PERSPECTIVE
published: 31 January 2020
doi: 10.3389/fbloc.2020.00002

Proof of Work as a Three-Sided Market

Chris Berg, Sinclair Davidson and Jason Potts*

Blockchain Innovation Hub, RMIT University, Melbourne, VIC, Australia

Blockchain technology is the distributed ledger technology underlying Bitcoin and other cryptocurrencies. We apply Oliver Williamson's transactions cost analysis to a proof of work blockchain consensus mechanism. Blockchains reduce the costs of opportunism, but are not "trustless." We show that blockchains are trust machines. Blockchains provide for three-sided bargaining that convert energy-intensive computation into economically-valuable trust in a proof of work context.

Keywords: blockchain, transaction costs, industrialization, proof of work, trust

OPEN ACCESS

Edited by:
Markos Zachariadis,
University of Manchester,
United Kingdom

Reviewed by:
Nadia C. Fabrizio,
CEFRIEL, Italy
Enrico Rossi,
London School of Economics and
Political Science, United Kingdom

****Correspondence:***
Chris Berg
chris.berg@rmit.edu.au

Specialty section:
This article was submitted to
Financial Blockchain,
a section of the journal
Frontiers in Blockchain

Received: *12 September 2019*
Accepted: *13 January 2020*
Published: *31 January 2020*

Citation:
Berg C, Davidson S and Potts J
(2020) Proof of Work as a Three-Sided
Market. Front. Blockchain 3:2.
doi: 10.3389/fbloc.2020.00002

INTRODUCTION

A blockchain is a distributed ledger technology that records transactions without the need for a trusted third party or other centralized authority. First described by the pseudonymous "Satoshi Nakamoto" in his white paper "Bitcoin: A Peer-to-Peer Electronic Cash system" (2008), the Bitcoin blockchain decentralizes the double spending prevention process, creating an open network governed by a protocol known as a consensus mechanism. The Bitcoin protocol time-stamps all transactions and rejects attempts to double spend currency (Narayanan et al., 2016).

In Bitcoin, "miners" play a central role for maintaining consensus over the state of the ledger. Miners compete to solve a computationally expensive cryptographic puzzle for the right to create a new block on the chain containing recent transactions. Successful miners are awarded with an amount of bitcoin (currently 12.5 bitcoin) for each correctly solved block. The difficulty of the puzzle changes periodically in order to maintain the average time it takes to process a block to ~10 min. The reward decreases periodically in order to maintain a steady rate of inflation. Nakamoto (2008) described the purpose of this architecture as to align users' incentives to maintain and protect valid data, and to reject invalid data. The resulting network embeds economic incentives into the structure of the network itself, thereby distributing economic value to those who maintain it. Swan (2015) described the mining process as the "key innovation" associated with distributed ledger technology:

> Users can trust the system of the public ledger stored worldwide on many different decentralized nodes maintained by "miner-accountants," as opposed to having to establish and maintain trust with the transaction counterparty (another person) or a third-party intermediary (like a bank). The blockchain as the architecture for a new system of decentralized trustless transactions is the key innovation.

Blockchains are often described as being "trustless" (Swan, 2015). Szabo (2014) argues that "trustless" is an exaggerated shorthand given Bitcoin's well-known security limitations, and that blockchains are better described as "trust-minimized."

In this paper we explore the notion of trust and trust-minimization in blockchain technology by incorporating it into an economic analysis. Satoshi Nakamoto's contribution was to devise a technology that resolved (or minimized) trust issues without relying on centralized control—creating a "three-sided market" between the two parties to the exchange (buyers and sellers), and miners. Each party has to be satisfied for the transaction to occur. We consider the economic function that miners (in a proof of work context) play through a transaction cost framework first developed by the economics laureate Williamson (1985, 1988, 1993a,b). This approach clarifies that blockchains are not trustless or trust-minimizing *per se*. Rather, they are trust machines, and their use constitutes the industrialization of trust. Blockchains suppress (some, but not all) opportunism costs that would otherwise prevent exchanges from taking place.

Our contribution applies to those blockchain technologies that rely upon a proof of work mechanism to govern consensus. There currently exist a wide variety of cryptocurrencies and blockchain applications with varied consensus mechanisms, and correspondingly different roles for validators. Likewise, cryptocurrencies can be built using alternative distributed ledger technologies such as directed acyclic graphs (Hileman and Rauchs, 2017). That is not to suggest that other distributed ledger technologies that rely on other consensus mechanisms do not industrialize trust, but merely to indicate that the research to demonstrate that point remains to be undertaken.

In the next section (following Berg et al., 2019) we discuss the notions of trust and opportunism and present a very simple schema that sets of the argument that the blockchain generates an industrialized form of trust. We then discuss the broader implications of that schema and identify when blockchain works well at generating trust and when it will not. A conclusion follows.

OPPORTUNISM AND TRUST IN AN INSTITUTIONAL FRAMEWORK

The notion of transactions costs can be traced to the work of economics laureate (Coase, 1937). Coase had asked the question as to why firms existed when standard economics suggested that markets were efficient at allocating resources. His insight was the recognition that there were costs to using the market mechanism, and that these costs could be minimized by organizing economic activity within hierarchies (i.e., firms). Of course, there were costs associated with the use hierarchy too, and firm boundaries would be established when these costs equilibrated. Coase himself was somewhat vague as to how these costs manifest themselves and the margins at which they operated. It was Williamson (1985), also an economics laureate, that carefully articulated how and when those transaction costs are important. Following Davidson et al. (2018a) we apply this institutional economic analysis to understanding the underlying economics of blockchain and proof of work.

In the economic literature trust as a precondition for exchange and trade has generally been subsumed into the general category of transaction costs. Davidson et al. (2018b) argue, however, that while there is some overlap between trust and generic transaction costs, the two concepts can and should be considered separately. Non-economists such as Schneier (2012), Sundararajan (2016), and Werbach (2018) have provided argument and evidence pointing to the importance of trust in a market economy well-beyond the notion of trust simply constituting yet another transaction cost. Schneier suggests society needs a lot of trust and it is costly. Davidson, Novak and Potts estimate the aggregate cost of trust (proxied by the amount of time and effort expended in each occupation to uphold trusting relations) to account for some 35 per cent of U.S. employment. Werbach argues that trust can be thought of as being "confident vulnerability" and he describes a number of architectures of trust. Importantly for our purposes he notes that blockchain "creates a new kind of trust that none of the established models [encompass]." In this section we set out an economic explanation of how distributed ledger technology deploys the proof of work consensus mechanism to create that trust.

The notion of blockchain being a "trust machine" was first proposed by *The Economist*. This view has been criticized as being a naïve model (see for example Vatiero, 2018). In this section we set out a theoretical explanation of how a proof of work consensus mechanism creates trust following Berg et al. (2019). We then use that framework to highlight what trust might mean in a blockchain framework and how trust could, in principle, be undermined in that framework. It is our contention that blockchain can and will dramatically expand the number of transactions that occur, and it will disrupt existing hierarchies and business models. We agree, however, with Vatiero's (2018) analysis that blockchain will not eliminate the need for all intermediaries and external enforcement.

Williamson (1985) has provided a comprehensive theory of how transactions are structured and how performance is monitored (he defines performance monitoring as "governance"). Williamson has specified two behavioral assumptions that drive the contracting process; bounded rationality and opportunism. Bounded rationality relates to the fact that there are limits to human rationality. Opportunism is self-seeking with guile. As Williamson (1985, p. 47) writes, opportunism includes, "calculated efforts to mislead, distort, disguise, obfuscate, or otherwise confuse," and as a result, "[p]romises to behave responsibly that are unsupported by credible commitments will not, therefore, be reliably discharged" (Williamson, 1988, p. 68). Williamson (1993a) argues that the notion of opportunism encompasses the so-called agency problem generated by the separation of ownership and control (see, for example, Jensen and Meckling, 1976). It also includes, and is broader in conception than, adverse selection and moral hazard. These two issues are economic problems that economists understand well. Adverse selection occurs where one party to a transaction has superior information to counterparties to the transaction and relies on that information to the disadvantage of the counterparty. This is a well-known problem in insurance markets. Moral hazard occurs when individuals change their behavior as a result of entering into a contract. It is important to emphasize that agency costs, adverse selection, and moral hazard are special cases of opportunism; they are not separate economic phenomena.

Williamson also relaxes the assumption of capital homogeneity—he employs the term "asset specificity" to denote that capital (assets) cannot always be easily and cheaply redeployed from one use to another. Assets in place to meet the specific needs of specific customers can be a lot more valuable than their next best use and so may be vulnerable to hold-up problems (also a form of opportunism).

These three variables then determine the nature of the contractual process that buyers and sellers employ to conduct their business. **Figure 1** illustrates the menu of alternatives faced by parties to a potential contract.

Short term contracting (Williamson refers to this as being "competition") is characterized by an absence of asset specificity. The capital employed to support the contract is homogenous, but bounded rationality and opportunism may be present. Yet performance in this type of contract is easily observable. This contract could be described as being the use of markets in a Coasian sense. The polar opposite situation—hierarchy—occurs when asset specificity, bounded rationality, and opportunism are all present. The choice between markets and hierarchies is driven by the presence of asset specificity (interacting with bounded rationality and opportunism).

Williamson, however, also discusses two other contracting regimes.

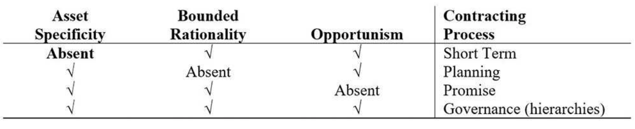
In the absence of either bounded rationality or opportunism contracting becomes trivial. Comprehensive "planning" becomes viable in the absence of bounded rationality while "promise" is viable in the absence of opportunism. The implications of a lack of opportunism are quite profound—Williamson (1993a, p. 97) argues, for example, that "most forms of complex transacting and hierarchy vanish." Hodgson (2004) argues this is an empirical claim, not a principled claim. Nonetheless it would be possible and credible to insert a "general clause" into contracts that promises to self-enforce the contract in the spirit of the original agreement.

Williamson (1993a) makes the argument that if parties to a contract promise to engage in cooperative behavior, *and* those contracts were self-enforcing, then promise is an efficient mechanism to facilitate trade. That sounds very much like what the blockchain and smart contracts (algorithmic contracts maintained and that are resolved on blockchains) can offer. Indeed, this could be what is meant when blockchain is described as being "trustless." This viewpoint would be consistent with Williamson (1993a) suggestion that "[t]rust is sometimes treated as an antonym for opportunism." Williamson (1993b), however, thinks this view is not quite correct and argues that calculated cooperative behavior should not be considered as being trustworthy.

Williamson illustrates his argument regarding opportunism and the control of opportunism using a diagram similar to our **Figure 2** (Berg et al., 2019). In Williamson's case he is contemplating a make or buy decision—we generalize his framework beyond that simple situation. In the first instance, following Williamson, consider modes A, B, and C. In the diagram "k" represents an investment hazard associated with opportunism. If there is no opportunism, then k = 0. In that instance contracts can be organized by what Williamson describes as being "competition"—contractual performance is easily observed and non-compliance is easily corrected. This is a short-term contract. In terms of **Figure 1** asset specificity is absent.

In those instances, however, where $k \neq 0$, then the question of contractual safeguards (denoted as "s") becomes important. Consider, for illustrative purposes, the well-known market for lemons problem—the purchase of a second-hand car that may or may not be defective (Akerlof, 1970). As the problem is usually described, the used car salesman has superior information as the true status of the car than does the buyer. To the extent that the car is defective, the salesman has an incentive to suppress that information i.e., behave opportunistically. In the instance that a used car salesman cannot adequately signal ($s = 0$) their trustworthiness (i.e., credibly commit to not defrauding the buyer) the transaction may not occur at all, or if it does, it will do so at a deep discount to true value. Of course, we know that various mechanisms to safeguard transactions evolve ($s > 0$) ensuring that transactions do occur. These mechanisms, however, are costly and impose costs on the parties to the transaction. Ultimately there are a range of transactions that never occur because costs ($k + s$) swamp the gains from trade—in other words, the gains from trade are not fully realized in a world of positive transactions costs and in a world characterized by a lack of trust.

The important point being that trust as usually described by economists is a mechanism to overcome opportunism—trust in **Figure 2** can be thought of as being "s"; the solution to problem k, not the absence of problem k.



Asset Specificity	Bounded Rationality	Opportunism	Contracting Process
Absent	√	√	Short Term
√	Absent	√	Planning
√	√	Absent	Promise
√	√	√	Governance (hierarchies)

FIGURE 1 | Williamson's contracting processes. Source: Berg et al. (2019).

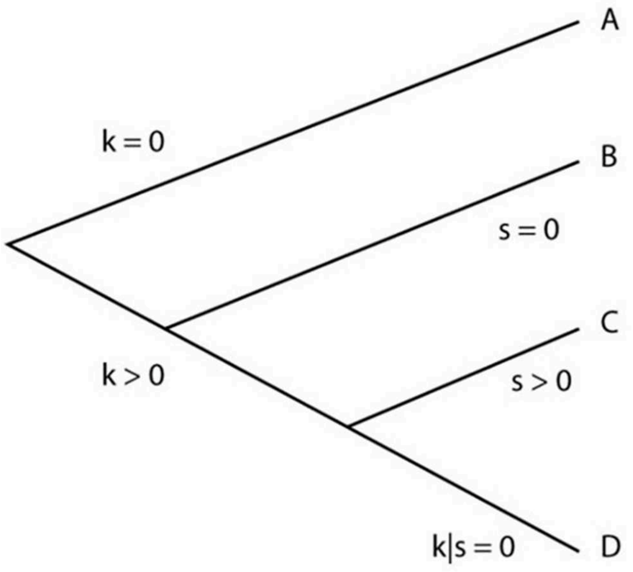


FIGURE 2 | Opportunism and contracts. Source: Berg et al. (2019).

In the context of a blockchain it would be easy to argue that the technology provides a safeguard to transactions when $k > 0$ and merely constitutes $s > 0$. This is how we understand the argument that the blockchain is a general purpose technology (Pilkington, 2015; Catalini and Gans, 2016; Yermack, 2017). The suggestion being that $s_{\text{Blockchain}} < s$; all that the blockchain does is further reduce existing transaction costs.

What blockchains do, however, is somewhat more subtle.

In Williamson's scheme k and s are independent of each other. Opportunism exists in the world giving rise to investment hazards and various safeguards emerge to facilitate trade. The transactions costs are cumulative and are borne by the parties to the transaction. Strictly Williamson assumes that the cost s is borne by the buyer. We make no assumption as to the eventual burden of s.

Blockchains that operate under a proof of work consensus mechanism, we believe, are best understood by reference to mode D. Now we have a transaction that ordinarily would have been associated with investment hazards due to opportunism and could take place in a non-blockchain environment if $s > 0$.

Conversely the transaction can occur on a blockchain.

Blockchain technology incorporating proof of work implies that for the parties to the transaction $k|s \approx 0$. It is not that s overcomes problem k at some cost to the parties, but that blockchains suppress k at a cost to a third party (miners). This implies that employing a blockchain would be a preferred transaction technology to both B and C. This is the mechanism whereby blockchains can and will disrupt existing hierarchy and business models. The condition $k|s \approx 0$ is not an externality—miners are paid to record transactions although they themselves are not party to the transaction. As a result of this feature the blockchain can be thought of as being a three-sided market. Three distinct groups of users must be simultaneously satisfied—buyers and sellers who transact, *and* miners who record those transactions.

DISCUSSION

The notion that a proof of work blockchain is a trust machine—or industrializes trust—has been described as being naïve. In the absence of a theory or detailed explanation as to how that trust is generated the naïve label may be appropriate. We, however, have provided a theory of how proof of work creates trust by suppressing opportunism (see also Berg et al., 2019). In our story, a world of "promise" becomes a viable alternative to governance: this lowered cost of promise expands the number of transactions that can occur now that transaction costs are reduced. As Williamson suggests, many problems of contracting become trivial or disappear. It is possible to promise to behave responsibly.

The benefits of the proof of work mechanism, however, should not be oversold.

Not all forms of opportunism are suppressed in a world of blockchain and smart contracts. Only those forms of opportunism that can be excluded by the operation of a smart contract are suppressed. This may include, for example, non-payment or non-performance of the terms of the contract or the automatic payment of penalty clauses and the like. It will not, however, preclude all forms of opportunism.

It should be emphasized that proof of work suppresses opportunism, it does not suppress bounded rationality. One of the consequences of bounded rationality is that contracts will be incomplete. While the ability to include smart contracts into a blockchain may have the effect of making (some) contracts more complete, it remains the fact that contracts will always be incomplete. Distributed ledger technology does not overcome bounded rationality problems.

It is also the case that distributed ledger technology cannot overcome maladaptation costs. Williamson's notion of maladaptation costs is due to a shifting contract curve. Aoki (1983), however, suggests that the shifting contract curve is due to the optimal contract deviating from the agreed contract over time. As circumstances in the real-world change over time, so the contract that individuals would have entered into also changes. While Williamson suggests that is a bounded rationality problem—not being able to write complete contracts because agents cannot foresee the future should rather be characterized as being a radical uncertainty problem. The distinction between bounded rationality and radical uncertainty is important. The former implies that individuals could never imagine every possible future outcome because of limited cognitive ability. The latter implies that individuals can never imagine every possible future because the future in inherently unknown. For Williamson's purposes the distinction is less important—bounded rationality works well in his theory—but in a world of artificial intelligence and the like human cognitive limitation could be less binding. Nonetheless we argue that radical uncertainty will ensure that contracts remain incomplete.

The important point is that a proof of work blockchain is not a miracle machine. It does, however, overcome many of the trust problems that current preclude transactions from occurring, or allow them to occur at a high cost. Those trust problems that arise due to bounded rationality and radical uncertainty, and the interaction between those two concepts, are not resolved by a proof of work blockchain. It is unlikely that a proof of stake blockchain would resolve them either.

Then we need to give some thought to the miners who secure the blockchain. Our argument is that $k|s \approx 0$, but as we suggest above, not all k is suppressed. Furthermore, however, what of the safeguards in the mining process? One of the benefits of the blockchain is that it resolves the double spending problem in a decentralized manner. What happens if the mining process is not decentralized? This raises a series of empirical questions. For example, how decentralized does the mining process have to be in order to adequately safeguard a blockchain? Does the existence of mining pools undermine the decentralization characteristics of a blockchain?

CONCLUSION

Our contribution here is to demonstrate that blockchains are platforms for three-sided bargaining. Expenditure s by miners suppresses k—opportunism on the part of buyers and sellers.

The analysis in this paper clarifies that blockchains are trust machines. Blockchains convert energy-intensive computation into economically-valuable trust. We expect to see rapid increases in the efficiency of these machines, as were seen in previous waves of industrialization. Of course, trust problems are not entirely eliminated from the economy by the application of distributed ledger technology: not all transactions can be digitized, not all exchanges can be reduced to a smart contract, and the technology does not prevent con artists spruiking business ideas that are inherently fraudulent. What this paper demonstrates is that a well-designed three-sided market, where transactions are recorded by miners hoping to earn native tokens, industrializes trust. Where trust is currently provided through institutional technologies—reputation, in the case of markets, and hierarchy in the cases of governments and firms—blockchains present a competitive challenge to those institutions along the technical margins of ledgers.

At the same time, our analysis highlights that blockchains are not miracle machines. Not all forms of opportunism can or will be suppressed. Smart contracts cannot resolve all contractual problems. Bounded rationality and radical uncertainty will mean that external legal enforcement and some intermediaries will remain important and viable in the economy. One immediate source of viability arises as smart contracts may be inflexible (Vatiero, 2018) and need to be renegotiated as maladaptation costs rise.

What we have attempted here is to demonstrate that the notion of industrialized trust is not a cure-all economic miracle, but neither should it be dismissed as being naïve. Future research will attempt to provide a basic economic analysis and understanding of other consensus mechanisms such as proof of stake. Proof of work converts electricity into valuable trust—proof of stake converts risk capital into valuable trust. The economics of that conversion are likely to be much more complex.

AUTHOR CONTRIBUTIONS

This paper was jointly conceptualized and written by CB, SD, and JP.

REFERENCES

Akerlof, G. (1970). The market for "lemons": quality uncertainty and the market mechanism. *Q. J. Econ*. 84, 488–500. doi: 10.2307/1879431

Aoki, M. (1983). Managerialism revisited in the light of bargaining-game theory. *Int. J. Ind. Organ*. 1, 1–21. doi: 10.1016/0167-7187(83)90020-6

Berg, C., Davidson, S., and Potts, J. (2019). *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics* (Cheltenham: Edward Elgar Publishing). doi: 10.4337/9781788975001

Catalini, C., and Gans, J. (2016). *Some Simple Economics of the Blockchain*. Cambridge, MA: National Bureau of Economic Research. doi: 10.3386/w22952

Coase, R. (1937). The nature of the firm. *Economica* 4, 386–405. doi: 10.1111/j.1468-0335.1937.tb00002.x

Davidson, S., De Filippi, P., and Potts, J. (2018a). Blockchains and the economic institutions of capitalism. *J. Inst. Econ*. 14, 639–658. doi: 10.1017/S1744137417000200

Davidson, S., Novak, M., and Potts, J. (2018b). The cost of trust: a pilot study. *J. Br. Blockchain Assoc*. 1, 21–27. doi: 10.31585/jbba-1-2-(5)2018

Hileman, G., and Rauchs, M. (2017). *Global Cryptocurrency Benchmarking Study*. Cambridge Centre for Alternative Finance. Available online at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

Hodgson, G. M. (2004). Opportunism is not the only reason why firms exist: why an explanatory emphasis on opportunism may mislead management strategy. *Ind. Corp. Change* 13, 401–418. doi: 10.1093/icc/dth016

Jensen, M., and Meckling, W. (1976). Theory of the firm: managerial behaviour, agency costs and ownership structure. *J. Finance Econ*. 3, 306–360. doi: 10.1016/0304-405X(76)90026-X

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online at: www.bitcoin.org

Narayanan, A. J., Bonneau, J., Felton, F., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University Press.

Pilkington, M. (2015). "Blockchain technology: principles and applications," in *Research Handbook on Digital Transformations*, eds F. Olleros, and M. Zhegu (Cheltenham: Edward Elgar), 225–253.

Schneier, B. (2012). *Liars and Outliers: Enabling the Trust That Society Needs to Thrive*. Indianapolis: Wiley.

Sundararajan, A. (2016). *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*. Cambridge: MIT Press.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: OReilly Media.

Szabo, N. (2014). *The Dawn of Trustworthy Computing*. Available online at: https://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html?m=1

Vatiero, M. (2018). *Smart Contracts and Transaction Costs*. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259958

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. Cambridge: The MIT Press. doi: 10.7551/mitpress/11449.001.0001

Williamson, O. (1985). *The Economic Institutions of Capitalism*. New York, NY: The Free Press.

Williamson, O. (1988). The logic of economic organization. *J. Law Econ. Organ.* 4, 65–93.

Williamson, O. (1993a). Opportunism and its critics. *Manage. Decis. Econ*. 14, 97–107. doi: 10.1002/mde.4090140203

Williamson, O. (1993b). Calculativeness, trust, and economic organization. *J. Law Econ. Org*. 36, 453–486. doi: 10.1086/467284

Yermack, D. (2017). Corporate governance and blockchains. *Rev. Finance* 21, 7–31. doi: 10.1093/rof/rfw074

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.