Scientific Research Publishing

iBusiness, 2020, 12, 103-112
https://www.scirp.org/journal/ib
ISSN Online: 2150-4083
ISSN Print: 2150-4075

Impact of Blockchain Applications on Trust in Business

Siming He

School of Engineering and Applied Science, University of Pennsylvania, Philadelphia, USA
Email: siminghe2020@gmail.com

How to cite this paper: He, S. M. (2020). Impact of Blockchain Applications on Trust in Business. *iBusiness, 12,* 103-112.
https://doi.org/10.4236/ib.2020.123007

Received: August 8, 2020
Accepted: September 25, 2020
Published: September 28, 2020

Abstract

Blockchain applications are considered as "trustless" machines, because they reduce business's needs of trust in others. The "trustless" nature draws researchers' attention on investigating the implications of blockchain in a business environment. From a view of business ethics, this paper aims at evaluating the impacts of blockchain applications on trust and business. After expounding the relations between trust in blockchain and trust in business partners, I evaluate the impacts based on a framework of competence trust, contractual trust, and goodwill trust. My conclusion is that full acceptance of trust in blockchain over trust in others is not good and will cause several risks that cannot be neglected. The main contribution of this paper is investigating and summarizing ethical and commercial risks of blockchain applications including disintermediation fallacy, centralization of trust, ambiguous contract, noncognitive trust in untrustworthy partners, and more actions guided by moral minimum.

Keywords

Trust, Blockchain, Data, Contract, Goodwill, Competence

1. Introduction

Blockchain has become an increasingly popular technical and commercial topic with the rise of various applications. It is a distributed database of records that are used and shared among participating parties (Crosby et al., 2016). Because every participant keeps a copy of the records, neither central databases nor intermediary agents are needed. Therefore, blockchain technology has a decentral, disintermediary, and democratic nature (Dierksmeier & Seele, 2020: p. 3). Bitcoin is one of the most well-known applications of blockchain technology. It is a kind of cryptocurrency, which is encrypted, generated, verified, and operated by

a person-to-person bitcoin network rather than a central bank (Swan, 2015). The nature of blockchain is well embodied by bitcoin. However, blockchain has much more applications in business and society above cryptocurrency. According to Swan (2015), applications of blockchain can be divided into three categories: cryptocurrency (blockchain 1.0), contracts (blockchain 2.0), and justice (blockchain 3.0). Blockchain 1.0 is for the decentralized transaction of money (Swan, 2015). A typical example is bitcoin, a digital payment system based on cryptocurrency. Blockchain 2.0 involves transfers of other assets beyond currencies (Swan, 2015). An example of blockchain 2.0 is smart contracts that form and self-execute transaction protocols based on decentralized blockchain networks (Swan, 2015). Therefore, not only money but also stocks, bonds, and properties can be transacted based on smart contracts (Swan, 2015). Blockchain 3.0 is applications in government, health, science, culture, and art (Swan, 2015). Blockchain can be used as a new model for organizing activity, leading to less friction and higher efficiency in society (Swan, 2015). For example, digital identity verification based on blockchain can speed up e-commerce purchases and simplify registrations to websites (Swan, 2015).

In this paper, I will focus on issues of trust related to blockchain 1.0 and blockchain 2.0. Unlike traditional contract that is an agreement between parties based on trust in other parties, blockchain 2.0, or technically known as algorithmic contract, replaces human judgement by automatic analysis of records of blockchain network (Swan, 2015). Therefore, parties minimize the needs of trust in other parties due to fewer needs for human judgement (Swan, 2015). In another word, data transparency allows parties to monitor each other's actions easily; thus, parties do not need to take costs and risks to be vulnerable and build up trust. As a result, a shift from trust in other parties to trust in blockchain raises concerns among researchers. Dierksmeier and Seele (2020) argue that the impact is morally ambivalent. Applications of blockchain technology reduce misuse of trust but may change our perception of trust in the individual and social level (Dierksmeier & Seele, 2020). The changing perception of trust may not be good, since there will be less personal and commercial trust and a possible trade-off between commercial efficiency and culture related to trust (Dierksmeier & Seele, 2020). (Berg et al., 2017) state that "economically-valuable trust", or trust in blockchain, is a better kind of trust. Trust is used as a safeguard against opportunism in transactions (Berg et al., 2017). Transactions will not happen if the costs of opportunism and risks of trust are too high (Berg et al., 2017). Trust in blockchain, instead, suppresses the cost of opportunism and risk of trust in other parties, and thus allows more transactions to happen (Berg et al., 2017).

However, I argue that trust in other parties is better than and is morally unfavorable to be replaced completely by trust in blockchain in many cases. In Section 2, I briefly define blockchain technology, and then explain the relation between trust in other parties and trust in blockchain. In Section 3, I clarify conditions of trust and compare trust in people and trust in blockchain. In Section 4, I

identify the impacts of increasing machine trust based on a framework of contractual trust, competence trust, and goodwill trust. In Section 5, I propose two dimensions of the impacts on trust to assess specific blockchain applications. In Section 6, I conclude that full acceptance of trust in blockchain causes issues including the centralization of platform and trust, opportunism, and moral minimum. And trust in other parties has some good commercial and social value that cannot be replaced.

2. Blockchain Technology

Blockchain is a public, distributed ledger that can verify and record transactions between two parties (Crosby et al., 2016). Transactions in blockchain are verified and recorded in four steps. Firstly, a transaction is presented as an online block (Crosby et al., 2016). Then, the block is sent to every participant in the blockchain network (Crosby et al., 2016). The block can be encrypted so participants cannot spy on other's transactions. Thirdly, participants' computers prove the validity of the transaction automatically based on a chain of records of transactions (Crosby et al., 2016). Lastly, the block is added to the chain and provides an indelible and transparent record of the transaction (Crosby et al., 2016). Blockchain is secure because copies of the chain are stored by every participant. Even if an attacker modifies a transaction in one copy, other copies will be able to detect the invalid transaction (Crosby et al., 2016). One way that an attacker could attack a blockchain network is called 51% attack in which the attacker modifies 51% of copies (Crosby et al., 2016). Consequently, the blockchain network would fail to detect the modified transaction; the modified transaction would become the real one (Crosby et al., 2016). However, 51% attack becomes more difficult with an increasing number of participants and copies (Crosby et al., 2016).

Contract, in law, is an agreement of obligations of parties and is enforceable (Peel, 2015). Similarly, each smart contract has two parts: an agreement and methods of enforcement. The agreement will be written in code and executed automatically when conditions are met (Law, 2017). Execution and enforcement of the agreement are based on and guaranteed by transparent records in a blockchain network (Law, 2017). Smart contracts can be applied in various scenarios. A major one is in supply chains. Previously, it has been hard to track a whole supply chain of a product, since each supplier has its way to record supplies and the ways are not compatible and transferable. Based on blockchain technology, details (producer, location, manufacturing date, etc.) of each component of a product are shared throughout the whole supply chain (Law, 2017). Therefore, supply chains with blockchain achieve higher transparency (Law, 2017). The details are, then, used to enforce smart contracts (Law, 2017). Applying Berg et al.'s theory (2017), suppliers can no longer exploit the information asymmetry and seek for opportunism. Consequently, less trust in suppliers is needed, and more transactions take place more efficiently.

3. Trust

There are three relatively uncontroversial conditions for trust (McLeod, 2020). To trust, we have to be vulnerable to others' betrayal, think well of others, and be optimistic that trustees are competent in certain aspects (McLeod, 2020). Since trustees have freedom, trustors cannot reject being vulnerable (McLeod, 2020). Moreover, people need to think well of others and cannot easily suspect each other if trust exists (McLeod, 2020). Moreover, the difference between trust in people and trust in machines should be noticed. Based on the conditions of trust in people, trust in machines is merely reliance. Trust can be betrayed while reliance can only be disappointed (Baier 1986: p. 235, as cited in McLeod, 2020). When an inanimate object breaks, people are disappointed but not betrayed (Baier 1986: p. 235, as cited in McLeod, 2020). The fundamental difference here is related to motivation. When trusting a person, we presume that the person has good motivation in doing a task. Therefore, we believe the person is supposed to do the task well. Moral conflicts due to the person failing the task result in a feeling of betrayal. However, without an expectation of motivation, we do not expect that the person ought to do the task well on a moral level. Therefore, we can only be disappointed or dissatisfied when the person fails. And because machines do not have any motivation, they cannot meet all conditions of trust in people. Particularly in this paper and many others (Berg et al., 2017; Dierksmeier & Seele, 2020; Karamitsos et al., 2018), the condition about vulnerability to betrayal when talking about trust in machines is removed.

Trust is dangerous due to risks on trustor, but trust is also good and important because it allows partners to form relationships for help and cooperation (McLeod, 2020). Blockchain technology undermines vulnerability in relations, thus results in less trust. In the example of smart contracts in a supply chain, blockchain achieves high data transparency which reduces information asymmetry and possible risks of opportunism. Therefore, people in the supply chain become less vulnerable to others' betrayal. Consequently, there is less trust among parties in the supply chain. From customers' perspective, data transparency allows themselves to reduce risk by monitoring behaviors of suppliers. Easier and more frequent monitoring results in fewer needs of trust in suppliers. From suppliers' perspective, data transparency would de-motivate them to be trustworthy. Some people may argue that data transparency allows suppliers to be more trustworthy because transparency forces suppliers to operate more properly. However, competence and motivational elements of trustworthiness are both crucial (McLeod, 2020). Data transparency cannot guarantee the motivation of suppliers. Since customers need less trust in suppliers while focuses more on data, suppliers have less chance to commit to cultivating trust in customers while have more chance to commit to present better and more reliable data. Because customers understand that suppliers are motivated to rather present more reliable data than be entrusted by customers, suppliers cannot betray customers but disappoint them. Therefore, data transparency only allows

suppliers to be more reliable rather than more trustworthy. From another perspective (Blois, 1999: p. 206), trustworthiness is a slow revolution that begins with small risks and builds on confirmations. Data transparency reduces the chances to continue the slow revolution. As a result, blockchain technology leads to a decreasing amount and importance of trust and trustworthiness in other parties.

4. Three Categories of Trust

Miyamoto & Rexha (2004) divide trust into three categories: competence trust, contractual trust, and goodwill trust. Competence trust is a confidence in partner's ability (Miyamoto & Rexha, 2004). Contractual trust is an expectation that a partner will keep promises (Miyamoto & Rexha, 2004). And goodwill trust is confidence in a partner's good intention and open commitment to support and continue partner relationships (Miyamoto & Rexha, 2004). Comparing the three categories with the three conditions of trust, competence trust shows optimistic attitudes toward partner's ability; contractual trust reflects less suspicion due to promises; and goodwill trust creates vulnerability to betrayal. Blockchain applications lead to a shift of trustees of competence trust from parties to machines, a reconstruction of contractual trust, and a reduction of goodwill trust.

4.1. Competence Trust

Competence trust in blockchain becomes confidence in a machine's ability to provide transparent data and enforce smart contracts. For example, customers trust machines' ability to provide transparent data of suppliers and goods in supply chains. The data are used to monitor and evaluate the ability and reliability of suppliers. Therefore, the competence trust in partners is replaced. If a customer directly trusts in the competence of a provider, the customer monitors the ability of blockchain to evaluate the competence of the provider. Thus, it shows suspicions and less trust in machines' ability, and competence trust in blockchain is reduced. As a result, the two kinds of competence trust are incompatible; an increase of trust in one must reduce trust in another.

The evaluation of ability and reliability by machine is more efficient since it requires minimum human judgement. However, it is not necessarily a good thing. Hawlitschek et al. (2020) argues that disintermediation fallacy appears in blockchain technology. Blockchain requires a huge number of participants to ensure security. Therefore, programmers, or people who know details of blockchain technology, are a relatively small portion of participants. And since most of the participants in blockchain do not understand details of blockchain technology, blockchain must be created and maintained by an agent. Consequently, the agent functions as new intermediation. Competence trust in the new intermediation creates new problems and inefficiency of human judgement regarding trust.

Moreover, the shift of object of competence trust entails risks of centralization. Trust is distributed in conventional competence trust; parties trust each other based on different relations and situations. Therefore, a single failure of

trust can only impact several parties. However, competence trust in blockchain requires a centralized trust in the ability of blockchain. Since trust is related to vulnerability, the extent of single betrayal increases; the failure of trust in blockchain impacts all trustors. Though the probability of risk of failure of blockchain is lower since it is shared and verified by all participants, it is unclear if the product of risk and extent of the negative impact of trust in blockchain (expected risk value) is lower.

4.2. Contractual Trust

Smart contracts are code that executes written and oral contracts. Since they are automatically executed based on code and data that humans cannot process, the contracts have to be interpreted by programmers and computers. Since many parties do not understand programming, it is difficult for them to understand the content of smart contracts and communicate with programmers. Moreover, programmers and computers may have different interpretations of code (functional errors). Thus, more steps of communication and interpretation will cumulate errors and ambiguities in contracts. As a result, trust in smart contract leads to more opportunism when hackers and partners exploit errors and ambiguities.

4.3. Goodwill Trust

Because blockchain technology provides data that reflect suppliers' reliability, customers would prefer this more transparent and efficient way to do transactions. It is less efficient and less necessary to judge the goodwill and trustworthiness of suppliers. As a result, there will be more noncognitive trust of customers toward suppliers. Noncognitive trust is a trustful attitude, emotions, or motivations that are not focused on specific individuals or institutions (Becker, 1996). In the case of blockchain technology in supply chains, customers have a trustful attitude towards data rather than focus on the trustworthiness of suppliers or questions the "trustworthiness" shown by blockchain data. Customers are less capable of recognizing noncognitive trust in untrustworthy suppliers. Since blockchain data may not include all data for every aspect of consideration, untrustworthy suppliers would act trustworthy according to data and continue untrustworthy actions in aspects uncovered by data. One example is the greenwashing of energy suppliers. Greenwashing is superficial efforts of companies for the sake of public relations rather than environmental protection (Byars & Stanberry, 2018). Since detailed data of sources of energy are recorded in a blockchain, customers will trust the suppliers who use wind turbines on being environmentally friendly. However, untrustworthy energy suppliers may build wind turbines in major migratory routes of birds for profit if data of harm of wind turbine to bird are not included in the blockchain. Because blockchain data are detailed and transparent, customers will have a strong noncognitive trust in suppliers as well as less consideration of goodwill and factors that not included

in blockchain data. In contrast, without blockchain technology, customers need to communicate and judge each company respectively, thus are more likely to consider more diverse factors and rule out greenwashing.

Suppliers, recognizing the decreasing importance of goodwill and trustworthiness during transactions, will focus more on achieving better data rather than goodwill. The shift of focus leads to a shift of contractual relations between corporations. Contractual relations between corporations can be divided into Arm's length contractual relation (ACR) and Obligational contractual relation (OCR) (Sako, 1992). In ACR, firms wish to retain full control of themselves (Sako, 1992). Therefore, they have less trust in each other, follow contract contents, and normally maintain short-term relationships (Sako, 1992). However, in OCR, firms prefer high-trust cooperation with commitments in the long run and value goodwill trust (Sako, 1992). Thus, they do beyond contract contents and are willing to help partners voluntarily or share risks caused by market fluctuation (Sako, 1992). Since it is less efficient to justify goodwill in the long run than to find reliable suppliers directly, both suppliers and customers will prefer to find short-run reliable partners based on blockchain data. As a result, suppliers are less motivated to do beyond the moral minimum. For example, they would be less willing to voluntarily share information that is related to profits or risks of their customers as long as sharing the information is not a duty declared by contracts and laws. Consequently, increasing ACR and decreasing OCR reduces the performance of partners (Sako, 1992).

5. Evaluation of Current Blockchain Applications

Though part of the issues discussed above can be solved by technology, regulation, and new structures of organization, it is necessary to have some measurements for trust issues of blockchain application. Three dimensions are emphasized during the previous discussion of trust: risk of centralization, opportunism, and moral minimum. Risk of centralization is the risk of the relationship with platforms, while opportunism and moral minimum are related to relations among parties. Therefore, opportunism and moral minimum can be combined to a single dimension that measures the impact of trust in blockchain among parties.

Based on the two dimensions, I create **Figure 1** and summarize my assessment of some existing blockchain applications. The most popular application of blockchain, Bitcoin, has high risks of centralization and opportunism. Because many owners of bitcoin are not able to join the bitcoin blockchain network due to technical and hardware difficulties, they have to choose to use cryptocurrency trading exchanges. As a result, the trading exchanges increase risks of centralization of platform and trust. The exchanges are subjected to failure of trust in protecting users' cryptocurrency and trust in the founders of the exchanges. Quadrigacx, a Canadian digital asset exchange, was bankrupted following the death of the chief executive officer Gerald Cotton (Gogo, 2020). As a result, 17,000 people failed to refund nearly 307 million dollars (Gogo, 2020). Similar risks are

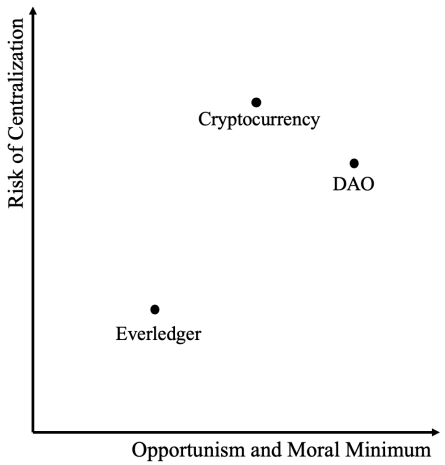

Figure 1. Measurements of trust issues of blockchain application.

particularly high in the cryptocurrency market since the centralization is under loose regulation. Another example is DAO, a decentralized autonomous organization, a program governed by a smart contract based on Ethereum (a kind of cryptocurrency) (Leising, 2017). In 2016, functional errors in DAO's design cause an ambiguous contract which puts 250 million dollars at risk of being stolen (Leising, 2017). 55 million dollars were stolen by hackers in one day (Leising, 2017). Everledger is an application of blockchain in the diamond supply chain (Ledger Insights, 2019). It tracks origin, features, and ownership of each diamond (Ledger Insights, 2019). The data help to solve worker exploitation and environmental degradation (Ledger Insights, 2019). Similar to the example of greenwashing, noncognitive trust in untrustworthy suppliers may exist, since the data of origin, features, and ownership only reflect very limited aspects of suppliers' actions.

6. Conclusion

Blockchain technology highlights applications of "trustless" machines and leads to reduction of the importance of trust and trustworthiness on other parties. It is controversial that whether the decrease is good or bad. Berg et al. (2017) argue that blockchain technology increases market efficiency and transactions by suppressing opportunism. However, based on my analysis of competence trust, contractual trust, and goodwill trust, it is clear that full acceptance of trust in blockchain over trust in other parties is not good and will cause several problems that cannot be neglected. The shift from competence trust in other parties to competence trust in blockchain will cause disintermediation fallacy which introduces new inefficient factors of human judgement. Centralization of trust also increases the extent of the impact of trust failure which may increase the expected risk value in the market. Contractual trust still exists while intermediate processes of coding and interpretations are required which increase ambiguities and result in more opportunism. The decreasing importance of and attention on

goodwill trust causes less capability of parties to recognize noncognitive trust in untrustworthy suppliers, as well as reduces the performance of partners. As the increasing applications of blockchain in daily lives, if we do not clearly understand and prevent these possible risks, they will go beyond the commercial level to the social and cultural level. Since applications of blockchain 2.0 are still at the initial stage, only a few real-life examples are discussed in this paper. More examples need to be compared and assessed in the future. This paper doesn't investigate the impacts of trust in blockchain on society and culture; thus, additional research is needed to identify them as well as to explore technical and regulatory solutions to the trust issues.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Baier, A. C. (1986). Trust and Antitrust. *Ethics, 96,* 235.

Becker, L. C. (1996). Trust as Noncognitive Security about Motives. *Ethics, 107,* 43-61. https://doi.org/10.1086/233696

Berg, C., Davidson, S., & Potts, J. (2017). Blockchains Industrialise Trust. *SSRN Electronic Journal,* November 2017. https://doi.org/10.2139/ssrn.3074070

Blois, K. J. (1999). Trust in Business to Business Relationships: An Evaluation of Its Status. *Journal of Management Studies, 36,* 197-215. https://doi.org/10.1111/1467-6486.00133

Byars, S., & Stanberry, K. (2018). *Business Ethics*. In OpenStax.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review, 2,* 6-19.

Dierksmeier, C., & Seele, P. (2020). Blockchain and Business Ethics. *Business Ethics, 29,* 348-359. https://doi.org/10.1111/beer.12259

Gogo, J. (2020). *17,000 Quadrigacx Users Seek $307M from the Failed Canadian Crypto Exchange*. Bitcoin.Com.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2020). A 2020 Perspective on "The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy." *Electronic Commerce Research and Applications, 40,* Article ID: 100935. https://doi.org/10.1016/j.elerap.2020.100935

Karamitsos, I., Papadaki, M., & Barghuthi, N. B. (2018). Design of the Blockchain Smart Contract: A Use Case for Real Estate. *Journal of Information Security, 9,* 177-190. https://doi.org/10.4236/jis.2018.93013

Law, A. (2017). *Smart Contracts and Their Application in Supply Chain Management*.

Ledger Insights (2019). *Everledger Upgrades Blockchain Platform, Expands beyond Diamonds*. Ledger Insights.

Leising, M. (2017). *The Ether Thief*. Bloomberg.

McLeod, C. (2020). Trust. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy (Fall 2020 Edition)*. Stanford: Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2015/entries/trust

Miyamoto, T., & Rexha, N. (2004). Determinants of Three Facets of Customer Trust. A Marketing Model of Japanese Buyer-Supplier Relationship. *Journal of Business Research, 57,* 312-319. https://doi.org/10.1016/S0148-2963(01)00327-7

Peel, E. (2015). *Treitel on the Law of Contract*. London: Sweet et Maxwell.

Sako, M. (1992). *Prices, Quality and Trust*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511520723

Swan, M. (2015). *Blockchain for a New Economy*.