GÖTEBORGS UNIVERSITET

DEPTARTMENT OF POLITICAL SCIENCE

BLOCKCHAIN TECHNOLOGY: A TRUST OR CONTROL MACHINE?

Theory and Experimental Evidence

Đorđe Milosav

Master's Thesis:	30 higher education credits
Programme:	Master's Programme in Political Science
Date:	27th of May 2019
Supervisors:	Marina Nistotskaya and Love Christensen
Words:	14 816

Abstract

After the introduction of Bitcoin in 2008, there has been a proliferation of interest in digital technology called Blockchain. It has been argued that Blockchain can sustain any transaction of value, be it monetary or information, in a manner that is secure and completely *independent of interpersonal trust*. This same technology is perceived to be so secure and reliable that *The Economist* named it a "trust machine". Yet, due to its relative novelty, there is still little theoretical and empirical research on how this technology is expected to provide such trust-free transactions. Moreover, there seems to be an unaccounted disagreement about whether this technology is capable of creating interpersonal trust or it is just managing human relationships by shifting the trust that people have in each other towards trust in the technology itself. Therefore, the aim of this paper is to provide an in depth theoretical understanding of the relationship between trust and Blockchain technology and by doing so, answer the question of whether Blockchain is a trust-free or trust-building technology. Furthermore, in order to test the proposed claim, I carry out an online experiment with US participants recruited from Amazon Mechanical Turk The results indicate, contrary to my expectations, that Blockchain-based technology would not omit trusting and trustworthy behavior from human relationship. On the contrary, the behavior of the participants in the Blockchain treatment exhibited more trusting and trustworthy behavior, indicating support for the claim that this technology might indeed be understood as a "trust machine".

Key words: Blockchain technology, Trust, Reciprocity, Control, Experiments

Table of Contents

Acknowledgements

I would like to thank the Center for Collective Action Research at the University of Gothenburg for providing the funding for this research. Also, I would like to thank Marina Nistotskaya and Love Christensen for providing valuable comments on the experimental design and theory. Natalia Alvarado and Richard Svensson provided technical support for which I am especially grateful.

1. Introduction

There is an overall agreement in the social science literature that high levels of interpersonal trust are related to many normatively desirable outcomes (Rothstein, 2013). Countries that have high levels of trust[1] are likely to have greater economic growth, better government performance, more efficient judicial and bureaucratic system and less corruption (Knack and Keefer,1997; Putnam, 1994; Rothstein, 2011; Richey, 2010; La Porta et al. 1997). Yet, most of the countries today still struggle with low levels of trust, and although different suggestions to promote trust were made, little success was accomplished. Clearly, a lack of interpersonal trust remains a pressing hurdle for many countries across the world.

When it comes to the determinants of interpersonal trust, at least three distinct theoretical suggestions were made. Putnam (2000) suggests that interpersonal trust is primarily dependent on the participation in associations through which individuals learn to cooperate with others. Uslaner (2002) on the other hand suggests that the upbringing in the early years of one's life determines the level of propensity to trust others, which in turn leads to a disposition to enter associations. Lastly, Rothstein (2013) argues that the level of interpersonal trust depends on the trust in governmental institutions. Having less trust in institutions leads to the assumption that other members of the society engage in a corrupted behavior with the government in order to fulfill their individual needs. This in turn results in a deterioration of interpersonal trust among the members of the society.

Furthermore, on a more practical note, since the internet, digital technologies have been seen as way to enhance interpersonal trust (Kumar, 2018). This line of literature rests on Putnam's argumentation that (online) participation, trough for example social media platforms, enhances the level of interpersonal trust (see e.g. Boulianne, 2009; Shah et al. 2001). Yet, it seems that nowadays, a substantial portion of the empirical research on trust-building and the internet is done in order to provide evidence for more engaging electronic commerce and more efficient business transactions (see e.g. Beldad et al. 2010 for a literature overview). Therefore, the focus of the research in internet technologies and trust shifted towards the exploration of its effectiveness in creating monetary value. Yet, after the introduction of Bitcoin in 2008, there has been a proliferation of interest in another digital technology called Blockchain. It has been argued that Blockchain can sustain any transaction

[1] For the purposes of this paper, I use the terms "trust" and "interpersonal trust" interchangeably.

of value, be it monetary or information, in a manner that is secure and completely *independent of interpersonal trust*. This same technology is perceived to be so secure and reliable that *The Economist* named it a "trust machine". (October 31st, 2015).

Yet, due to its relative novelty, there is still little theoretical and empirical research on how this technology is expected to provide such trust-free transactions. Moreover, there seems to be an unaccounted disagreement about whether this technology is capable of creating interpersonal trust or it is just managing human relationships by shifting the trust that people have in each other towards trust in the technology itself. Therefore, the aim of this paper is to provide an in depth theoretical understanding of the relationship between trust and Blockchain technology and by doing so, answer the question of whether Blockchain is a trust-free or trust-building technology. As it will be shown below, I argue that Blockchain is a trust-free control machine that would crowd-out trusting and trustworthy behavior from the human relationship.

Furthermore, in order to test the proposed claim, I carry out an online experiment with US participants recruited from Amazon Mechanical Turk, an internet-based labor market with a pool of over 500,000 workers (Arechar et al. 2017). I compare the results of two experimental treatments based on a trust game from Berg et al. (1995). I utilize a between – subject design with anonymous participants. While the first treatment is a simple trust game designed by Berg et al. (1995) without the social history report, the second treatment is an adjusted trust game in which I operationalize the key aspects of Blockchain technology. The results indicate, contrary to my expectations, that Blockchain-based technology would not omit trusting and trustworthy behavior from human relationship. On the contrary, the behavior of the participants in the Blockchain treatment exhibited more trusting and trustworthy behavior, indicating support for the claim that this technology might indeed be understood as a "trust machine". Therefore, the results of this paper could be of importance to policy makers interested in the application of the technology in the economic and political areas in which a lack of trust represents a serious impediment for development.

The remaining of the paper is structured as follows: in the second section I present the key features of Blockchain technology in general and smart contracts as one subtype of its implementation. In the third section I present previous research on trust and Blockchain technology and my theoretical framework. In the fourth section I present the experimental design and hypothesizes together with the short summary of the experimental protocol and

features of Amazon Mechanical Turk. I analyze and discuss the results in section 5. Finally, concluding remarks are presented in section six.

2. Blockchain: what is it and how it works?[2]

Blockchain technology originated in 2008 with the introduction of Bitcoin, the first virtual cryptocurrency that is still operating today.[3] It is important to note that Blockchain technology cannot be equalized with Bitcoin since Blockchain is the mechanism that makes Bitcoin, the virtual currency, operating. Therefore, criticizing Bitcoin as a way of allowing the black market of for example drugs and weapons to flourish, although relevant, has nothing to do with the Blockchain technology itself (Zambrano, 2017).

Blockchain can be understood as a decentralized, distributed peer-to-peer network that stores and contains the data about all previous activities carried out within the network of users, called the nodes. This network is understood to be decentralized because each node within the network has a copy of the complete data of all previous activities, making it different from other systems sometimes referred to as systems with a "single point of failure" (Zambrano, 2017). Since the same data is stored on multiple locations at the same time, a loss of one copy of the data would not affect the network and the data availability. On the other hand, a loss of data that is stored in only one central repository would mean that the information stored on it does no longer exist. If, for example a centralized state repository of land registries burns in the accidental fire or experiences a hacker attack, all the data on the land registries would be gone. In the case with Blockchain technology, the data regarding the land registries would be on as many copies as there are nodes in the network, thus making it especially hard to lose the data.

Furthermore, Blockchain network is distributed, meaning that the enlargement of the dataset is not possible without the agreement of everyone in the network. This means that the new *block* of information (e. g. new set of Bitcoin transactions) is added to the dataset only after a process of "mining" is applied. In this process, some of the nodes use the computing power of their computers to find a solution for a highly complex mathematical problem through which they confirm that the new block of information is consistent with the previous

[2] My aim in this section is to present the key features of the technology that are important for the assessment of my research question. For a more technical explanation of Blockchain technology see: Raval (2016); Swan (2015).

[3] The identity of the inventor of this technology is still unknown since the article that introduced it was published under a pseudonym of Nakamoto (2008).

information stored in all previous blocks.[4] By doing so, the *new* block is added to the existing ones in a way that it becomes impossible to tamper with the whole content of the dataset. In return, nodes that perform the "mining" receive some monetary value in return (Bitcoin for example) for the work that they have done. More technically speaking, through "mining", a new block of information is added to Blockchain through the production of a new "hash" that guarantees the incorruptibility of the Blockchain system" (see Galati, 2018).

Thus, Blockchain is able "to facilitate the exchange of value in a secure and decentralized manner without the need for intermediary" (De Filippi, 2017). This "ability of Blockchain based systems to enforce rules and contractual agreements without an arbitrating authority" attracted the most interest when it comes to addressing trust related issues (Hawlitschek et al. 2018 p. 57). Taking the same example of the land registries, by using the Blockchain system, the public bureaucracy would not be able to unilaterally (or within the group of corrupted officials for example) change the ownership of the land to accommodate their own corrupted needs, because all the rest of the nodes would be informed about inconsistent changes in the registry. Taken together, these properties make Blockchain network secure, transparent and open for storing and using any kind of information.

Therefore, Blockchain technology provides a way to secure the content of the data from loss and unilateral retroactive change. Furthermore, since the enlargement of the data (e. g. addition of the information regarding new monetary transactions) is not possible without the agreement of everyone in the network it is argued that there would be no need for trust between the actors in order for it to function properly. In one word, Blockchain technology is argued to be a "trust machine" (Economist, Oct 31st, 2015).

Smart Contracts

Smart contracts were initially defined by Nick Szabo as "contractual clauses embedded into hardware and software in such a way that makes breach more expensive" (in: Raskin, 2017 p. 320). Yet, due to the previous lack of technology, only after the introduction of Blockchain it was possible to actually implement the concept completely. Utilizing the previously described characteristics of Blockchain technology, smart contracts are now

[4] Due to the high complexity of the mathematical problem, the "mining" process is extremely energy consuming. This is often stressed in the literature as a downside of the Blockchain implementation possibilities, especially in the countries with high energy costs or countries that do not have the infrastructure to support the energy needs (see Kshetri 2017).

understood as agreements with automated execution (Raskin, 2017 p. 306). Parties involved in the construction of such a contract agree *ex ante* on a set of conditional statements that are encoded in the smart contract. When these conditions are met, the smart contract executes itself according to the agreed rules.

When compared to traditional contracting, two aspects of smart contracts make them distinctive and innovative. Firstly, as with the case of Blockchain in general, smart contracts function without the need for an intermediary. More specifically, this means that smart contracts are executed without the need of any kind of legal support. Similarly, Sklaroff (2017) argues that smart contracts allow the contracting parties to be involved in an exchange that is autonomous from "inefficient and corruptible institutions" (p. 268) Therefore, since any third party is excluded from the relationship, these contracts are by definition insisting on the "privacy and desirability of private social ordering" (Sklaroff 2017 p. 268). Furthermore, the parties involved in the contract do not need to trust each other either because the transparency and verifiability of the information is guaranteed by the Blockchain on which the contract is operating.

Secondly, some legal scholars argue that the logic of smart contract enforcement is completely different when compared to traditional contracts. Traditional contracts are enforced in a court process, only in cases in which parties differed from the actions they were supposed to follow. Smart contracts, on the other hand, prevent the possibility for unwanted behavior before it occurs, thus making the court process obsolete (Werbach and Cornell, 2017). Another aspect of smart contracts relates to the execution process. Contrary to the distinction between the time of agreement formation and execution in the traditional contract, smart contracts are executed at the very moment when the encoded rules are uploaded on the Blockchain.[5]

[5] A will for example can be encoded in a smart contract. When a person who the will is referred to passes away, the property listed in the will is automatically transferred to the individuals stated in the will. Through functioning on Blockchain, the execution of such a will is based on a "decision" of a neutral uninterested third party – nodes on the network - who confirm that the new block of information is in line with the previously stipulated conditions in the contract (Raskin, 2017). Therefore, enforcing a will on a smart contract would omit the need for a notary since the information stated in the contract is already registered and confirmed as "true" at the moment when it was successfully uploaded on the Blockchain.

On the other hand, a smart contract must be completely defined before it gets updated on the Blockchain, thus eliminating the flexibility of a contractual process. Related to the lack of flexibility, Hawlitschek et al. (2018) argue that if the rules themselves encoded in the contract are not secure and "smart", the execution of the contract can have devastating effects on the parties involved. Therefore, even though it is argued that smart contracts can significantly lower the costs of enforcement by excluding the state from the process, the costs of completely defining all the conditional statements (if that is indeed possible) would prove to be substantial (Sklaroff 2017). This aspect is seen by the author as a crucial disadvantage of smart contracts when it comes to implementation in the business environment. On a more general note Sklaroff (2017) concludes that the flexibility of a semantic contract (i.e. non-smart contract) "is a feature, not a bug" (p. 303).

Before presenting previous empirical research on Blockchain and trust it is worth reiterating the key aspects of the technology on which arguments on trust are based on. Following Hawlitschek et al. (2018) Blockchain based systems are "trust-free" because the information on the network is stored on a ledger that is publicly disclosed and immutable. This aspect is nicely described by Wenger who defines Blockchain as "logically centralized (there is only one ledger), but organizationally decentralized (many entities maintain copies of that ledger)" (in: Werbach 2018 p. 500). Furthermore, based on the "hashing" mechanism Blockchain provides consensual agreement of the data record that is immutable and secure.[6]

3. Previous Research and Theoretical Framework

a. Previous Research in Blockchain Technology and Trust

Although the empirical research related to trust and Blockchain technology is still rather scarce, it provides two major findings relevant for this paper. Firstly, it seems that existing Blockchain-based solutions are not as "trust-free" as they are argued to be. Fröwis and Böhme (2017) present conditions on which they argue a smart contract is "trust-free" and analyze all smart contracts published on Ethereum, a network similar to Bitcoin. Their findings suggest that "two out of five smart contracts deployed on Ethereum do require trust in at least one third party" (Fröwis and Böhme, 2017 p. 370). These contracts lack the "immutability of the control flow" which means that their content can be changed unilaterally even after they are signed (Fröwis and Böhme 2017 p. 357). This problem emerged due to the

[6] Due to space constrains, I present a set of existing applications of the technology together with a short overview of previous academic and ideology-focused interest in Appendix 1.

lack of expertize when coding the contracts and is therefore not an intrinsic general failure of the Ethereum network.

Secondly, most of the existing research in the area is investigating the question of trusting the technology itself. Although answering this question is not the aim of this paper it is worth nothing the results of this research. Sas and Khairuddin (2017) interviewed the users of Bitcoin in order to investigate the aspects that might enhance or hinder the trust in the technology itself. They found out that decentralization, deregulation, miners' expertize and reputation are all contributing to trust in the technology. These indeed are the aspects of the technology that are theorized to bring about its "trust-free" feature. Yet, insecure transactions are shown to be the main reason for hindering the trust in the technology.

Similarly to what Fröwis and Böhme (2017) found in their study, Sas and Khairuddin (2017) argue that the main reason for transaction insecurities are due to a human factor, such as protecting passwords for Bitcoin wallets or failures to reverse wrongly initiated transactions. Furthermore, since Bitcoin network is registering only Bitcoin transactions, the users often stated that they were scammed when buying fiat currencies or goods. Put simply, even though they sent Bitcoins in return for goods, they never received the goods. For some of the respondents this was one of the main arguments in support for introducing state regulation in the Bitcoin system (Sas and Khairuddin, 2017).

Lustig and Nardi (2015) argued that the trust in Blockchain technology should be based on "Algorithmic authority" that they define as "trust in algorithms to direct human action" (p. 743). After conducting a survey on Bitcoin users, the authors suggest that, even though their respondents trust the technology more than existing institutions, they still are in favor of a possibility of introducing an outside third party support to make Bitcoin more legitimate. Furthermore, as noted in the previous paragraph, since there are possibilities of fraud on the network, the surveyed respondents indicated that in addition to trusting the technology, they need to have trust in others in order to execute a transaction on the network. Therefore, it seems that there is a discrepancy between the vision and practice of Blockchain-based systems (Fröwis and Böhme, 2017). For that reason, in this paper I suggest that operationalizing key aspects of Blockchain-based systems in an experimental design could allow me to better understand the actual effects this technology might have on human relationships. Yet, before presenting the experimental design, I propose a new in-depth understanding of the relationship between trust and Blockchain technology.

b. Understanding Trust and Blockchain

Although there has been an advance in the understanding of the possible implications of utilizing this technology across different areas in which humans interact (see Appendix 1), less work has been done on the theoretical specification that Blockchain has on trust (Hawlitschek et al. 2018). A closer look at the literature on Blockchain and trust indicates that there seems to be a misunderstanding in which various authors perceive that they are interpreting this relationship in the same manner. I argue that conceptualizing Blockchain as a "trust machine" (Economist, 2015) and as a technology that allows a system to be "trust-free" (Beck et al. 2016 for example) are two distinct concepts with radically different implications. In this paper, I would argue for the second type of explanation.

The most prominent difference between these two conceptions is based on the question whether this technology is seen as a potential producer of trust between the actors in the network. If Blockchain is understood as a "trust machine" then its mechanisms are expected to produce more trust within the network. On the other hand, if the system is understood to be "trust-free", there would be neither production nor loss of trust within the network. More precisely, one should argue based on the context and theory what will happen with trust in cases in which it is exempted from the relationship.

For example, Grainer and Wang (2015) argue that Blockchain is a trust-free environment in which "costly mechanisms to build trust in intermediaries or interpersonal trust are thought to be rendered obsolete by design" (in: Hawlitscheck, 2018 p. 57). Therefore, the authors essentially argue that the *importance* of trust would be reduced. Yet, if Blockchain is indeed a "trust-free" system, what is then the mechanism that is driving the relationship to the exceptional results which are argued this technology would bring? I argue that this mechanism is a mechanism of control. In the remaining of this section I present my argumentation in more detail.

No Risk - No Trust

Although the literature on the conceptualization of trust is vast and often with opposing definitions across the different fields, a general agreement among scholars is that trust is consisted of two key aspects. An actor who trusts[7] is expressing *a willingness to be*

[7] Although, both the trustors and the trustees can be individuals, organizations or institutions, the focus of this paper is the trust that individual trustors have in other individuals.

vulnerable and has *a positive perception of the intentions of the other party* (Rousseau et al.,1998, italics added for emphasis) If the actor does not have such willingness and/or believes that the other party has ill intentions, he or she will not trust that other party.[8] Rousseau et al. (1998) describes trust as a "psychological state comprising the intention to accept vulnerability upon positive expectation of the intentions or behavior of another" (p. 395).

The willingness to be vulnerable is often understood as a form of risk that is integral to the definition of trust. Hardin (2002) for example argues that when one is "giving the discretion to another to affect one's interests" he/she is "subject to the risk that the other will abuse the power of discretion" (p. 11-12). Similarly, Gambetta (1988) argues that in a trust relationship, a trustee has to have a possibility of betrayal or defection in order for one to say that the relationship between these individuals is one of trust. Therefore, if the setting that governs the relationship is fully determined in a sense that the trustee cannot betray or defect the trustor, one cannot argue that the relationship between those individuals is based on trust. Moreover, by having a perception of the intentions of another party, the trustor is willing to be vulnerable to another *human's* behavior. Therefore, if for example a person is willing to be vulnerable to make a risky investment in another actor's business based on a roll of a dice, there cannot be a relationship of trust established since the dice is not human.

This conceptualization of trust could be understood to be a highly restrictive one, especially in the context of this paper. Research in human-computer interaction (see for example: Sas and Khairuddin, 2017) and research related to trust on the internet (van der Werf et al. 2018) conceptualize the notion of trust in the technology itself. Trusting the technology is indeed crucial for its successful implementation. Yet, in order to assess the usability of the technology I put aside this concern and understand technology to be a key mediating factor that regulates the relationship between the individuals.[9]

Much research has been done on investigating the key antecedents of trust. In the context of human-computer interaction research, Riegelsberger et al. (2005) suggest a framework of mechanics of trust and identify contextual and intrinsic properties as key

[8] Yet, it is often put aside that the actual action of a trustor does not have to coincide with the existence of trust in another party. In other words, it is possible that an actor will act as if he/she trusts another actor even though that might not be the case (Glaeser at al. 2000).

[9] For a more in-depth theoretical assessment of the question of trust in the technology itself see Appendix 2

factors that determine individual trust in others.[10] Contextual factors are temporal, social and institutional embeddedness. Temporal embeddedness refers to "parties' potential for engaging in future transactions and interest in their relationship's longevity". Social embeddedness refers to the information exchange among trustors about trustees' past performance" that in turn motivates the trustee to protect his reputation and fulfill the agreement. Lastly, institutional embeddedness refers to the "legal aspects underpinning transactions" and enforcement sanctions for the actors who do not comply with their part of the agreement (in: Sas and Khairuddin, 2017 p. 6500).

Intrinsic factors on the other hand include the trustee's internalized norms, benevolence and ability to act in a trustworthy manner. Internalized norms refer to the trustee's moral principles that guide the individual to act in a trustworthy way. Similarly, benevolence of a trustee refers to his/her disposition to act in accordance of the wellbeing of another. Lastly, the ability to act in a trustworthy manner is based on the trustee's credibility (in: Sas and Khairuddin, 2017 p. 6500).

If this model of trust relations is applied on the case of Blockchain-based smart contracts it provides support for the argument that the technology should indeed provide a base for "trust-free" social interactions. Although it is still a relationship between *humans*, smart contracts are governing the behavior according to encoded immutable rules that are forbidding potential changes in the behavior after the contract is uploaded on the ledger. Additionally, since the patterns of possible behavior are imposed *ex ante*, risk is omitted from the relationship. In other words, when the trustor specifies the allowed behavior of the trustee in an encoded smart contract he/she indicates *no* willingness to be vulnerable. In the smart contract, the trustor is omitting the possibility of the trustee's potential betrayal by basing the relationship in a risk-free Blockchain environment.

Furthermore, smart contracts figure as a form of institutional embeddedness. Enforcement sanctions are, by definition, entrenched in the smart contract in a way that it makes incompliance with the agreement impossible. Moreover, a shown interest in the relationship longevity between the contracting parties (temporal embeddedness) and information exchange on the parties past performance (social embeddedness) can be

[10] Although I noted that the relationship between individuals in a Blockchain is not one of trust, this framework could be used to specify the fine conceptual differences between trust and control.

understood as obsolete. If contracting parties conducted their business on a smart contract before or have been informed from a third party that their counterpart used smart contracts in other businesses, they can only conclude that the contracts were executed in accordance to the previously stipulated rules. The proposed irrelevance of temporal and social embeddedness is further supported by the fact that most of the existing transactions over Blockchain-based smart contracts are anonymous. Similarly, intrinsic factors could as well be understood as irrelevant as long as the rules encoded in the smart contract are agreed upon by both parties. Although the process of writing the contract may be affected by contractors' signaling of their intrinsic dispositions, when the contract is signed the trustee's moral principle, benevolence and an ability to be trustworthy cease to be of importance.

Therefore, to reiterate, through defining the rules of the agreement *ex ante*, Blockchain-based smart contracts are omitting risk from the human relationship. This in turn indicates support for the argument that Blockchain technology provides a system that is independent of interpersonal trust. Furthermore, smart contracts should be understood as a form of institutional embeddedness since its enforcement sanctions make incompliance with the agreement impossible.

No Trust - No Trustworthiness

Although trustworthiness is a concept that is highly related to the concept of trust, it received less attention in the literature. In most of the cases, trustworthiness is described in relation it has to trust and is understood as the "capacity to judge one's interest as dependent on doing what one is trusted to do" (Hardin, 2002 p. 28). Therefore, the central problem when it comes to trustworthiness is the issue of commitment to fulfill the expectation of the trustor. (Hardin, 2002). It is no surprise that one of the main interests among researchers of trust is to understand the reasons behind a trustworthy behavior. Hardin (2002) suggests, similar to the Riegelsberger et al. (2005) trust model, three types of inducements: internal inducement, such as moral compunction or individual character traits, external inducements such as social and institutional constrains and mixed inducements.[11] As it will be shown below, internal inducements are understood to be rendered obsolete by the Blockchain mechanism.

[11] Riegelsberger et al. (2005) trust model figures as an example in which trustworthiness is referred to only in relation to the effects it has on trust. Although it might seem that Hardin's scheme of different types of trustworthy inducements overlaps with Riegelsberger et al. (2005) trust model, it is important to specify which factors from their model are referring to the trustor's and trustee's behavior.

Therefore, for the purposes of this paper, I am presenting external inducements only, and suggest that sometimes these inducements can work against a trust-building relationship.

Hardin (2002) understands external inducements to be "external devices that secure our important commitments that depend on… the actions - often sanctions - of others" (p. 41). He makes a distinction between three types of external inducements: small scale controls of ongoing relationships such as relationships within a family or between close friends; broad social controls and controls based on law or other formal institutions. (see: pp 40-48). In the context of Blockchain technology, I argue that, since the actors in a relationship are anonymous, social control based on close relationship or broad social rules could easily be avoided. Yet, similarly to Riegelsberger et al. (2005) concept of institutional embeddedness, strict formal rules, embedded in the technology itself could figure as a type of formal, technology-based regulation that can externally impose a trustworthy behavior.

Technology as a mediating factor of control

By presenting the discussion of the trust-control nexus, I lay out the argumentation for how Blockchain systems are able to crowd-out trust from the human relationship by means of control. Following the work of Bijlsma-Frankema and Costa (2005), I understand formal control to be a "regulatory process by which elements of a system are made more predictable through the establishment of standards in pursuit of some desired objective or state" (p. 259). Furthermore, formal control is dependent on the existence of three factors: the principle of specification, the possibility of monitoring and the institutional structure that enables enforcement (Bijlsma-Frankema and Costa, 2005).

Firstly, in the context of this paper, the principle of specification in which "actions leading to successful cooperation and exploitation of value can be specified *ex ante*" (Bijlsma-Frankema and Costa, 2005 p. 264) could be understood as a hallmark of Blockchain based smart contract. The ability of smart contracts to facilitate "trustless exchange" (Sklaroff, 2017) is based on the immutability of previously fully specified rules that govern the behavior of the contractual actors. Defining the behavior based on encoded conditional claims assures the parties that cooperation would transpire when the stipulated conditions are met.

Secondly, the possibility of monitoring as a requirement of formal control in Blockchain based smart contracts is met by the fact that a Blockchain network is distributed.

If all of the nodes in the network receive a warning in which it is stated that there are discrepancies in the information presented on the smart contract, the action, for example a transaction of information, would not be executed. By this way, nodes in the network function as a set of monitoring actors who are objectively determining[12] if actors affected by the smart contract are deviating from the rules they agreed upon (Bijlsma-Frankema and Costa, 2005 p. 264).

Thirdly, in a manner of the argument of institutional embeddedness, a formal control needs to be based on an institutional structure that "enables [the] enforcement of the contract or rules, so that a credible treat can be made" (Bijlsma-Frankema and Costa, 2005 p. 264). Since the monitoring mechanism within the Blockchain-based smart contract is "perfect", I would argue that a fraud attempt against the rules of the agreement would most certainly be detected. In this way a punishment (for example, an exclusion from the network) represents a credible threat against misbehavior.

In the context of the discussion of the relationship between trust and control I argue that Blockchain systems would crowd out trust from the human relationship. Therefore, this claim should be in support for the idea that the technology is indeed "trust-free". More importantly, this paper is aiming to provide further support for the substitution perspective on the relationship between trust and control. As it will be shown in the experimental design I argue that previously presented aspects of Blockchain control would destroy potential trust-building behavior between the participants in the experiment. An alternative, complimentary perspective, in which control is seen to go hand in hand with trust-building relationship, would assume that Blockchain control mechanism would enhance the level of trust between the individuals making the technology a "trust machine".

[12] It is worth noting that since smart contracts are designed according to the "private social ordering" (Sklaroff 2017 p. 268), *objective* in this sense would mean that the contract is executed exactly according to the rules stipulated by the individuals that signed it. This indicates that the contractual rules themselves can, theoretically speaking, remain unjust or morally questionable. This is one of the reasons why Werbach (2018b) concluded that Blockchain and law should go hand in hand with each other.

4. Experimental Design and Hypothesizes

a. Experimental Design

In order to operationalize the key aspects of Blockchain technology in the experimental design I build on previous experimental work based on a trust game from Berg et al. (1995). This area of experimental research is well established and provides a considerable set of design alternatives that serve as a foundation on which I am able to create the treatments according to my own research needs (see: Johnson and Mislin, 2011 for a meta-analysis of Trust games).

I compare two experimental treatments and utilize a between – subject design. The first treatment is based on a simple Trust game designed by Berg et al. (1995) without the social history report. It is a two person, two stage, anonymous game in which participants are randomly paired strangers. Before the beginning of the game, both participants are paid a $1 participation fee and receive 10 game points (1 point equals to 1 US cent). When the game starts, First mover (from here FM) makes the decision to either "invest" some or all of his 10 game points by sending it to Second mover (from here SM) or to leave the game without investing. [13] In case FM does not invest, the game ends and both players earn $1 and 10 cents. In case FM decides to invest, the amount sent is tripled and sent to the SM. Then, SM can decide whether she wants to return some, all or none of the received amount back. After the decision is made, participants answer a short survey and are informed about their final earnings in US dollars. The amount sent by the FM is understood to capture trust and the amount returned from the SM to the FM to capture trustworthiness (Johnson and Mislin, 2011).[14]

The second treatment is designed with an aim to operationalize a Blockchain-based smart contract. In addition to the rules of the Trust game treatment, I introduce a notion of a smart contract by informing both participants that if FM decides to invest, SM would be bounded by the contractual agreement to return at least the amount FM sent before the

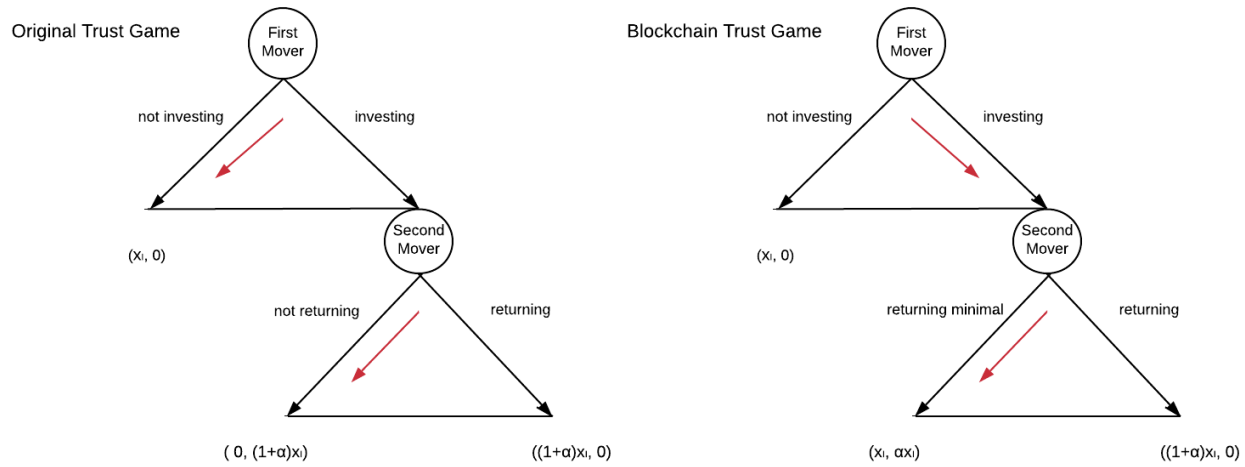
[13] In line with the practice within the literature and for the sake of simplicity, the FM would be regarded using male pronouns and the SM would be regarded using female pronouns.

[14] Contrary to the expectations of rational choice theory, Berg et al. (1995) showed that the FM is often investing, showing the readiness to trust and that the second mover often behaves in a trustworthy way by returning some portion of the sent amount back. The meta-analysis by Johnson and Mislin (2011) further supports these results.

investment multiplication. For example, if FM decides to invest 4 game points, SM receives 12 points of which she is obliged to return a minimum of 4 points or more. SM cannot decide to return less than it was initially sent by FM, but she can decide to return more than the minimal amount stated in the contractual rule.

In Figure 1, I present a decision tree for both treatments. Following the rational choice theory, two treatments produce two differing subgame perfect equlibira. In the case of the original trust game, by applying the backward induction, second mover is expected to always decide to not return any points back to the first mover. Knowing this, first mover is expected to always decide not to invest any amount of his initial 10 game points. If he decides to invest some or the entire initial amount of 10 game points (the possibility to invest from some to the entire amount of points is depicted in the horizontal line), second mover will decide not to return any amount back and keep the entire invested amount to herself. Therefore, the subgame perfect equilibrium is <not investing>; <not returning>.

Figure 1: Decision trees for Trust and Blockchain treatments



Note: For both games: FM: xI = x(1+α) and SM: xI (1+ α)

x: Amount sent before multiplication
xI: Amount sent after multiplication
α: investment multiplication factor = 2

On the other hand, in the Blockchain treatment, second mover can decide between returning the minimal amount (amount invested by the first mover before the multiplication) and returning the entire invested amount back. Similarly to the expected decision of the

second mover in the Trust treatment, second mover in the Blockchain treatment is expected to return the minimal amount back. Knowing this, first mover should always decide to invest the maximal amount of points because of the contractual restriction that disables the second mover to return less than what is sent before the multiplication. Moreover, by investing, the FM has a chance of earning more than the amount of game points received at the beginning of the game. Therefore, the subgame perfect equilibrium for the Blockchain treatment is <investing>; <returning minimal>.

b. Reciprocity argumentation and hypothesizes

As previously noted, key antecedents of trust could be conceptually divided into contextual and intrinsic factors. In the context of one-time, anonymized Trust game, I argue that contextual factors such as temporal, social and institutional embeddedness are by design excluded from the trust "equation". Temporal embeddedness is excluded due to the lack of repetition in the game. Social embeddedness is excluded due to the anonymous nature of the game and Institutional embeddedness due to the lack of any rules guiding the behavior of both the first and the second mover.

On the other hand, intrinsic traits of the trustee, such as internalized norms, benevolence and an ability to act can be seen as crucial when it comes to trustworthy behavior. Since the players in the anonymized trust game do not know the identity of each other, it is argued that the trustor makes a decision based on his previous experience when trusting others. (Glaeser et al. 2000).[15] Additionally, Berg et al. (1995) content that in repeated trust games, the trustee can behave in a trustworthy manner out of concerns for her reputation or potential punishment threats. Behaving in an untrustworthy manner hinders the trustee's reputation which in turn makes the trustor send less or none of his endowment in the succeeding games (Berg et al. 1995).

Additionally, McCabe et al. (2003) argue for what they call an intention-based model in which a trustee acts according to her own perceived motivations of the trustor. These models emphasize "the role of intentions in achieving cooperative outcomes in personal exchange" and essentially rely "on players reading each other's motives (and not merely their

[15] In non-anonymous trust games, Glaeser et al. (2000) suggest, based on their own experimental results that social connections between the trustor and the trustee and their social capital positively affect the amount sent. On the other hand, a difference in the nationality and race of the participants negatively affects trusting behavior (see pp. 813-14).

actions)" (McCabe et al. 2003 p. 268). One type of this model is based on the *trust and reciprocity hypothesis*. Two players enter a reciprocal trust relationship if "(1) there are mutual gains from their joint actions, (2) Player 1 takes a risk by trusting Player 2, and (3) Player 2 gives up something in order to reciprocate Player 1's trust" (McCabe et al. 2003 p. 269). Furthermore,

> "Player 1 trusts Player 2 only if Player 1 has two relevant *beliefs*: that Player 2 will interpret his move as a trusting one, and that Player 2 will reciprocate… it is clear that Player 2's action can be described as reciprocal only if she *interprets* Player 1's action as trusting. That is, Player 2 must attribute to Player 1 the *intention* of entering into a reciprocal-trust relationship" (McCabe at al. 2003 p. 269).

In the case of my two experimental treatments I argue that in the Trust treatment, all the contextual factors are omitted by the design of the game. Temporal and social embeddedness are excluded due to the fact that it is an anonymized one-shot game. Likewise, institutional embeddedness is excluded due to the lack of restrictions when it comes to the amount that can be sent and returned by the First and the Second Mover respectively. Moreover, intrinsic factors, such as internalized norms, benevolence and previous experience can affect the decisions of both the First and the Second Mover. Yet, due to the experimental design, these factors should be randomly distributed across the participants in the game. Furthermore, the design meets all the necessary requirements for a reciprocal trust relationship. If the FM in the Trust game sends some or all game points to the SM, by tripling the amount sent, the SM has the ability to increase the gains of both players in the game, by sending at least one point more than the initially sent amount before investment multiplication. Due to the fact that SM can abstain from sending any points back, the FM is taking a risky decision to trust the SM. Lastly, if the SM returns something back, she is reciprocating the FM's decision to trust.

In the case of Blockchain treatment, the existence of contractual rules that regulate the behavior of the SM figure as a form of institutional embeddedness. The obligation imposed on the SM to return at least the amount sent by the First Mover is understood here as a regulatory process that makes incompliance with the agreement impossible. Similarly to the Trust game treatment, due to the anonymized one-shot design, temporal and social embeddedness are omitted from the Blockchain game as well. Furthermore, I argue that the possibility for reciprocal behavior of the second mover in the Blockchain treatment is

restricted. If the FM decides to invest and sends some or all of his game points to the SM, he is not making a risky decision since he knows that the SM is obliged to return at least the same amount sent before the investment multiplication. Yet, I expect that the FM would always invest due to the lack of risk of losing the amount invested. On the other hand,]although the features of the design allow for the possibility for the SM to reciprocate, I argue that she would return the minimal amount not in order to reciprocate the FM but in order to abide to the rules of the contract agreement. The reason for this claim is due to my expectation that the SM will not interpret the move of the FM as a trusting decision. In other words, SM is not interpreting the FM's decision to invest as an intention to enter a reciprocal trust relationship. Thus, I present the following hypothesizes:

H1. On average, First Mover in the Blockchain treatment would decide to invest more often than the First Mover in the Trust treatment.

H2. On average, First Mover in the Blockchain treatment would invest more points than the First Mover in the Trust treatment.

H3. On average, Second Mover in the Blockchain treatment would return a smaller proportion of the investment amount after multiplication than the Second Mover in the Trust treatment.

H4. The amount returned by Second Mover in the Blockchain treatment is not be affected by the amount sent by First Mover.

H5. The amount returned by Second Mover in the Trust treatment is positively affected by the amount sent by First Mover.

c. Amazon Mechanical Turk and Experimental Protocol

This paper is based on the experiments conducted over Amazon Mechanical Turk, (from here: MTurk), an online labor market with a pool of over 500,000 workers (Arechar et al. 2017). After creating an account, the requesters (employers) create a task called HIT (Human Intelligence Task) and publish it on the platform. The workers, often called "Turkers" can decide, after reading the short HIT description whether to accept the work or not. Buhrmester et al. (2011) suggest that the acceptance of a HIT mostly depends on the presented compensation rate and expected task length but argue that higher compensation rates do not significantly affect the quality of the data. Following the suggestion from

Arechar et al. (2017), I set my compensation rate to be around $ 8.5 US per hour.[16] Due to the easiness and relatively cheap way of obtaining experimental data, MTurk experienced a growing popularity among experimental researchers in social science. Furthermore, the growing use of this Amazon service was followed by research that deals with methodological issues that comes with its use and the potential differences between MTurk based experimental research with more traditional lab and field experiments. Due to space constrains, I address these issues shortly.

Buhrmester et al. (2011) suggest, based on their own research, that MTurk participants are demographically more diverse than standard internet and college samples. The research done by Paolacci and Chandler (2014) arrives at the same conclusions suggesting that, although more diverse, MTurk workers are on average younger, overeducated, underemployed, less religious and more liberal when compared to random US sample. Although these authors argue that MTurk workers pool is at least equally good as the traditional experimental participants, they suggest that an MTurk sample should not be regarded as representative (Paolacci and Chandler, 2014). Lastly, there is growing and concurring evidence that the data obtained over MTurk support the findings of classical experiments conducted in the traditional lab.[17]

Both experimental treatments were coded in an online software called LIONESS[18] After reading and accepting the HIT containing a short description of the task and information disclosure statement[19], the participants entered the experiment by clicking on a link. After the Welcome page, they were guided through the game instructions and control questions. Due to potential high dropout rates the participants were informed that they will be granted a $1 participation fee after the successful completion of comprehension questions related to the rules of the game. Thereupon, the participants are randomly paired in a "lobby" and are guided through the decision steps and presented final results. Before receiving a randomly generated number based on which they were paid, the participants had to fill out a short survey consisted of several demographic questions. Furthermore, they were asked

[16] For an important discussion about the fairness of the compensation rates on MTurk see: Samuels (2018).
[17] For examples see: Horton et al. (2011); Klein et al. (2014) and Paolacci et al. (2010).
[18] See LIONESS webpage for further information: https://lioness-lab.org/about-us/
[19] For both of the treatments I applied exactly the same HIT description in order to avoid any potential self-selection bias (Horton et al. 2011 p. 415). The HIT description can be found in Appendix 3.

whether or not they have played a similar game before and if the game that they played reminded them of something that they have encountered in real life.[20] Lastly, no deception was used in either of the two treatments.

All of the experimental sessions were conducted between 16th and 24th of April 2019 with a starting time between 4 and 7pm (CEST). I conducted 6 sessions of Blockchain treatment and 7 sessions of the original Trust treatment yielding in total, 950 participants, 454 and 496 participants respectively. Following the suggestions of good practice from Arechar et al. (2017), I restricted the participants to be from the US with at least 95% HIT approval rate and with at least 500 previous HITs approved. These restrictions were expected to contribute to the exclusion of potential inattentive and inexperienced workers with the aim of lowering down the drop-out rates during the experiment. Furthermore, I utilized the option in the LIONESS softer that allowed me to omit the double entry of the participants within the session by partial IP address tracking. When it comes to double entries across sessions I used "Unique Turker" identifier[21] by which I prohibited reentering of the participants that have already participated in any of the two treatments.

When it comes to the characteristics of the sample, in the Blockchain treatment the average age of the participant was 36 (sd=11.01) ranging from 18 to 69, and 52% were male. In the Trust treatment the average age is 36 (sd=10.5) ranging from 20 to 71, and 55% were male. Out of the participants from both treatments taken together, 21% have previously taken part in an experiment similar to this one, 30% in the Trust treatment and 25% in the Blockchain treatment. Furthermore, an overview of descriptive statistics of game-related variables (see Table 1) provides some important information prior to the analysis. FMs in the Blockchain treatment on average transfer roughly 1.5 points more than the FMs in the Trust treatment before investment multiplication. The mean values are 7.6 points (sd=3.1) and 6.18 (sd=3.8) respectively. SMs in the Blockchain treatment on average return 10 points or 45% of the transferred amount after multiplication. On the other hand, SMs in the Trust treatment on average return 6.6 points back or 35% of the invested amount after multiplication. Lastly, final earnings of the FMs in Blockchain treatment are higher than the final earnings of the FMs in the Trust treatment. Earnings of the SMs in both treatments are roughly the same,

[20] Instructions, control questions and questionnaires for both treatments can be found in Appendix 4.

[21] For details see Arechar et al (2017) and Unique Turker webpage: http://uniqueturker.myleott.com/

with a difference of 0.7 $US cents. To improve readability, I present the results of hypothesizes testing for the first and the second mover separately.

Table 1: Descriptive Statistics
Blockchain treatment

Variable	Obs	Mean	Std.Dev.	Min	Max
Amount transferred x 3	248	18.556	11.392	0	30
Amount returned	248	6.637	6.771	0	30
Proportion returned	212	.349	.25	0	1
Previous Experience	492	.23	.421	0	1
Gender	492	.48	.5	0	1
Age	492	36.23	10.508	20	71
Earnings FM	248	10.452	5.385	0	30
Earnings SM	248	21.919	9.045	10	40
Earnings combined	496	16.185	9.394	0	40

Trust treatment

Variable	Obs	Mean	Std.Dev.	Min	Max
Amount transferred x 3	227	22.982	9.375	0	30
Amount returned	227	10.332	5.183	0	30
Proportion returned	216	.45	.129	.333	1
Previous Experience	450	.2	.4	0	1
Gender	450	.442	.497	0	1
Age	450	36.393	11.01	18	69
Earnings FM	227	12.696	3.166	10	30
Earnings SM	227	22.626	5.893	10	30
Earnings combined	454	17.661	6.858	10	30

5. Analysis of the results and Discussion

a. Analysis

First mover behavior

In order to test H1, I created a dummy variable *Investing decision* indicating FM's decision to enter the game and transfer any amount of the initial 10 points to SM. I coded *Invest* as 1 and *Not invest* as 0. Firstly, I conducted a Chi-squared test between *Investing decision* and a dummy treatment variable, capturing the type of treatment (0 being Trust

treatment and 1 being Blockchain treatment). The results indicate that the relationship between the decision to invest and the treatment groups is statistically significant (N = 475, p < 0.001). In the Trust treatment 14.52% of FMs decided not to invest, compared to only 4.85% of FMs in the Blockchain treatment. This corresponds to a difference of roughly 10%. Furthermore, I conducted a logistic regression on the focal relationship with the inclusion of gender, age and previous experience as controls. The results (not presented) point that FMs in the Blockchain treatment are more likely to decide to invest than FMs in the Trust treatment (p < 0.001). As expected, control variables did not affect the focal relationship and were statistically insignificant. Therefore I conclude that the data provides support for H1.

In order to test H2 I conduct a two-sample t-test. The results show that the difference in the mean amount of points of FM's investment between the Trust and Blockchain treatment is almost -1.5 and statistically significant (t (473) = -4.59, p < 0.001). In other words, on average, FMs in the Blockchain treatment invest about 1.5 points more than the FMs in the Trust treatment. When it comes to the effect size, computed Cohen's d value of 0.42 indicates that the difference in the size of FM's investment between the treatments is 0.42 standard deviation. Following Mitchell (2015), I would argue that the Blockchain treatment has medium effect when it comes to the behavior of the FMs. Lastly, omega-squared value of the ANOVA test showed a value of 0.04 indicating that the Blockchain treatment explains 4% of the variance of the amount invested by FM. Therefore, I conclude that that the data provides support for H2.

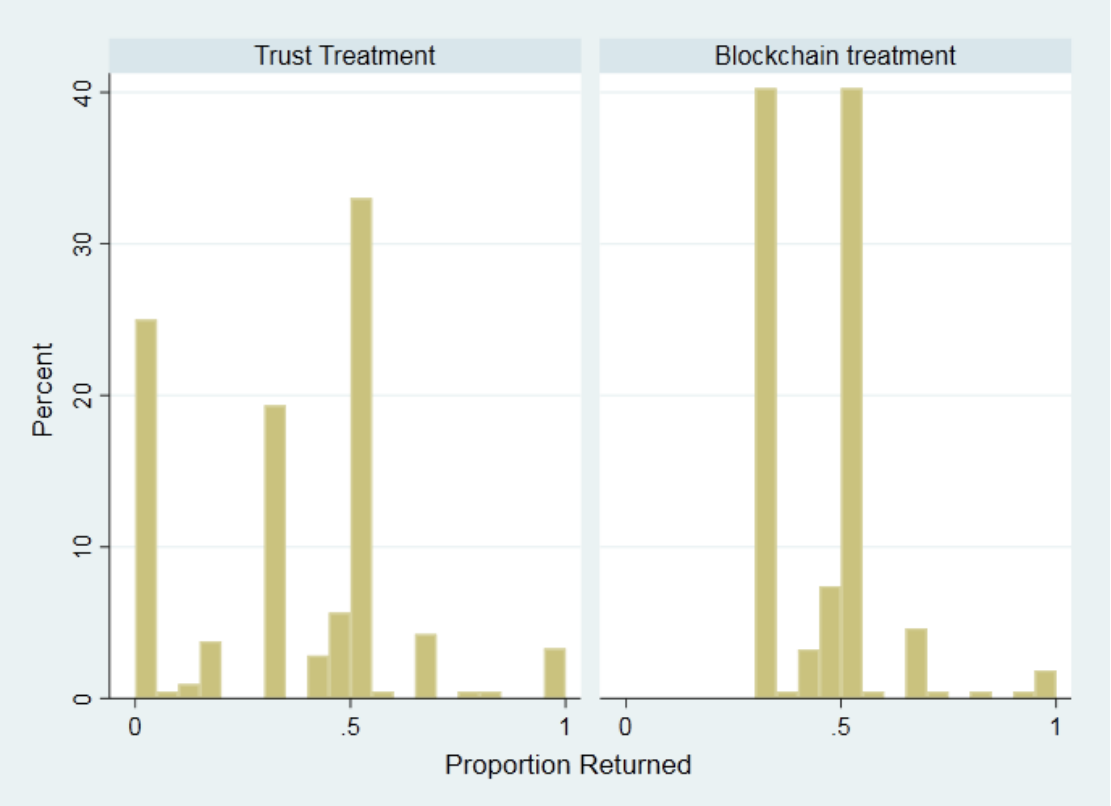
Second mover behavior

The behavior of the SM is addressed in hypothesizes 3 to 5. According to H3, I expect that the proportion returned by SM would be *lower* in the Blockchain treatment compared to the Trust treatment. In order to test this hypothesis, I created a focal dependent variable *Proportion returned* by dividing the amount of points returned by SM with the amount of points sent after multiplication by FM (see descriptive statistics in Table 1). I test H3 by using a two-sample t-test with *Proportion returned* as the main dependent variable. The results suggest that there is a statistically significant difference between the means of SM's *Proportion returned* in the two treatments (t (426) = -5.25, p < 0.001). Contrary to the expectation, SMs in the Blockchain treatment return 10% more than their counterparts in the Trust treatment. On average, SMs in the Trust treatment return 34,8% of the invested amount (sd = 0.24) compared to 44.9% (sd = 0.12) in the Blockchain treatment. Cohen's d value of

0.5 indicate a medium size effect of the Blockchain treatment and omega-squared value of the ANOVA test showed a value of 0.058 indicating that the Blockchain treatment explains 5.8% of the variance of the proportion returned by the SM. Therefore, there results show that I have to reject hypothesis 3, due to statistically significant results in support for the opposite claim.

Yet, because of the features of the experimental design, one could argue that due to the existence of the lower boundary for the return rate in the Blockchain treatment (minimal return rate > 0), the SMs that would have otherwise behaved "greedy" and returned 0 points back, were forced to return at least one third of the amount sent after multiplication (see Graph 1 for distributions of the *Proportion returned*). If this is the case, based on the data gathered, it is impossible to qualitatively differentiate between "greedy" and contract-abiding SMs. Yet, it is possible to assume that all of SMs in the Blockchain treatment who returned the minimal amount are either 1) "greedy" or 2) contract-abiding. Assuming that they are all "greedy", I created a new variable called *Voluntary proportion returned* in which I recoded the 0.33 observations in the Blockchain treatment as 0. This was done in order to check whether there is a difference in the proportion returned when only voluntary returns are taken into account. The results of the two-sample t-test of *Voluntary proportion returned* and a treatment dummy show that there is no meaningful difference between the means of focal dependent variable in the two treatments. Furthermore, p value of 0.186 indicate that I cannot reject the null hypothesis. Therefore, these results suggest that the Blockchain treatment does not affect the behavior of SMs who *voluntarily* retuned some amount of points back to FM.

Graph 1: Distributions of the proportion returned by treatment



On the other hand, assuming that SMs in the Blockchain treatment are all contract-abiding individuals, it is worth testing the difference between treatments in the probability that the SM will return one third of the invested amount. I created a new dummy variable *1/3 proportion returned* that takes the value of 1 if the amount sent is 0.33 and 0 otherwise. Observations from the trust treatment that are between 0 and 0.33 are coded as 0 since the decision to invest any amount within this interval could still be regarded as "greedy" behavior. If SM returns the amount between 0 and 0.33, FM ends up with less than what he got at the beginning of the game. Doing so, I am able to compare "non-greedy" SMs in the trust treatment to contract-abiding SMs in the Blockchain treatment. Indeed a Chi-squared test on a dummy variable *1/3 proportion returned* across treatments indicate a statistically significant difference (N = 428, p value < 0.001). More specifically, in the Trust treatment 19.3% of the SMs decided to return 1/3 of the invested amount, compared to 40.3% of the SMs in the Blockchain treatment. This corresponds to a difference of 21%.[22]

[22] The results of a logistic regression with the inclusion of age, gender and previous experience as controls confirm the results (not shown) All control variables were insignificant at 95% confidence interval.

Lastly, I test hypothesizes 4 and 5 concomitantly by utilizing an OLS regression with robust standard errors. I use the variable *Amount returned* as the focal dependent variable and *Amount sent* as the focal independent variable. The results are shown in Table 2. Model 1 presents the results for the Trust treatment and Model 2 for the Blockchain treatment. The effect of the amount transferred on the amount returned is positive and statistically significant at the 99.9% level in both models.[23] Furthermore, a one point increase in the amount transferred by the FM leads to a 1.08 points increase in the amount returned in the Trust treatment and 1.37 points increase in the amount returned in the Blockchain treatment. Lastly, model 4 presents an interaction effect of the *Treatment dummy* (Trust treatment coded as a reference category) and *Amount transferred*. The results indicate that a one point increase in the amount sent in the Blockchain treatment leads to a 0.28 points increase in the amount returned, compared to the amount returned in Trust treatment. The results are statistically significant at the 99% level.[24]

Table 2: OLS regressions testing hypothesizes 4 and 5

	Trust Treatment (1) Amount returned	Blockchain Treatment (2) Amount returned	Treatment Control (3) Amount returned	Interaction effect (4) Amount returned
Amount sent	1.084***	1.368***	1.193***	1.084***
	(0.0829)	(0.0477)	(0.0550)	(0.0829)
Treatment dummy			1.960***	-0.0515
			(0.450)	(0.406)
Amount sent # Treatment dummy				0.283**
				(0.0957)
Intercept	-0.0698	-0.121	-0.741***	-0.0698
	(0.281)	(0.294)	(0.218)	(0.281)
Observations	248	227	475	475
R^2	0.370	0.677	0.517	0.522
Adjusted R^2	0.367	0.676	0.515	0.519

Robust standard errors in parentheses; Reference category for treatment dummy variable is Trust treatment.
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

[23] Introducing Gender, Age and Previous Experience as control variables (not presented) in both Model 1 and 2 for Trust and Blockchain treatments respectively do not change the coefficients in a meaningful way. As expected, all the control variables were statistically insignificant.

[24] Interested reader may find a plot of marginal effects in the Appendix 5.

Therefore, the results indicate support only for the hypothesis 5. On the other hand, a positive relationship between the amount returned and amount transferred in the Blockchain treatment indicate that I have to reject H4. Moreover, the tested relationship is, contrary to the expectations, stronger in the Blockchain than it is in the Trust treatment.

b. Discussion

In this section I discuss the implications of the results in terms of the trust-control nexus and, more broadly, suggest how the results might be interpreted when it comes to the possible applications of Blockchain technology. Also, I present and discuss a set of potential factors of the experimental design itself that might have had an effect of the results I obtained. As it was done in the analysis, I discuss the behaviour of the FMs and the SMs separately.

Trust –Control Nexus

The results presented in the previous section indicate that the probability of deciding to invest in the Blockchain treatment is 10% higher compared to the Trust treatment. Furthermore, the amount invested in the Blockchain treatment is on average 1.5 points higher than the one in the Trust treatment. Following the interpretation of the behavior in Trust games (Johnson and Mislin, 2011), the results indicate that FMs in Blockchain treatment seems to *trust* more than their counterparts in the Trust treatment. Yet, due to the fact that risk is by design omitted from the relationship it could be argued that the behavior observed is not one of trust. In spite of this potential operationalization issue, during the construction of the experimental design I opted for the treatment presented due to two key reasons. Firstly, it was necessary to operationalize the technological aspects of Blockchain in the best possible way which included the necessity of omitting risk from the relationship. Secondly, constructing the Blockchain treatment in a way that includes non-human related risk[25] would produce incomparable samples and further complicate the coding procedure in LIONESS.

In terms of the discussion of the relationship between trust and control, it seems that the results are in support of the complementarity perspective in which trust and control can go hand in hand. Sitkin (1995) argues that "formal control mechanisms may increase trust by

[25] One option was to include a 1 point "transaction cost of contract use" to the FM in order to include a possibility of receiving less than it was sent before the multiplication, thus creating a risk for the second mover.

providing people with objective rules and clear measures on which to base their assessments and evaluations of others. Trust and control can both contribute to the level of cooperation needed in a relationship." (in: Bijlsma-Frankema and Costa, 2005 p. 270).

In terms of the behavior of the second mover, contrary to my expectations, hypothesizes 3 to 5 provide support for the complementarity perspective as well. By returning on average a 10% bigger proportion of the amount invested, SMs in the Blockchain treatment behave more trustworthy than their counterparts in the Trust treatment (H3). Furthermore, unexpectedly, even though FMs in the Blockchain treatment operate in a risk-free environment, SMs do reciprocate by sending 1.5 points more with each 1 point increase invested by FM (H5). Therefore, it seems that control mechanisms embedded in the contractual clause of the Blockchain treatment create a *reciprocity enhancing environment*. Opposite to a similar experiment done by McCabe et al. (2003) in which the authors restrict the possibility of the FM to signal trusting behavior, this experiment shows that, even though there is no risk involved in the relationship, when FMs are capable of signaling the expectations from their game counterparts, SMs are still prone to reciprocate "trusting" behavior.[26]

The follow up analysis of the H3 in which the results showed that the probability of returning the minimal 33% of the amount invested could be perceived as a test for alternative hypothesis 3. Here, I would expect that the decision to return the minimal amount is more probable in the Blockchain treatment than in the Trust treatment. Although the results provided support for this hypothesis, they are dependent on the assumption that *all* SMs in the Blockchain treatment that did return the minimal amount 1) exhibited a contract-abiding behavior and 2) are not "greedy". The necessity of introducing these two assumptions comes from the need for conceptually just comparative purposes across treatments in which the return rates smaller than 33% of the amount invested in the trust treatment are coded as 0. Yet, it is highly unlikely that some portion of SMs who returned the minimal amount in the Blockchain treatment would have not otherwise returned less if there was no contractual clause that forbid them to do so. In other words, it is reasonable to argue that some portion of

[26] It is important to note that reciprocal behavior cannot be equalized with altruistic behavior due to the fact that reciprocal behavior results in unequal final earnings in which the earnings of the SM are bigger. On the contrary, altruistic behavior of the second mover would result in the final earnings being equal or bigger for the FM. The results presented in this paper indicate that this is clearly not the case (see Table 1 for descriptive statistics)

SMs in the Blockchain treatment that returned the minimal amount did so due to utility maximizing, "greedy" preferences.

One way to approximate the percentage of contract-abiding "non-greedy" participants in the Blockchain treatment is to subtract the number of "greedy" participants from the Trust treatment (proportion returned between 0 and 0.33) from the number of participants that returned the minimal amount in the Blockchain treatment. After the subtraction, out of 87 participants, 34 participants (39%) could be regarded as contract-abiding. Although these results might indicate some support for the claim that control crowds out reciprocating behavior (which is the same underpinning reasoning behind hypothesis 3), I refrain from such conclusions and suggest further research in order to account for the differences between contract-following and "greedy" individuals.

Therefore, taken together the results show support for the complementarity perspective of the trust-control relationship. Indeed, in the words of Poppo and Cheng (2018) it seems that trust and contract reinforcement "address the limitations of each other" (p. 229). Especially in the cases where the trustor does not have any information of the trustee's previous behavior, contract reinforcement might prove essential for the improvement of the relationship. Furthermore, Poppo and Cheng (2018) present a overview of similar studies and conclude that there is greater overall support that contracts and trust combined promote better performance, rather than substitute each other in a way in which their combination weakens or destroys it. Indeed, based on the two-sample t test analysis of final earnings in the two treatments, on average participants from the Blockchain treatment earn 1.48 points more than the participants in the Trust treatment ($t(948) = -2.74$, $p < 0.01$).

Implications for Blockchain technology

On the condition that the operationalization of the presented key features of the technology is theoretically sound, I would argue that Blockchain-based smart contracts would indeed act as a "trust machine". Yet, paradoxically, higher levels of both trusting and trustworthy behavior were obtained in a trust/risk-free environment through a restrictive control system. In terms of reciprocal behavior, although both players understood that the behavior of the first mover could not be viewed as a trusting decision, contrary to the expectations, second movers did indeed reciprocate and returned comparatively more than their counterparts in the Trust treatment. Moreover, the comparison of the final earnings in both treatments indicates support that Blockchain-based relationships could produce better

performance in terms of monetary rewards. Therefore, counter-intuitively, Blockchain technology could be understood as *trust-free trust machine*.

Furthermore, as it was noted in the theoretical section I assume that both the participants of the experiment and the potential future users of Blockchain-based services trust the technology itself when entering a relationship with another individual. As it was shown in the review of the previous research on Bitcoin and Ethereum users, this is not always the case. Therefore, it is worth discussing how this issue might have had an effect in the experimental operationalization itself. In the context of the study, the participants had to trust the experimenter that they will get their final earnings according to the rules of the game presented in the instructions. I argue that the lack of trust in the experimenter was highly unlikely to occur due to the MTurk secure pay feature. A so called "batch" of HITs cannot be published unless there are enough funds on the experimenter's account to pay for the asked work. Even though there is a possibility that some of the MTurk workers are not familiar with this Amazon feature, it is indicative that, unless the requester denies the payment due unsatisfactory work, the workers will always get paid.

Another important difference between the experimental operationalization and the way smart contracts are expected to function is the difference in the actor who stipulates the contractual rules. As an experimenter, I created the contractual rules that the participants had to agree to follow, contrary to the smart contract mechanism in which the contractors *ex ante* create the rules themselves. This could problematize the operationalization in two distinct ways. Firstly, by constructing the contractual rules, I have probably incorporated my own social norms on what is the "fair" amount returned.[27] Secondly, experimental settings lack wider social context that might have an influence on the specification of the contractual rules and the behavior of the participants.[28] In spite of these potential issues I argue that the results presented in this paper are a good starting point in the experimental Blockchain research. I argue that the results of the experimentally induced "private social ordering" (Sklaroff, 2017

[27] The decision to create a contract based on which the SM must return the minimal amount sent was made following the key aspects of technology. Smaller minimal return would create risky investment conditions (see footnote 18), while introducing larger minimal returns would have to be based on the assumption that first movers are utility maximising individuals. The option in which the First mover only knows that he cannot lose any value when investing allowed me to investigate both players' behavior in a risk-free environment without the need for introducing any additional assumptions.

[28] For an example of contextualized experimental design see: Hajikhameneh and Kimbrough (2017)

p. 268) do indicate that the participants do not need to trust each other or rely on an intermediary in order to securely (and more efficiently) accommodate their own needs.

Lastly, the contract under which the participants of the experiment operated in was based on only one contractual rule. If the implementation of Blockchain-based contracts is to be successful, it has to be capable of securing and enforcing more complicated rules in order to accommodate the actual business and/or governmental needs. Yet, as previously noted, encoding all the potentially important aspects of a relationship in a smart contract before its employment is almost an impossible task to accomplish. Furthermore, even with the exclusion of the intermediary, the costs of devising and encoding rules of the agreement might surpass its potential benefits. In spite of these downsides, the results presented in the paper indicate that the potential future implementation, if done properly, might prove to bear positive effects on the level of trust and trustworthiness in human-to-human relationships.

Potential factors of the experimental design

There are four potential issues of the experimental design that might unintentionally influence the behavior of the participants. Firstly, when it comes to Blockchain treatment effect, one could argue that the participants have not understood the meaning of "entering the contract". Yet, I argue that this is not likely the case due to the fact that one of the comprehension questions for both players before the actual game was directly related to the behavior of the second mover. Only the participants that have answered the question correctly were able to enter the game. Furthermore, in the questionnaire after the game, I asked the participants if they have played similar games before and in case they did I asked them to describe the differences between previous games and the one presented here. In the Blockchain treatment, almost all of the participants that have played similar games before answered that the main difference between those games and mine is the obligation to return the minimal amount sent. I understand this to be an indirect but sufficient proof that the instructions were clear and the treatment effective.

Secondly, it could be argued that the incentives in both treatments were too low to promote utility maximizing behavior. To reiterate, the participants received a flat fee of 1$ after the successful completion of the comprehension quiz and could be awarded an additional prize of maximum 30 cents. Although the earnings for the time spent on the experiment were average compared to other HITs published on MTurk, an addition of a maximum of 30 cents might seem too small. Yet, when the averages of the amount sent and

proportion returned are compared to the results of the meta-analysis of trust games (see: Johnson and Mislin, 2011; table 1 p. 871), it seems that there are no major differences. In the meta-analysis, the FMs send on average 50% of their initial endowments and SMs return 37% back. Therefore, I would argue that, even though the incentives for play in my experiment were relatively small, they did not have a major impact on the behavior of both the first and the second mover.

Thirdly, one of the reasons that might explain the observed reciprocal behavior even in the Blockchain treatment might be due to unaccounted effects of broad social control (Hardin, 2002) within the MTurk community. Although, to the best of my knowledge, there is still no research on possible effects of social norms formation within the MTurk community, it is reasonable to assume that workers on the Amazon platform might have shared values, beliefs and goals that would constitute the basis of clan control (Das and Teng, 2001). If this is indeed the case, one could argue that this might be the reason why most of the second movers returned some of the amount invested even though it is impossible for the participants to know who the person that they are playing the game with is. In other words, being a "Turker" could produce other-regarding internalized norms through which the participants of the experiment avoided "greedy", utility-maximizing behavior.

Fourthly and lastly, in the experiment presented in this paper, I did not check for the potentially differing effects of repeated games. As it was indicated before, both treatments are one-shot games based on the Berg et al. (1995) trust game. The strongest critiques of one-shot trust games in general is that, since trust relationship is a process, they cannot capture trust-building or trust-impairing behavior (see for example: Hardin, 2002).[29] Furthermore, in the case of the Blockchain treatment, iteration in a risk-free contractual environment might produce differing results as well. Although the results of such an experiment might be important for the better understanding of the relationship between trust and control, I opted for the one-shot design for several reasons. As noted, on the conceptual level, since Blockchain is mostly used today for one-time transaction purposes between anonymized parties, I decided to restrict my analysis on one-shot games only. Furthermore, on a more practical note, iterated trust games are more complex to code, last longer and are more expensive to conduct.

[29] For repeated trust games see for example: Bohnet, Frey and Huck (2001); Eckel and Wilson (2004) and Houser et al. (2010).

6. Conclusion

In this paper I aimed at presenting and testing a new in-depth theory on trust and Blockchain technology. As outlined in the theoretical section, I argued that this technology should be understood to provide the base for a trust-free relationship. Furthermore, I argued that this "trust-free" feature is based on a strong control mechanism that was not previously specified within the literature. Following the argumentation based on the discussion regarding the relationship between trust and control (Bijlsma-Frankema and Costa, 2005) and based on the *reciprocity hypothesis* presented by McCabe et al. (2003), I hypothesized that Blockchain-based systems such as smart contracts would crowd out trust from the human relationship.

In order to test this claim, I conducted an experiment on an online sample of US citizens. Building on the experimental design of a simple Trust game by Berg et al. (1995) I constructed a treatment with the aim of operationalizing the key features of the technology. The comparison of the results between the Trust and Blockchain treatments showed that, contrary to expectations, SMs in the Blockchain treatment did reciprocate and on average returned around 10% more than their counterparts in the Trust treatment. These findings suggest that, even when risk is not included in the decision to invest, SMs exhibit trustworthy behavior. Therefore, the results presented in the paper indicate that the potential future implementation of Blockchain technology, if done properly, might prove to bear positive effects on the level of trust and trustworthiness in human-to-human relationships. In terms of the implications for Blockchain technology in general, the result provided support that Blockchain technology should be understood as both a trust-free and a trust-building machine.

Thus, taken together, I aimed at contributing to the literature in two distinct ways. Firstly, I offered a new theoretical understanding of trust and Blockchain technology and linked it to the wider discussion of the relationship between trust and control. Secondly, I empirically tested the presented hypothesizes in an original manner utilizing experimental methodology. When it comes to the potential future research I suggest that the main focus should be on disentangling the "greedy" from contract-abiding participants by devising a more complex experimental design. Furthermore, it would be important to test the proposed hypothesizes by running iterated Trust and Blockchain treatments and therefore, answer to the critiques related to the understanding of trust relationship as a process (Hardin, 2002).

Lastly, further research about the MTurk community is needed in order to assess whether workers have a sense of group belonging and therefore might influence their decisions in an experiment.

References

Arechar, A.A., Gächter, S. and Molleman, L., 2018. Conducting interactive experiments online. *Experimental Economics*, *21*(1), pp.99-131.

Arruñada, B., 2018. Blockchain's struggle to deliver impersonal exchange. *Minn. JL Sci. & Tech.*, *19*, p.55.

"Awesome Non-financial Blockchain" (undated) *Github commit*. Retrieved from: https://github.com/machinomy/awesome-non-financial-blockchain (last visit: 10. 05. 2019.)

Babbitt, D. and Dietz, J., 2014. Crypto-economic design: a proposed agent-based modeling effort. In *English. Conference Talk. University of Notre Dame, Notre Dame, USA*.

Beck, R., Czepluch, J.S., Lollike, N. and Malone, S., 2016, May. Blockchain-the Gateway to Trust-Free Cryptographic Transactions. In *ECIS* (p. ResearchPaper153).

Beldad, A., De Jong, M. and Steehouder, M., 2010. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in human behavior*, *26*(5), pp.857-869.

Berg, J., Dickhaut, J. and McCabe, K., 1995. Trust, reciprocity, and social history. *Games and economic behavior*, *10*(1), pp.122-142.

Bijlsma-Frankema, K. and Costa, A.C., 2005. Understanding the trust-control nexus. *International Sociology*, *20*(3), pp.259-282.

Bohnet, I., Frey, B.S. and Huck, S., 2001. More order with less law: On contract enforcement, trust, and crowding. *American Political Science Review*, *95*(1), pp.131-144.

Boulianne, Shelley. "Does Internet use affect engagement? A meta-analysis of research." *Political communication* 26, no. 2 (2009): 193-211.

Buhrmester, M., Kwang, T. and Gosling, S.D., 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data?. *Perspectives on psychological science*, *6*(1), pp.3-5.

Davidson, S., De Filippi, P. and Potts, J., 2016. Economics of blockchain. *Available at SSRN 2744751*.

Das, T.K. and Teng, B.S., 2001. Trust, control, and risk in strategic alliances: An integrated framework. *Organization studies*, *22*(2), pp.251-283.

De Filippi, P., 2017. What blockchain means for the sharing economy. *Harvard Business Review Digital Articles*, pp.2-5.

Economist (2015a). Blockchain - The next big thing. Retrieved from: http://www.economist.com/news/ special-report/21650295-orit-next-big-thing (last visit: 19. 03. 2018.)

Economist (2015b). The Great Chain of Being Sure about Things. Retrieved from: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (last visit: 10.05. 2019.)

Eckel, C.C. and Wilson, R.K., 2004. Is trust a risky decision?. *Journal of Economic Behavior & Organization*, *55*(4), pp.447-465.

Fröwis, M. and Böhme, R., 2017. In Code We Trust?. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 357-372). Springer, Cham.

Galati, F., (2018, March 26th). "Blockchain as a Process: Ideologies and Motivations behind the Technology" *Medium.* Retrieved from: https://medium.com/coinmonks/blockchain-as-a-process-ideologies-and-motivations-behind-the-technology-c25219d87881 (last visit 10. 04. 2019.)

Gambetta, D., 2000. Can we trust trust. *Trust: Making and breaking cooperative relations*, *13*, pp.213-237.

Glaeser, E.L., Laibson, D.I., Scheinkman, J.A. and Soutter, C.L., 2000. Measuring trust. *The quarterly journal of economics*, *115*(3), pp.811-846.

Glaser, F., 2017. Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Greiner, M. and Wang, H., 2015. Trust-free systems-a new research and design direction to handle trust-issues in P2P systems: the case of Bitcoin.

GovLab (undated) "Curated Examples" Retrieved from: https://blockchan.ge/curatedexamples.html (last visit: 10. 05. 2019)

Greiner, M. and Wang, H., 2015. Trust-free systems-a new research and design direction to handle trust-issues in P2P systems: the case of Bitcoin.

Hardin, R., 2002. *Trust and trustworthiness*. Russell Sage Foundation.

Hajikhameneh, A. and Kimbrough, E.O., 2017. Individualism, collectivism, and trade. *Experimental Economics*, pp.1-31.

Hawlitschek, F., Notheisen, B. and 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*, pp.50-63.

Horton, J.J., Rand, D.G. and Zeckhauser, R.J., 2011. The online laboratory: Conducting experiments in a real labor market. *Experimental economics*, *14*(3), pp.399-425.

Houser, D., Schunk, D. and Winter, J., 2010. Distinguishing trust from risk: An anatomy of the investment game. *Journal of economic behavior & organization*, *74*(1-2), pp.72-81.

Huckle, S. and White, M., 2016. Socialism and the blockchain. *Future Internet*, *8*(4), p.49.

Johnson, N.D. and Mislin, A.A., 2011. Trust games: A meta-analysis. *Journal of Economic Psychology*, *32*(5), pp.865-889.

Karch, B., (2018 October 10th). "Five Use Cases for Blockchain in Financial Services" *Accenture*. Retrieved from: https://financialservicesblog.accenture.com/five-use-cases-for-blockchain-in-financial-services (last visit: 10. 05. 2019.)

Klein, R.A., Ratliff, K., Vianello, M., Adams Jr, R.B., Bahník, S. and Bernstein, M.J., 2014. Investigating variation in replicability: A "many labs" replication project. Open Science Framework.

Knack, S. and Keefer, P., 1997. Does social capital have an economic payoff? A cross-country investigation. *The Quarterly journal of economics*, *112*(4), pp.1251-1288.

Kshetri, N., 2017. Will blockchain emerge as a tool to break the poverty chain in the Global South?. *Third World Quarterly*, *38*(8), pp.1710-1732.

Kumar, A., (2018, November 12th). "Does the Internet Brings Us Closer?" *Medium*. Retrieved from: https://medium.com/@abhishekkumar020591/does-the-internet-bring-us-closer-29064c7f1abf (last visit 10. 05. 2019)

Lustig, C. and Nardi, B., 2015, January. Algorithmic authority: The case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences* (pp. 743-752). IEEE.

McCabe, K.A., Rigdon, M.L. and Smith, V.L., 2003. Positive reciprocity and intentions in trust games. *Journal of Economic Behavior & Organization*, *52*(2), pp.267-275.

Mitchell, M.N., 2015. *Stata for the behavioral sciences*. College Station, TX: Stata Press.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

Paolacci, G., Chandler, J. and Ipeirotis, P.G., 2010. Running experiments on amazon mechanical turk. *Judgment and Decision making*, *5*(5), pp.411-419.

Paolacci, G. and Chandler, J., 2014. Inside the Turk: Understanding Mechanical Turk as a participant pool. *Current Directions in Psychological Science*, *23*(3), pp.184-188.

Pazaitis, A., De Filippi, P. and Kostakis, V., 2017. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Technological Forecasting and Social Change*, *125*, pp.105-115.

Poppo, L. and Cheng, Z., 2018. Complements versus substitutes in business-to-business exchanges. *The Routledge Companion to Trust*.

Porta, R.L., Lopez-De-Silane, F., Shleifer, A. and Vishny, R.W., 1996. *Trust in large organizations* (No. w5864). National Bureau of Economic Research.

Putnam, R.D., Leonardi, R. and Nanetti, R.Y., 1994. *Making democracy work: Civic traditions in modern Italy*. Princeton university press.

Putnam, R.D., 2000. Bowling alone: The collapse and revival of American community. New York, NY, US.

Raskin, M., 2016. The law and legality of smart contracts.

Raval, S., 2016. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. " O'Reilly Media, Inc.".

Richey, S., 2010. The impact of corruption on social trust. *American Politics Research*, *38*(4), pp.676-690.

Riegelsberger, J., Sasse, M.A. and McCarthy, J.D., 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*, *62*(3), pp.381-422.

Rothstein, B., 2011. *The quality of government: Corruption, social trust, and inequality in international perspective*. University of Chicago Press.

Rothstein, B., 2013. Corruption and social trust: Why the fish rots from the head down. *social research*, *80*(4), pp.1009-1032.

Rothstein, B. and Teorell, J., 2008. What is quality of government? A theory of impartial government institutions. *Governance*, *21*(2), pp.165-190.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C., 1998. Not so different after all: A cross-discipline view of trust. *Academy of management review*, *23*(3), pp.393-404.

Santiso, Carlos. (2018, March 5th). "Will Blockchain Disrupt Government Corruption?" *Stanford Social Innovation Review*. Retrieved from: https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption?utm_campaign=crowdfire&utm_content=crowdfire&utm_medium=social&utm_source=facebook_page#827476593980853-fp#1520327374341 (last visit: 19. 03. 2018.)

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

Semuels, A., (2018, January 23rd). "The Internet is Enabling a New Kind of Poorly Paid Hell" *The Atlantic*. Retrieved from: https://www.theatlantic.com/business/archive/2018/01/amazon-mechanical-turk/551192/ (last visit 10. 05. 2019)

Sitkin, S.B., 1995. On the positive effects of legalization on trust. *Research on negotiation in organizations*, *5*, pp.185-218.

Sklaroff, J.M., 2017. Smart contracts and the cost of inflexibility. *U. Pa. L. Rev.*, *166*, p.263.

Sun, J., Yan, J. and Zhang, K.Z., 2016. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1), p.26.

Swan, M., 2015. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

"UAE aims to be at forefront of global technology innovation" (2016, November 23rd) *The Economist Intelligence Unit.* Retrieved from: https://country.eiu.com/article.aspx?articleid=574843641 (last visit: 10. 05. 2019)

Uslaner E. M. 2004. Trust, civic engagement, and the internet, *Political Communication*, Vol. 21, pp. 223-242.

van der Werff, L., Real, C. and Lynn, T., 2018. Individual trust and the internet.

V. Shah, Nojin Kwak, R. Lance Holbert, Dhavan. "" Connecting" and" disconnecting" with civic life: Patterns of Internet use and the production of social capital." *Political communication* 18, no. 2 (2001): 141-162

Werbach, K. and Cornell, N., 2017. Contracts ex machina. *Duke LJ*, *67*, p.313.

Werbach, K., 2018a. Trust, but verify: Why the blockchain needs the law. *Berkeley Tech. LJ*, *33*, p.487.

Werbach, K., 2018b. *The Blockchain and the New Architecture of Trust*. Mit Press.

"XinFin Partners With R3 Corda, A Consortium Blockchain Platform With Over 200+ Financial Institutions" (undated) *Medium*. Retrieved from: https://medium.com/xinfin/xinfin-partners-with-r3-corda-a-consortium-blockchain-platform-with-over-200-financial-797b8bea457d (last visit: 10. 05. 2019.)

Zambrano, R., Seward, R.K. and Sayo, P., 2017. Unpacking the disruptive potential of blockchain technology for human development.

Zambrano, R., Young, A. and Verhulst, S., 2018. Connecting Refugees to Aid through Blockchain-Enabled ID Management: World Food Programme's Building Blocks.

Appendix 1

Application Examples

Although only a bit more than a decade passed since the introduction of the technology, there has been a proliferation of startups, organizations and governmental agencies that initiated the research focusing on the implementation of the technology in various areas of innovation, business and administration. Until now, the innovative use of Blockchain technology has most often been within the financial sector. One of the biggest companies that base their work on Blockchain technology is R3. This company leads a consortium of more than 200 organizations, including Barclays, Credit Suisse, Goldman Sachs, J. P. Morgan and UBS, to mention just a few (Medium, 2019). Their main goal is to produce a Blockchain based platform that "removes costly friction in business transactions by enabling institutions to transact directly using smart contracts while ensuring the highest levels of privacy and security." (The Corda Platform)[30]. Other uses within the financial sector are, for example innovative solutions for clearing and settlement, trade finance, cross-border payments and insurance contracts (Karsch, 2018).

Outside of the financial world, the technology is used in fostering independent journalism through a platform called "Civil", decentralized social network platforms such as "Steem" and distributed video sharing such as "PopChest".[31] The technology is also used for the creation of tamper-proof timestamps through which it is possible to track the origin or the creation of intellectual property, luxury goods or any sort of products or information that might be of importance to an individual. More generally, there has been a proliferation of organizations, such as "Decenter", that are trying to build platforms in order to "decentralize the internet" and as they argue, make people again in control of their digital identities and their data (Github commit, 2018)[32].

As noted, many governmental institutions became interested in the technology and its potential use. Countries such as Switzerland, Canada, Sweden, South Korea, US, UK and

[30] https://www.r3.com/corda-platform/

[31] See: "Civil": https://civil.co/ ; "Steem": https://steem.com/ ; and "PopChest": https://www.thepopnetwork.org/ .

[32] For a trusted time stamping of a digital content see "OriginStamp" (https://originstamp.org/home). SmartWater is an example of proof stamping real, physical objects (https://www.smartwater.com/). More about "Decenter" can be found at https://www.decenter.com/.

Indonesia are piloting various projects in order to digitalize their citizens' identities for purposes such as identity identification, voting, taxes and subsidy distributions (GovLab, undated). Singapore is implementing the technology to fight money laundering and India is trying to utilize the benefits of it through the implementation of Blockchain in the so called "Know Your Customer Regulations" (Karsch, 2018). Interestingly, United Arab Emirates can be seen at the forefront of the governmental use of this technology. Their government stated that by 2030 it will move all of its business transactions onto Blockchain (The Economist Intelligence Unit, 2016). In 2017, World Food Program launched a project called "Building Blocks" in order to help refugees in Jordan. By bypassing local financial sector and reducing transaction fees, the program was saving $150.000 a month by eliminating 98% of bank related fees (Zambrano, 2018 p. 4) Lastly, within the land registries regulations, several projects are being successfully developed in for example Sweden and Georgia. On the other hand, less successful applications within the land registries administration were tested in Ghana and Honduras (Santiso, 2018).

Academic Interest

Unsurprisingly, the interest in the academia is growing, especially in the most recent years. In economics, Hawlitschek et al. (2018) give a literature overview on Blockchain technology and trust in sharing economies. Since the novelty of the research area, the authors argue that it is "necessary to critically asses and discuss the 'promises' derived from a non-academic literature and media, from a scientific, well-structured and theory-grounded point of view" (Hawlitschek et al. 2018 p. 59). One of their most important findings is that the conceptualization of trust in contexts of Blockchain and sharing economy are substantially different and thus, plead for further research towards a consistent cross-disciplinary understanding of the concept of trust.

Davidson et al. (2016) understand Blockchain technology as an "economic world of complete contracts" (p. 16) and argue that Blockchain is a matter for new institutional economics. Discussing the issue of opportunism, which they understand is arising when there is an "intent and the ability of agents to exploit trust" the authors argue that in Blockchain-based environments there are no issues of opportunism simply because the agents have no ability to exploit the other party's trust (Davidson et al. 2016 p. 10). Similarly, Babbit and Dietz (2015) are introducing and defining "cryptoeconomy" as an "economy unconstrained by geography and political and legal institutions in which Blockchains rather than trusted

third parties constrain behavior of all transactions recorded on a decentralized public ledger" (in Davidson et al. 2016 p. 4). Furthermore, this means that rent seeking is severely undermined. In the context of politics, the authors suggest that governments, politicians and bureaucrats as potential rent seekers are expected to resist the implementation of Blockchain based "crypto-governance" (Davidson et al. 2016).

In Raskin (2017); Sklaroff (2017); Werbach and Cornell (2017) and Werbach (2018a), Blockchain is assessed from the juridical academic discipline. Within the discipline, smart contracts attracted the most attention due to the effects it might have on law and state regulation. Werbach (2018b) in a recently published book expanded his argumentation that law and Blockchain need each other if we are to see the implementation of the technology in the mainstream and legal economy.

Within political science, Santiso (2018) gives suggestions about the mechanism through which the government can curb corruption by using Blockchain technology. Identity verification, registration of assets such as property registry and land titling and the tracking of financial transactions are seen to be the most plausible and convenient use of the Blockchain features (Santiso, 2018). When it comes to registering assets, the author gives examples of Sweden and Georgia on one side and Ghana and Honduras on the other, as counties that are (or were) in the process of implementing Blockchain technology within the asset registry sectors. In the case of the first two countries, the implementation is giving positive results while in the second two countries the whole idea was abandoned because it did not work at all. Santiso argues that the reason for such outcomes is due to different initial conditions in the four countries. The strength of the initial institutions is a "critical condition for making Blockchain solutions work" (Santiso, 2018). Therefore, Blockchain solutions are showing positive results in Georgia and Sweden partially because the initial institutions of land registries were already in place and functioning. On the contrary, Ghana and Honduras have extremely inefficient and corrupted public service systems and the use of Blockchain solution was therefore harder to apply.[33]

[33] for readers interested in the use of Blockchain for the development of sharing economies such as Uber or AirBnB see: Pazitas et al. (2017); smart cities: Sun et al (2016). Kshetri (2017) presents the argumentation and gives examples for why and how Blockchain can help reduce poverty in the Global South.

Ideology

As it was the case with the invention of Internet, Blockchain technology is also assessed through discussions with a more ideological focus. Due to its features, Blockchain is argued to be a "cure" for both libertarian and more left-wing individuals (Economist, 2015b). Libertarian and anarchist advocates argue that due to the lack of the need for an intermediary, through the implementation of smart contracts for example, the role and importance of the state regulation would be made obsolete (Galati, 2018). On the other hand, left-wing advocates of Blockchain technology argue, based on the same argumentation, that "big tech" companies would no longer be able to collect and control personal data of its users. Furthermore, Huckle and White (2016) emphasize the cooperative aspects of Blockchain and argue that this technology is in line with the ideals of socialist societies. For some critics of the technology, Blockchain is understood to be a part of the wider "Californian Ideology" in which the proponents of its use promise "salvation through technology" (Economist, 2015b). Lastly, Davidson et al. (2016) stress the capabilities of Blockchain to be used for the advancement of book keeping and point out that the qualities of Blockchain utilized for such purposes can further foster the development of capitalist economy.

Appendix 2:

Trusting a trust-free technology?

In spite the fact that the Blockchain network is distributed, some authors argue that this does not mean that "hierarchies and inequality among peers will not take place." On the contrary, Zambrano (2017) argues that "this is exactly what seems to be happening now when it comes to…mining, coders and developers" (p. 51). In order to better understand the dynamics of such a claim I argue that there are at least two types of relationships within the Blockchain network. Moreover, I argue that these two types of relationships would have different implications for the claim that Blockchain is a "trust machine".

First of these two relationships is a horizontal one between the nodes in the network. Speaking in terms of the land registry example, this relationship would be identified between two citizens in dispute over a piece of land. If the dispute is handled through a Blockchain, the implementation of mutually agreed rules *encoded* on the ledger would most possibly result in a just solution, based on the previous immutable data about the ownership of the land. Furthermore, since the rules themselves are immutably embedded in the computer code, the implementation of such rules will not be affected by the differences not previously stated in the government policy or law, thus making the Blockchain implementation *impartial* in a sense argued by Rothstein and Teorell (2008). Therefore, I argue that in node to node/citizen to citizen relationship within the Blockchain network, we can expect to identify the conditions where trust would no longer be necessary for the network to function properly.

Second relationship within the network is a vertical one, between the individual nodes and the coders/developers of the Blockchain program. Speaking in governmental terms, the coders would in this case be the IT specialists hired by the state to write the code in order for the system to work properly. Essentially, they would be the actors who are creating the immutably embedded rules that everyone else would have to agree upon (Arruñada, 2017). Yet, if there is not enough knowledge among the citizenry about Blockchain coding (which is arguably the case even in the most developed countries), there are at least two ways of acting against the public good. Firstly, the political elite in government can, with the help of corrupted state IT specialists, curb the rules for their own private gains. Secondly, IT specialists could be seen as public servants that can "trick" both the public officials and the

citizenry by coding the rules just for their own private gain. In both cases, it can be argued, we encounter a classical principle-agent problem. [34]

Therefore, ironically, it can be argued that there is a need for high interpersonal and governmental trust before Blockchain can be implemented. Examples such as tracking food aid distribution in Jordan (see: Zambrano, 2018) and the attempts to implement the technology in the administration of land registries (see: Santiso, 2018) indicate that "the hurdle for these systems is the human actor outside the ledger. It seems that the attempt to employ a "trust-free" technology where trust is needed to begin with seems futile, if not nonsensical. Thus, the question of how to apply this technology in societies with low levels of trust is still to be answered. Although one could argue that this would be the most important question to deal with, in this paper I will try to address the question of is it really worth applying it in the first place.

[34] A similar take on the issue presented is given by Glaeser (2017) who distinguished two layers of Blockchain, a fabric and an application layer. For the author, the fabric layer is the one on which the Blockchain is produced (i.e. coders) and the application layer is the one on which the users of the network communicate. Therefore, Glaeser argues that "[r]eplacement of trusted-third party service providers might be a limited fit due to the governance centralization of the fabric layer… Decentralization and hence trust decentralization is always as good as the most basic layer" (1551p.)

Appendix 3

Description of HIT on Amazon Mechanical Turk:

Title Two Persons Decision Making Game

Description

Title of the study Two Persons Decision Making Game

Length of the study 5 to 7 minutes

Payment A flat fee of $1.00 upon completion of a quiz plus a bonus that depends on your decision and the decision of the other player.

What is this study about?

This is a study about two persons decision making. You will make decisions based on which you can receive a bonus dependent on your on other person's decisions, in addition of a flat payment of $1.00 for completing a quiz.

Voluntary participation and confidentiality

Participation in this study is entirely voluntary and may be withdrawn at any given moment without further consequences. All decisions will be made anonymously, and results will only be analyzed at the group level for publications in scientific journals.

Browser compatibility

This HIT will not work on Internet Explorer

Risks

To our knowledge there are no risks involved in participating in this survey

Informed consent

By accepting this HIT you give us informed consent that we can use your answers in anonymized form for research purposes only.

- Groups of 2 real people recruited via MTurk
- 5 to 7 minutes required, WHITOUT INTERUPTION, STARTING IMMEDIATELLY
- We can allow up to 100 participants in this group of HITs

Appendix 4:

a.) LIONESS instructions for Trust treatment

Instructions

In this experiment, you will be randomly paired with another participant. Each participant will get a 1$ participation fee after the successful completion of the quiz. Before the start of the experiment you will be randomly assigned to be either Player A or Player B and each of you will get an initial 10 points.

1 point = 1 US cent

When the game starts, Player A can decide to send some, all, or none of his/her initial 10 points to Player B. Each point sent to Player B will be tripled.

After receiving the tripled amount, Player B can decide to return some, all, or none of the received amount sent by Player A.

In case Player A decides to send zero points, both Players keep their initial 1$ participation fee and earn 10 cents (equivalent of their initial endowment of 10 points).

If Player A sends X number of points to Player B, the tripled (X*3) amount of points become Player B' property and he/she can decide whether or not he/she wants to return some or all of the received amount back to Player A. If Player B decides to return he/she can return any number of points to Player A.

This game is played once.

Examples

If Player A sends 2 points, Player B will receive 6 points. Player B can decide not to return anything to Player A or to return any number of points between 1 and 6.

If Player A sends 9 points, Player B will receive 27 points. Player B can decide not to return anything to Player A or to return any number of points between 1 and 27.

Control Questions

If you are Player A and have 10 points, how many points can you transfer at most?

If you are Player B, after receiving 16 points from Player A, how many points at most can you transfer back?

If you are Player B, after receiving 24 points from Player A, how many points you are obliged to return back?

b.) LIONESS instructions for Blockchain treatment

Instructions

In this experiment, you will be randomly paired with another participant. Each participant will be paid a 1$ participation fee after the successful completion of the quiz. Before the start of the experiment you will be randomly assigned to be either Player A or Player B and each of you will get an initial 10 points.

1 point = 1 US cent

When the game starts, Player A can decide to send some, all, or none of his/her 10 points to Player B. Each point sent to Player B will be tripled.

After receiving the tripled amount, both Players enter a Contract in which Player B is obliged to send back at least the amount of points sent by Player A before the multiplication.

In case Player A decides to send zero points, both Players keep their initial 1$ participation fee and earn 10 cents (equivalent of their initial endowment of 10 points).

If Player A sends X number of points to Player B, the tripled (X*3) amount of points become Player B' property and he/she can return any number of points to Player A, but no less than what Player A sent before the multiplication.

This game is played once.

Examples

If Player A sends 2 points, Player B will receive 6 points. Player B can return to Player A any number of points between 2 and 6.

If Player A sends 9 points, Player B will receive 27 points. Player B can return to Player A any number of points between 9 and 27.

Control Questions

If you are Player A and have 10 points, how many points can you transfer at most?

If you are Player B, after receiving 16 points from Player A, how many points at most can you transfer back?

If you are Player B, after receiving 24 points from Player A, how many points you are obliged to return back?

c.) Common pages for both treatments

- **Welcome Page**

Welcome

Thank you for accepting our HIT.

This game will last approximately 7 minutes.

The maximum amount of money that you can earn is 1$ and 30 cents, yet the amount of money that you **will** earn depends on the choices that you make while interacting with another participant.

Please read the instructions carefully because you will be quizzed before the game starts.

Please remember that you will only get paid if you complete the task.

- **Questionnaire**

Questionnaire

We hope that you enjoyed the game and that you are satisfied with the result. We kindly ask you to answer a short questionnaire after which your payment code will be send to you.

1. What is your gender?
2. What is your age?
3. Did you participate before in a game that is the same or similar to this one?
4. If you answered "yes" to the previous question, please write at least one sentence about the previous game(s) that you played.
5. Please describe in one or two sentences what real life situations this game reminds you of?

Appendix 5:

Graph 1: Plot of marginal effects of an interaction term (treatment and amount invested) on amount returned