during late 2017. However, it has been considered very important to measure perceived trust in them as potential scope of SI application is significantly broader than in the case with FI, not to mention the possible difference in public trust between two iterations. Among possible challenges in SI implementation, it is important to point out the following: existing systems lack uniformity and sometimes scalability, while it is very difficult to find suitable implementation specialists on the labor market. These factors may be preventing potential users from adopting SI blockchain technologies.

A methodology proposed by McKnight et. al. (2002), appeared to suit the need of this research well, despite being initially designed to evaluate trust in web-vendors. It was found sufficient to measure the most important trust-related variables in assessing trust in blockchain-based technologies, indicated in the research of Duane et al. The model was simplified and the provided questionnaire adapted in order for them to be used in this research without re-validation. Two groups of variables were formed:

- Trusting Beliefs: competence, benevolence, integrity
- Trusting Intentions: willingness to depend.

Trusting Intentions group was considered the most important in determining the final extent of trust towards FI and SI, as it represented the publics' "willingness to depend", e.g. the degree of readiness to apply these technologies on the daily basis, trust them personal data and finances. Using group difference testing, it was determined that the extent of trust differs significantly between FI and SI of blockchain-based services and technologies. The only group of respondents where the differences were insignificant was people who held High School degrees. Mean values indicated that people tend to trust more in SI, but are still rather cautious about it. Alongside that, by means of linear regression analysis, it was discovered that perceived trust in 2 iterations is interconnected and thus perceived trust or mistrust in one scope of application, e.g. crypto currencies (FI) may influence the degree of trust in the seemingly unrelated scope of application, e.g. property rights registry (SI). Given that, it can be suggested that the development of both technology iterations will rely one on another to some extent. Further examination of possible prediction of trusting intentions by different aspects of trusting beliefs made it possible to discover that competence belief has a very important role, especially for the FI of blockchain. In case of almost any demographical stratification, it remained the valid predictor of trusting intentions, unlike other aspects. It was important for SI as well but to a lesser extent. This insight can be very important for developers of both crypto currencies and a wide variety of SI services, as it indicates that people are willing to trust a product with a solid and experienced team behind it. For the younger part of respondents, BBA/BSc graduates and respondents living in CIS countries, perceived integrity plays quite an important role as well. This way, all the research questions raised at the beginning of this paper were covered. For further researches on this topic, it would be gladly recommended to consider the following areas for deeper investigation:

- Reasons for the interrelation of trust in different iterations of blockchain technologies
- Reasons for the predominant role of competence belief over integrity and, especially, benevolence beliefs
- Methodology development for governmental application of blockchain, aiming to produce guidelines for the development of a uniform system which can address governmental scalability and security requirements.

Bibliography

Alexandre, A. (2018, July 13). New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams. Retrieved April 8, 2019, from Cointelegraph website: https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams

Asharaf, S., & Adarsh, S. (2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*. https://doi.org/10.4018/978-1-5225-2193-8

Ba, S., & Pavlou, P. A. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, *26*(3), 243. https://doi.org/10.2307/4132332

Babkin, Burkaltseva, Pshenichkov, & Tylin. (2017). *Cryprocurrency and blockchain in digital economy: development genesis.*

Bucko, J., Paľová, D., & Vejačka, M. (2015). *Security and Trust in Cryptocurrencies*. 11.

Buterin, V. (n.d.). *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*. 36.

Cellan-Jones, R. C.-J., Rory. (2018, May 9). *Magical Money: Is the crypto-boom doomed?* Retrieved from https://www.bbc.com/news/technology-44038181

Chan, S., Chu, J., Nadarajah, S., & Osterrieder, J. (2017). A Statistical Analysis of Cryptocurrencies. *Journal of Risk and Financial Management*, *10*(2), 12. https://doi.org/10.3390/jrfm10020012

Chiu, J., & Koeppl, T. V. (2017). The Economics of Cryptocurrencies Bitcoin and Beyond. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3048124

Choo, K.-K. R. (2015). Cryptocurrency and Virtual Currency. In *Handbook of Digital Currency* (pp. 283–307). https://doi.org/10.1016/B978-0-12-802117-0.00015-1

Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches*.

Duane, A., O'Reilly, P., & Andreev, P. (2014). Realising M-Payments: modelling consumers' willingness to M-pay using Smart Phones. *Behaviour & Information Technology*, *33*(4), 318–334. https://doi.org/10.1080/0144929X.2012.745608

Foley, S., Karlsen, J. R., & Putniii, Tt. J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3102645

Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J. (n.d.). *TERRORIST USE OF VIRTUAL CURRENCIES*. 56.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, *98*, 461–466. https://doi.org/10.1016/j.procs.2016.09.074

Janze, C. (n.d.). *Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets*. 11.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140

Mansfield-Devine, S. (2017). Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world. *Computer Fraud & Security*, *2017*(5), 14–18. https://doi.org/10.1016/S1361-3723(17)30042-8

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Ogono, U. (2018, May 25). Fantastic Boost In Awareness on Ellen Show: Ripple Is The Future. Retrieved March 21, 2019, from Smartereum website: https://smartereum.com/16035/fantastic-boost-in-awareness-on-ellen-show-ripple-is-the-future/

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Ong, B., Lee, T. M., Li, G., & Chuen, D. L. K. (2015). Evaluating the Potential of Alternative Cryptocurrencies. In *Handbook of Digital Currency* (pp. 81–135). https://doi.org/10.1016/B978-0-12-802117-0.00005-9

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Rogers, E. M. (2003). *Diffusion of Innovations, 5th Edition*. Retrieved from https://books.google.rs/books?id=9U1K5LjUOwEC

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

Rushe, D. (2012, July 17). HSBC “sorry” for aiding Mexican drugs lords, rogue states and terrorists. *The Guardian*. Retrieved from https://www.theguardian.com/business/2012/jul/17/hsbc-executive-resigns-senate

Veuger, J. (2018). Trust in a viable real estate economy with disruption and blockchain. *Facilities*, *36*(1/2), 103–120. https://doi.org/10.1108/F-11-2017-0106

Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/IJWGS.2018.10016848

Wei, W. C. (2018). Liquidity and market efficiency in cryptocurrencies. *Economics Letters*, *168*, 21–24. https://doi.org/10.1016/j.econlet.2018.04.003

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & FFhr, L. (2017). The ICO Gold Rush: It’s a Scam, It’s a Bubble, It’s a Super Challenge for Regulators. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3072298

Sources with undefined authors*

*sorted in an alphabetical order by article name

Bitcoin Energy Consumption Index. (n.d.). Retrieved April 7, 2019, from Digiconomist website: https://digiconomist.net/bitcoin-energy-consumption

Citigroup is looking to staff up its anti-money laundering unit with bitcoin pros - Business Insider Deutschland. (n.d.). Retrieved from https://www.businessinsider.de/citigroup-is-looking-to-staff-up-its-anti-money-laundering-unit-with-bitcoin-pros-2018-4

Cryptocurrency Survey: Awareness of Bitcoin Reaches Record High Among Business Professionals - Data Science - Opportunity. (2017). Retrieved March 21, 2019, from https://myopportunity.com/data-science/cryptocurrency-survey-awareness-of-bitcoin-reaches-record-high-among-business-professionals

Distributed Ledgers Definition. (2019). Retrieved April 12, 2019, from https://www.investopedia.com/terms/d/distributed-ledgers.asp

Exit scammers run off with $660 million in ICO earnings. (n.d.). Retrieved March 18, 2019, from TechCrunch website: http://social.techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/

Illegal Activity No Longer Dominant Use of Bitcoin: DEA Agent. (2018, August 10). Retrieved April 9, 2019, from Bitcoin News website: https://news.bitcoin.com/illegal-activity-use-bitcoin-dea-agent/

New Study: 20% of ICOs Are Scams, But Investors Aren’t Fazed. (2018, May 21). Retrieved April 8, 2019, from Bitcoinist.com website: https://bitcoinist.com/new-study-icos-scams-investors/

Number of Blockchain wallets 2018 | Statistic. (n.d.). Retrieved March 18, 2019, from Statista website: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

SEC.gov | Spotlight on Initial Coin Offerings (ICOs). (n.d.). Retrieved April 8, 2019, from https://www.sec.gov/ICO

Supply chain trends: spending on blockchain 2019 | Statistic. (n.d.). Retrieved March 18, 2019, from Statista website: https://www.statista.com/statistics/827408/spending-blockchain-supply-chain/

XRP (XRP) price, charts, market cap, and other metrics. (n.d.). Retrieved March 21, 2019, from CoinMarketCap website: https://coinmarketcap.com/currencies/ripple/

Appendices

Appendix A

Supplement ID: GSBT001

GSBT001 is a spreadsheet in .xlsx format containing detailed records on data analysis, indicating testing hypothesis for each test, and other details on testing procedures. Shipped in an archive alongside this document to the supervising body. Text version of it is presented on the following pages.

1) **Abbreviations:**

Var - variable from SPSS.

Abbreviations:

- TBb - Trusting Beliefs benevolence aspect

- TBi - Trusting Beliefs integrity aspect

- TBc - Trusting Beliefs competence aspect

- TIwtd - Trusting Intentions willingness to depend aspect

Graph - distribution normality evaluation via histogram ("+" if normal, "-" if abnormal)

*KS** - distribution normality evaluation via Kolmogorov-Smirnov test ("+" if normal, "-" if abnormal)

N - number of respondents in the category

*Test*** - a test selected for given group difference testing

Sig. 2-t. - result of two-tailed group difference testing ("+" if significant and H1 supported, "-" if non-significant, H1 rejected)

Sig. - significance value (p-value)

2) **Conditions:**

*KS test has been considered prevalent over visual examination when the amount of respondent exceeded 30

**in every testing, confidence interval was set at 95%, so difference has been considered significant at p-value < 0.05

I. Group Difference Testing

Note: Model Hypothesis for the respective tests will be provided above each table.

H1: There is a significant difference in TBb/TBi/TBc/TIwtd aspect of trust between FI and SI of Blockchain among the whole sample.

No Split	Var	Graph	KS	N	Test	Sig. 2-t.	Sig.
All resp.				109			
	TBb	+	-		Wilcoxon	+	<0,01
	TBi	+	+		P. S. t-test	+	<0,01
	TBc	+	-		Wilcoxon	+	<0,01
	TIwtd	-	-		Wilcoxon	+	<0,01

H1: There is a significant difference in TBb/TBi/TBc/TIwtd aspect of trust between FI and SI of Blockchain among the given age group (Below 30/Above 30).

Age	Var	Graph	KS	N	Test	Sig. 2-t.	Sig.
Below 30				85			
	TBb	+	+		P. S. t-test	+	<0,01
	TBi	+	+		P. S. t-test	+	<0,01
	TBc	+	+		P. S. t-test	+	<0,01
	TIwtd	-	+		P. S. t-test	+	0,03
Above 30				24			
	TBb	-	+		Wilcoxon	+	0,48
	TBi	-	+		Wilcoxon	+	0,49
	TBc	+	+		P. S. t-test	-	0,09
	TIwtd	-	+		Wilcoxon	+	0,01

H1: There is a significant difference in TBb/TBi/TBc/TIwtd aspect of trust between FI and SI of Blockchain among the given residency group (OECD/CIS).

Residency	Var	Graph	KS	N	Test	Sig. 2-t.	Sig.
OECD				38			
	TBb	-	+		P. S. t-test	+	<0,01
	TBi	+	+		P. S. t-test	+	<0,01
	TBc	-	+		P. S. t-test	+	<0,01
	TIwtd	-	-		Wilcoxon	+	<0,01
CIS				71			
	TBb	+	+		P. S. t-test	+	<0,01
	TBi	+	+		P. S. t-test	+	<0,01
	TBc	+	+		P. S. t-test	+	<0,01
	TIwtd	+	+		P. S. t-test	+	<0,01

H1: There is a significant difference in TBb/TBi/TBc/TIwtd aspect of trust between FI and SI of Blockchain among the given gender group (Male/Female).

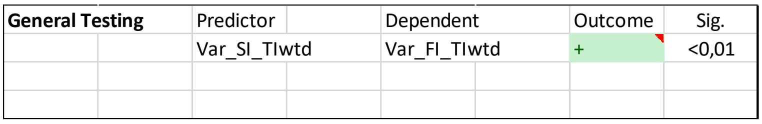
Gender	Var	Graph	KS	N	Test	Sig. 2-t.	Sig.
Male				71			
	TBb	+	+		P. S. t-test	+	0,12
	TBi	+	+		P. S. t-test	+	<0,01
	TBc	+	+		P. S. t-test	+	<0,01
	TIwtd	+	+		P. S. t-test	+	<0,01
Female				35			
	TBb	+	+		P. S. t-test	+	<0,01
	TBi	-	+		P. S. t-test	+	<0,01
	TBc	+	+		P. S. t-test	+	<0,01
	TIwtd	+	+		P. S. t-test	+	<0,01

H1: There is a significant difference in TBb/TBi/TBc/TIwtd aspect of trust between FI and SI of Blockchain among the given education group (High School Diploma/BSc & BBA/MSc & PhD).

Education	Var	Graph	KS	N	Test	Sig. 2-t.	Sig.
HSDip.				12			
	TBb	-	+		Wilcoxon	-	0,36
	TBi	-	+		Wilcoxon	-	0,29
	TBc	-	+		Wilcoxon	-	0,24
	TIwtd	-	+		Wilcoxon	-	0,14
BSc / BBA				65			
	TBb	+	-		Wilcoxon	+	<0,01
	TBi	+	+		P. S. t-test	+	<0,01
	TBc	-	-		Wilcoxon	+	<0,01
	TIwtd	-	+		P. S. t-test	+	<0,01
MSc / PhD				26			
	TBb	-	+		Wilcoxon	+	0,03
	TBi	+	+		P. S. t-test	+	0,01
	TBc	+	+		P. S. t-test	+	0,02
	TIwtd	-	+		Wilcoxon	+	<0,01

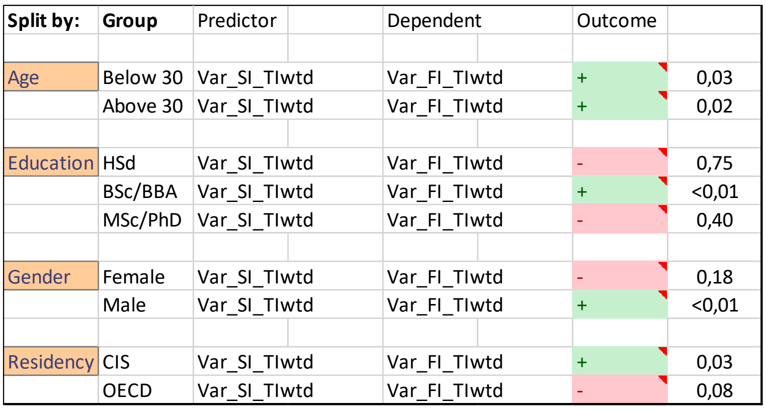
II. Linear Regression Analysis

H1: Trusting Intentions (willingness to depend aspect) in Fi of blockchain can be predicted by the independent variable (Trusting Intentions wtd aspect in SI of blockchain) in the model.



General Testing	Predictor	Dependent	Outcome	Sig.
	Var_SI_TIwtd	Var_FI_TIwtd	+	<0,01

H1: Trusting Intentions (willingness to depend aspect) in Fi of blockchain can be predicted by the independent variable (Trusting Intentions willingness to depend aspect in SI of blockchain) among the given age/education/gender/residency group in the model.



Split by:	Group	Predictor	Dependent	Outcome	
Age	Below 30	Var_SI_TIwtd	Var_FI_TIwtd	+	0,03
	Above 30	Var_SI_TIwtd	Var_FI_TIwtd	+	0,02
Education	HSd	Var_SI_TIwtd	Var_FI_TIwtd	-	0,75
	BSc/BBA	Var_SI_TIwtd	Var_FI_TIwtd	+	<0,01
	MSc/PhD	Var_SI_TIwtd	Var_FI_TIwtd	-	0,40
Gender	Female	Var_SI_TIwtd	Var_FI_TIwtd	-	0,18
	Male	Var_SI_TIwtd	Var_FI_TIwtd	+	<0,01
Residency	CIS	Var_SI_TIwtd	Var_FI_TIwtd	+	0,03
	OECD	Var_SI_TIwtd	Var_FI_TIwtd	-	0,08

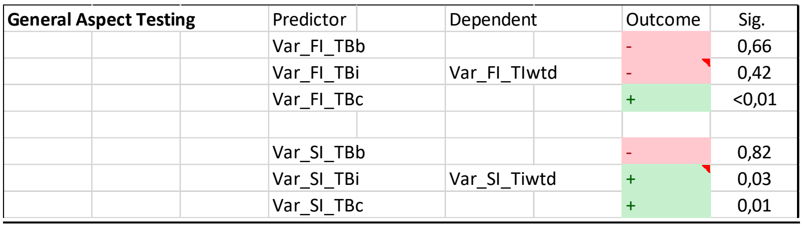
H1: Trusting Intentions (willingness to depend aspect) in FI/SI of blockchain can be predicted by the independent variables in the model.

Independent variables (all related to FI/SI of blockchain):

- Trusting Beliefs benevolence aspect

- Trusting Beliefs integrity aspect

- Trusting Beliefs competence aspect



General Aspect Testing	Predictor	Dependent	Outcome	Sig.
	Var_FI_TBb		-	0,66
	Var_FI_TBi	Var_FI_TIwtd	-	0,42
	Var_FI_TBc		+	<0,01
	Var_SI_TBb		-	0,82
	Var_SI_TBi	Var_SI_Tiwtd	+	0,03
	Var_SI_TBc		+	0,01

H1: Trusting Intentions (willingness to depend aspect) in FI/SI of blockchain can be predicted by the independent variables (same as above) among the given age/gender/education/residency group in the model.

Split by:	Group	Predictor	Dependent	Outcome	
Age	Below 30	Var_FI_TBb		-	0,68
		Var_FI_TBi	Var_FI_Tiwtd	+	0,04
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		-	0,15
		Var_SI_TBi	Var_SI_Tiwtd	-	0,29
		Var_SI_TBc		+	<0,01
	Above 30	Var_FI_TBb		-	0,35
		Var_FI_TBi	Var_FI_Tiwtd	-	0,65
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		-	0,39
		Var_SI_TBi	Var_SI_Tiwtd	+	0,05
		Var_SI_TBc		-	0,89
Gender	Male	Var_FI_TBb		-	0,10
		Var_FI_TBi	Var_FI_Tiwtd	-	0,73
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		+	0,03
		Var_SI_TBi	Var_SI_Tiwtd	-	0,83
		Var_SI_TBc		-	0,97
	Female	Var_FI_TBb		-	0,42
		Var_FI_TBi	Var_FI_Tiwtd	-	0,23
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		-	0,41
		Var_SI_TBi	Var_SI_Tiwtd	-	0,07
		Var_SI_TBc		+	<0,01
Education	HSd	Var_FI_TBb		-	0,41
		Var_FI_TBi	Var_FI_Tiwtd	-	0,65
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		-	0,25
		Var_SI_TBi	Var_SI_Tiwtd	-	0,25
		Var_SI_TBc		-	0,95
	BSc/BBA	Var_FI_TBb		-	0,42
		Var_FI_TBi	Var_FI_Tiwtd	+	0,05
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		-	0,33
		Var_SI_TBi	Var_SI_Tiwtd	-	0,23
		Var_SI_TBc		+	0,02
	MSc/PhD	Var_FI_TBb		-	0,13
		Var_FI_TBi	Var_FI_Tiwtd	-	0,97
		Var_FI_TBc		-	0,21
		Var_SI_TBb		-	0,28
		Var_SI_TBi	Var_SI_Tiwtd	-	0,29
		Var_SI_TBc		-	0,47
Residency	CIS	Var_FI_TBb		-	0,46
		Var_FI_TBi	Var_FI_Tiwtd	+	0,02
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		+	<0,01
		Var_SI_TBi	Var_SI_Tiwtd	-	0,69
		Var_SI_TBc		-	0,17
	OECD	Var_FI_TBb		-	0,51
		Var_FI_TBi	Var_FI_Tiwtd	-	0,70
		Var_FI_TBc		+	<0,01
		Var_SI_TBb		-	0,25
		Var_SI_TBi	Var_SI_Tiwtd	+	<0,01
		Var_SI_TBc		-	0,15

Appendix B

Supplement ID: GSBT002

GSBT002 is a spreadsheet in .xlsx format containing the final version of a dataset resembled of all the responses gathered during survey research from 109 respondents. Shipped in an archive alongside this document to the supervising body.

Appendix C

Supplement ID: GSBT003

GSBT003 is an SPSS Data Document in .sav format containing the final version of a dataset used during statistical analysis. It differs from GSBT002 as it contains additional computed variables required for running certain tests.