THE QUALITY OF
GOVERNMENT INSTITUTE

UNIVERSITY OF
GOTHENBURG

Blockchain Technology

A Trust or Control Machine?
Theory and Experimental Evidence

20
22

Working paper series 2022:2

Đorđe Milosav
Marina Nistotskaya

THE QUALITY OF
GOVERNMENT INSTITUTE

Blockchain Technology

A Trust or Control Machine? Theory and Experimental Evidence

Đorđe Milosav

Marina Nistotskaya

WORKING PAPER SERIES 2022:2

QoG THE QUALITY OF GOVERNMENT INSTITUTE
Department of Political Science
University of Gothenburg
Box 711, SE 405 30 GÖTEBORG
March 2022
ISSN 1653-8919

BLOCKCHAIN TECHNOLOGY: A TRUST OR CONTROL MACHINE? THEORY AND EXPERIMENTAL EVIDENCE

Đorđe Milosav[1*] and Marina Nistotskaya[2]

*Corresponding author[1]
[1] Trinity College Dublin
[2] University of Gothenburg

E-mails: milosavo@tcd.ie / marina.nistotskaya@gu.se

ABSTRACT: Blockchain technology has attracted considerable interest in the last 15 years. It is argued that Blockchain can sustain any transaction of value, be it monetary or information, in a manner that is secure and independent of interpersonal trust. Yet, there remains little understanding on whether and how this technology enables trust-free transactions. This paper provides a novel theoretical account on the relationship between trust and Blockchain technology. Furthermore, it tests a set of hypotheses, associated with the conception of Blockchain as a trust-free environment, through an online experiment in which the properties of Blockchain-based smart contacts are exploited. The results indicate that the presence of Blockchain technology does not eliminate trusting and trustworthy behavior from human interactions. On the contrary, in comparison to the baseline group, 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-building machine".

Keywords: Blockchain technology, Trust, Reciprocity, Control, Experiments

[1] We would like to thank the Center for Collective Action Research and the Quality of Governemnt Institute at the University of Gothenburg for financially supporting this project. Also, we would like to thank Love Christensen for providing valuable comments on the experimental design and theory. Natalia Alvarado and Richard Svensson provided technical support for which we are especially grateful.

1 Introduction

Since the introduction of Bitcoin in 2008, there has been a proliferation of interest in a 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. At the same time, this technology is perceived to be so secure and reliable that The Economist named it a "trust machine". (October 31, 2015). Yet, due to its relative novelty, there is still little theoretical and empirical research on whether and how this technology may affect human-to-human trust relations. At the theoretical level, there seems to be an unaccounted disagreement about whether the technology works independently of interpersonal trust by shifting the trust that people have in each other towards trust in the technology itself or it affects interpersonal trust. Therefore, the aim of this paper is to provide a better understanding of the effects Blockchain technology on trust. Is Blockchain a trust-free and/or trust-building technology?

Based on the insights from the literature on institutionalized control, we argue that Blockchain is a trust-free environment that would crowd-out trusting and trustworthy behavior from the human relationship and set forth a set of hypotheses based on this conceptualization of Blockchain. We test these hypotheses by carrying out an online experiment based on Berg et al.'s (1995) trust game with anonymous participants, recruited from the Amazon Mechanical Turk. We run two experimental treatments: a simple trust game without the social history report and an adjusted trust game in which we operationalized the key aspect of Blockchain-based smart contracts — ex-ante specified actions with automatic enforcement. The experimental results indicate that Blockchain-based smart contracts would not omit trusting and trustworthy behavior from human relationship. On the contrary, the participants in the Blockchain treatment exhibited more trusting and trustworthy behavior compared to the baseline group, indicating support for the claim that this technology might indeed be a "trust-building 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 we present the key features of Blockchain technology in general and smart contracts as a case of its application. In the third section we review previous research on trust and Blockchain technology and present our theoretical framework. In the fourth section we present the experimental design and hypotheses together with the short summary of the experimental protocol and features of Amazon Mechanical Turk. We analyze and discuss the results in section 5 and 6, respectively. Finally, concluding remarks are presented in section 7.

2 Blockchain Technology and Smart Contracts

Originated back in 2008, Blockchain is a decentralized, distributed peer-to-peer network that stores data about all previous activities carried out by the network's users (Nakamoto, 2008; Raval 2016; Swan 2015). Each user (node) has a copy of the complete data of all previous activities, making the Blockchain different from other traditional databases known for a "single point of failure" (Zambrano, 2017). Since the same data is stored on multiple locations at the same time (decentralized), 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.

Blockchain is a distributed network, 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. a 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 information stored in all previous blocks. 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 monetary compensation in return for the work that they have done.

Due to these properties, Blockchain technocolgy provides a way to secure the content of the data from loss and unilateral retroactive change. Furthermore, since the enlargement of the data is not possible without the agreement of everyone in the network it is argued that there would be no need for trust between the users in order for it to function properly (De Filippi 2017; Hawlitschek et al. 2018). Interestingly, for the same reasons Blockchain technology is also argued to be a "trust machine" (Economist, Oct 31, 2015).

2.1 Smart Contracts

Smart contracts are "contractual clauses embedded into hardware and software in such a way that makes breach more expensive" (Raskin, 2017 p. 320). Yet, due to the lack of technology, it became possible to actually implement the concept only after the emergence of Blockchain. Utilizing the previously described characteristics of Blockchain technology, smart contracts are now understood as agreements with automated execution (Raskin, 2017 p. 306). Parties involved in such contractual relations agree ex ante on a set of conditional statements that are encoded in the smart contract. When these conditions are met, the agreed provisions are executed automatically.

Compared to traditional contracting, smart contracts have two key properties. Firstly, smart contracts need support neither of the legal profession nor of any institutionalized contract enforcer (Sklaroff (2017). In other words, smart contracts are a phenomenon of the "private social ordering" (Sklaroff 2017 p. 268), which would require interpersonal trust. However, the verifiability and transparency of the Blockchain-based transactions seem to eliminate the interpersonal trust requirement.

Secondly, some legal scholars argue that the logic of smart contract enforcement is completely different to traditional contracts, which are enforced in a court *after* an alleged violation of a contract has happened. 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).

3 Theoretical Framework

3.1 Previous Research on Blockchain and Trust

The existing empirical research on trust and Blockchain provides two major findings relevant for this paper. Firstly, it is argued that existing Blockchain-based applications may require trust. Fröwis and Böhme (2017) discuss conditions under which a smart contract is "trust-free" and analyze all smart contracts published on Ethereum. Their findings suggest that two out of five smart contracts 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). Yet, this problem emerged due to the lack of expertise with contracts coding and is therefore not an intrinsic general failure of the smart contracts.

Similarly, 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. By interviewing the users of Bitcoin, Sas and Khairuddin (2017) found that decentralization, deregulation, miners' expertise and reputation are all contributing to trust in the technology. However, these are exactly the properties of the technology that are believed to bring about its "trust-free" feature. Therefore, there seems to be a discrepancy between the Blockchain-based systems as a concept and practice (Fröwis and Böhme, 2017), that requires further examination.

3.2 Blockchain as a trust-free environment

We argue that the view of Blockchain as a "trust machine" (Economist, 2015) or as a technology that allows a system to be "trust-free" (Beck et al. 2016 for example) is based on two distinct concepts with radically different theoretical implications.

The most prominent difference between these two conceptions is based in whether this technology is seen as a producer of interpersonal trust within the network or not. Blockchain as a "trust machine" would produce more trust among the network's users.If Blockchain is understood as a "trust-free" environment, no clear expectations emerge regarding trust gain or loss within the network. Therefore, if Blockchain is a "trust-free" system, does it affect trust and, if so, how? In the remaining of this section, we present our argument that Blockchain will crowd-out trust through a mechanism of control.

The literature on trust is in consensus that trust has two key aspects. An actor who trusts is expressing a willingness to be vulnerable and has a positive perception of the intentions of the other party (Rousseau et al. 1998). If the actor does not have such willingness and/or believes that the other party has ill intentions, she will not trust that other party. The willingness to be vulnerable is often understood as a form of risk that is integral to the definition of trust (Gambetta 1988; Hardin 2002). For example, 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 settings that govern the relationship are fully determined that the trustee cannot betray or defect the trustor — such as the case in Blockchain-based smart contracts — one cannot argue that the relationship between those individuals is based on trust.

Smart contracts govern relationship between humans in accordance with encoded immutable rules. Since the parameters of permissible and impermissible behavior (and sanctions for such) are specified ex ante in smart contracts, risk (of betrayal or defection) is no longer part of the interpersonal relationship. In other words, in smart contracts the possibility of the trustee's potential betrayal is eliminated, and this leaves no room for the trustor to wish to be vulnerable. If the risk (of defection) associated the human (contractual) relationship is absent in smart contracts, this supports the argument that Blockchain is an environment that is independent of interpersonal trust.

3.3 Technology as a mediating factor of control

In this section we lay out the argument on how smart contracts might be able to crowd-out trust from the human relationship by means of control. We define control as 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" (Bijlsma-Frankema and Costa 2005, 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).

The principle of specification, which relates to "actions leading to successful cooperation and exploitation of value can be specified ex ante" (Bijlsma-Frankema and Costa, 2005 p. 264) is fully consistent with Blockchain-based smart contracts. Smart contracts facilitate "trustless exchange" (Sklaroff, 2017) because of the immutability of previously fully specified rules that govern the contractual behavior of the parties. By defining the possible behavior of the parties through encoded conditional claims, smart contracts assure the parties that cooperation would transpire when the stipulated conditions are met.

The second property of formal control — monitoring — is met in smart contracts because Blockchain network is distributed. If all nodes in the network receive a warning of discrepancies in the information contained in a smart contract, then a contractual action, associated with this compromised information (for example a transaction of information) would not be executed. In other words, nodes in the network function as monitoring actors who can objectively determine whether any party to a smart contract has breached the agreed upon rules (Bijlsma-Frankema and Costa, 2005 p. 264).

Thirdly, 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 in smart contract is "perfect", we would argue that attempts to breach the agreement would most certainly be detected. In this way a punishment (for example, exclusion from the network) represents a credible threat against misbehavior.

In light of these considerations, we argue that Blockchain is a control environment in which there is no room for trust. Blockchain-embedded control systems would crowd out trust from human relationships. We set to examine this theoretical claim using experimental methods.

4 Experimental Design and Hypotheses

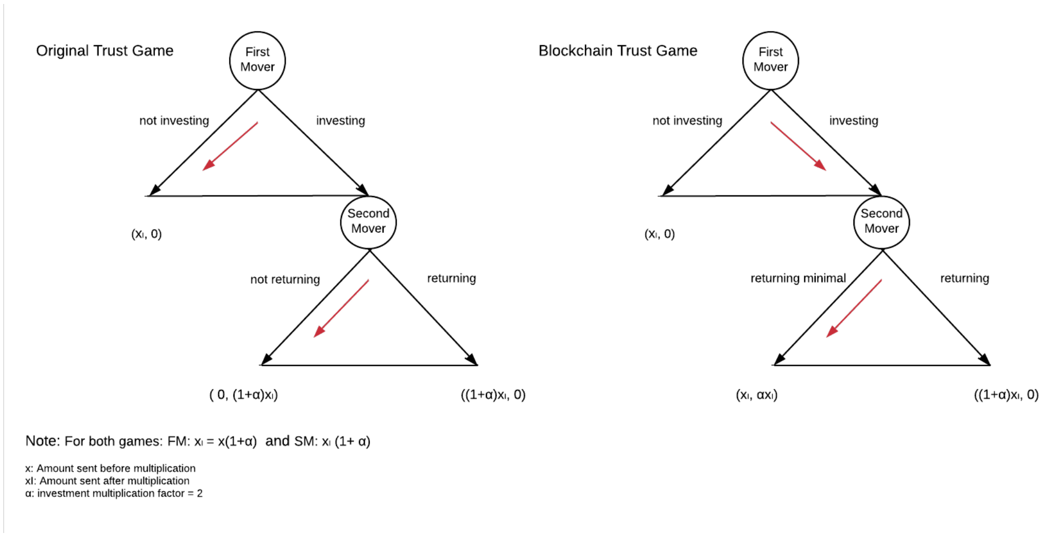
4.1 Experimental Design

Our experimental design builds on a well-established trust game from Berg et al. (1995). The baseline treatment 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 (hereafter FM) makes the decision to either "invest" some or all of his 10 game points by sending it to second mover (hereafter SM) or to leave the game without investing. 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$. The amount sent by the FM captures trust and the amount returned from the SM to the FM captures trustworthiness (Johnson and Mislin, 2011). Contrary to the standard 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.

The experimental treatment is designed to operationalize the key properties of smart contracts. In addition to the rules of the trust game treatment, we 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 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. 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, we 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, SM is expected to always decide to not return any points back to the first mover. Knowing this, FM 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), SM 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: $x_I = x(1+\alpha)$ and SM: $x_I\ (1+\alpha)$

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

On the other hand, in the Blockchain treatment, SM can decide between returning the minimal amount (amount invested by the FM before the multiplication) and returning the entire invested amount back. Similarly to the expected decision of the SM in the baseline treatment, SM in the Blockchain treatment is expected to return the minimal amount back. Knowing this, FM should always decide to invest the maximal amount of points because of the contractual restriction that disables the SM 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>.

4.2 Reciprocity Considerations and Hypotheses

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 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 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 factors that determine individual trust in others. 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 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).

In the case of the two experimental treatments, we argue that in the baseline/Trust treatment, all of 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 figures as a form of institutional embeddedness. The obligation imposed on the SM to return at least the amount sent by the FM is understood here as a regulatory process that makes noncompliance 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, we argue that the possibility for reciprocal behavior of the SM 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, we 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, we 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 our 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, we present the following hypothesizes:

H1: *First Mover in the Blockchain treatment would decide to invest more frequently than the First Mover in the Trust treatment.*

H2: *First Mover in the Blockchain treatment would invest more points than the First Mover in the Trust treatment.*

H3: *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 going to 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.*

4.3 Experimental Protocol

The experiments were conducted on Amazon Mechanical Turk (hereafter MTurk), an online labor market with a pool of over 500,000 workers (Arechar et al. 2017). The requester (employer) sets up a task (called Human Intelligence Task, HIT) and publishes 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 Arechar et al. (2017), we set our compensation rate to be around $ 8.5 US per hour.

For both of the treatments we applied exactly the same HIT description in order to avoid any potential self-selection bias (Horton et al. 2011 p. 415). Having accepted a HIT, 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 the 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 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. No deception was used in either of the two treatments. The HIT descriptions can be found in Appendix 1, and instructions, control questions and questionnaires for both treatments can be found in Appendix 2.

All of the experimental sessions were conducted between 16th and 24th of April 2019 with a starting time between 4 and 7pm (CEST). We 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 Arechar et al. (2017), we restricted the subjects 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. Experimental data were coded in an online software, called LIONESS (Giamattei et al. 2020). We utilized the option in the LIONESS that allowed us to omit the double entry of the participants within the session by partial IP address tracking. When it comes to double entries across sessions we used "Unique Turker" identifier, by which we prevented the subjects who had already participated in any of the treatments to reenter the experiment.

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. Descriptive statistics of the game-related variables (see Table 1) provides some important information. 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 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, with a difference of 0.7 $US cents. To improve readability, we present the results of hypothesizes testing for the first and the second mover separately.

5 Analysis

5.1 First Mover Behavior

In order to test H1, we 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. We coded Invest as "1" and Not invest as "0". Firstly, we conducted a Chi-squared test between Investing decision and a dummy treatment variable, capturing the treatment effect. The results indicate that the relationship between the decision to invest and

Table 1: Descriptive Statistics

Trust Treatment

Variable	Obs	Mean	Std.Dev.	Min	Max
Amount Transferred x 3	248	18.56	11.39	0	30
Amount Returned	248	6.64	6.78	0	30
Proportion Returned	212	.349	.25	0	1
Gender	492	.48	.5	0	1
Age	492	36.23	10.51	20	71
Earnings FM	248	10.45	5.38	0	30
Earnings SM	248	21.92	9.04	10	40
Earnings combined	496	16.18	9.39	0	40

Blockchain Treatment

Variable	Obs	Mean	Std.Dev.	Min	Max
Amount Transferred x 3	227	22.98	9.37	0	30
Amount Returned	227	10.33	5.18	0	30
Proportion Returned	216	.45	.13	.33	1
Gender	450	.44	.5	0	1
Age	450	36.39	11.01	18	69
Earnings FM	227	12.7	3.17	10	30
Earnings SM	227	22.63	5.89	10	30
Earnings combined	454	17.66	6.86	10	30

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, we conducted a logistic regression on the focal relationship with the inclusion of gender, age and previous experience as controls. The results (not reported) point that FMs in the Blockchain treatment are more likely to invest than FMs in the Trust treatment (p < 0.001) with all control variables entering statistically not significant. Therefore, we conclude that the data provides support for H1.

In order to test H2 we performed a two-sample t-test. The difference in the mean amount of points invested by FM in 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), we would argue that the Blockchain treatment has medium effect size when it comes to the behaviour 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, we conclude that that the data provides support for H2.

5.2 Second Mover Behavior

The behaviour of the SM is addressed in hypothesizes 3 to 5. According to H3, we 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, we created a 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). We 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 we have to reject hypothesis 3, due to statistically significant results in support for the opposite claim.

Lastly, we test hypothesizes 4 and 5 concomitantly by utilizing an OLS regression with robust standard errors. We 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.[1] 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 3 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 95% level.

[1] 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. Furthermore, all the control variables were statistically insignificant.

Table 2: OLS regressions for the effects on Amount returned

	Model 1 **Trust treatment**	**Model 2** **Blockchain Treatment**	**Model 3** **Interaction Effect**
Amount sent	1.084^{***}	1.368^{***}	1.084^{***}
	(0.0829)	(0.0477)	(0.0829)
Treatment Dummy			-0.0515
			(0.406)
Amount sent x Treatment			0.283^{**}
			(0.0957)
Intercept	-0.0698	-0.121	-0.0698
	(0.281)	(0.294)	(0.281)
Observations	248	227	475
R-squared	0.370	0.677	0.522
Adj. R-squared	0.367	0.676	0.519

***p < .01; **p < .05; *p < .1
Robust standard errors reported in parentheses. Reference category for treatment dummy is Trust treatment.

Therefore, the results indicate support only for H5. On the other hand, a positive relationship between the amount returned and amount transferred in the Blockchain treatment indicate that we have to reject H4. Moreover, the tested relationship is, contrary to the expectations, stronger in the Blockchain than it is in the Trust treatment.

6 Discussion

In this section we discuss the findings in terms of the trust-control nexus and a broader context of the application of Blockchain-based environments.We also discuss a set of potential factors of the experimental design itself that might have had an effect of the results we obtained. As it was done in the analysis, we discuss the behaviour of the FMs and the SMs separately.

6.1 Trust-Control Nexus

Our experimental findings indicate that the probability of the invest decision 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 behaviour 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 we argue that the behavior observed is not one of trust. During the construction of the experimental design, we opted for the treatment presented as it was necessary to operationalize the theoretical aspects of

Blockchain in the best possible way. This included the necessity of omitting risk from the relationship.

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 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 SM, contrary to our 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.[2]

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 an 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] 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)

-2.74, $p < 0.01$).

6.2 Implications for Blockchain technology

On the condition that the operationalization of the presented key features of the technology is theoretically sound, we would argue that Blockchain-based smart contracts would indeed act as a "trust machine". 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 FM could not be viewed as a trusting decision, contrary to the expectations, SMs 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, somewhat counter-intuitively, Blockchain technology could be understood as *trust-free trust machine*.

Furthermore, as it was noted in the theoretical section, we 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. We 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 MTurk 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 experimenters, we 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, we have probably incorporated our own social norms on what is the "fair" amount returned.[3] 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.[4] In spite of these potential issues we argue that the results presented in this paper are a good starting point in the experimental Blockchain research. We argue that the results of the experimentally induced "private social ordering" (Sklaroff, 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 a single 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 of 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.

6.3 Potential Limitations of 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, we 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, we asked the participants if they have played similar games before and in case they did we asked them to describe the differences between previous games and the one

[3] 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, 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 us to investigate both players' behavior in a risk-free environment without the need for introducing any additional assumptions.

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

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 ours is the obligation to return the minimal amount sent. We 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, we would argue that, even though the incentives for play in the 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 our 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, we 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. One of 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). 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, we 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, we decided to restrict the analysis on one-shot games only. Furthermore, on a more practical note, iterated trust games last longer and are more expensive to conduct.

7 Conclusions

In this paper we presented and tested a new theoretical account of the effects of Blockchain on trust. We argued that this technology is best understood as providing a base for a trust-free relationship, and hypothesized that Blockchain-based systems such as smart contracts would crowd out trust from the human relationship. In order to test this claim, we conducted an online experiment in which we operationalized a key property of smart contracts in our experimental treatment. We found that, contrary to the expectations, subjects in the Blockchain treatment did reciprocate and on average returned around 10% more than their counterparts in the baseline treatment — a classic one-shot trust game. These findings suggest that, even when risk is not a consideration in investment decision, SMs exhibit a trustworthy behavior. This suggests that the spread of Blockchain technology might bear positive effects on the level of trust and trustworthiness in human-to-human relationships.

This paper makes at least two important contributions to the literature. First, we nuanced the argument about Blockchain technology as a trust-free environment by integrating the literature on institutionalized control. Second, we empirically tested a set of hypotheses stemming from the conceptualization of Blockchain as a trust-free environment, utilizing experimental research design. Our findings suggested that the concept of Blockchain as a trust-free environment is incomplete: Blockchain is both a trust-free and a trust-building machine.

When it comes to the potential future research, we suggest that the main focus should be on testing the proposed hypotheses by running iterated Trust and Blockchain treatments and thereby engaging with the literature that underscores that trust relationship is 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.

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

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.

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.

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.)

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

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

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.

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

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

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

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

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.

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.

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.

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.

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)

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

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