Blockchains industrialise trust

Chris Berg, Sinclair Davidson and Jason Potts*

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

Keywords: blockchain, transaction costs, industrialisation, platforms

20 November 2017

* RMIT Blockchain Innovation Hub, School of Economics, Finance and Marketing, RMIT University.

1. Introduction

The blockchain is the underlying technology that powers the cryptocurrency Bitcoin (Nakamoto 2008). Since Bitcoin's release in 2009, blockchains have been applied to a wide variety of use-cases from financial clearing, to identity management, to distributed computing. Here we apply Williamson's (1985, 1988, 1993) transaction cost analysis to understand the economic attributes of blockchain technology. Blockchains are sometimes described as "trustless" (Swan 2015, Kiviat 2015). Williamson's approach clarifies that blockchains are not trustless. Rather, they are *trust machines*, and their use constitutes the *industrialisation of trust*. Blockchains suppress opportunism costs that would otherwise prevent exchanges taking place.

2. The economic significance of blockchains

Digital currencies are vulnerable to the "double spending" problem – similar to the counterfeiting problem with paper currency. Typically this problem has been solved by relying on a trusted intermediary to validate transactions. With Bitcoin, the pseudonymous "Satoshi Nakamoto" (2008) developed a native digital currency which was not reliant on a centralised authority. Bitcoin is a digital distributed ledger that records transactions – that is, achieve consensus on what transactions are to be included in the ledger – in a decentralised manner.[1]

In Bitcoin the consensus mechanism is known as "proof-of-work". Proof of work rewards "miners" who compete to solve a computationally difficult puzzle that allows them to create a new block of transactions in the blockchain, claim a reward (currently 12.5 Bitcoin), and claim any transaction fees offered by users of the network to prioritise their transactions. Consensus in the network is established by following the longest chain of blocks. Proof of work is extremely energy-intensive and requires significant capital investment. An alternative blockchain consensus mechanism is "proof of stake", which requires allows large cryptocurrency holders to validate transactions. Other consensus mechanisms are in various stages of development. Their basic attribute is that those who validate changes on the shared ledger are rewarded with a valued token native to the network (a coin).

It is an open question whether blockchains as established by Nakamoto will persist or simply become an historic curiosity. Its significance is that decentralised distributed ledgers have been shown to be viable. The economic study of distributed ledgers is in its infancy. One strand of the literature conceptualises blockchains as a new *general purpose technology* (see Bresnahan and Trajtenberg 1995), characterised by its broad potential use-cases ("pervasiveness") and complementarity with other technologies. Blockchains reduce the costs of verifying identities and networking without intermediaries; opening up the possibility of new markets, and significantly reducing transaction costs in existing markets. (Catalini and Gans 2016, Pilkington 2015, Yermack 2017). Another strand sees blockchains as an *institutional technology*. Blockchain is a decentralised computation technology for coordinating activity in a distributed economy (Davidson, de Filippi and Potts forthcoming, Berg 2017). This view follows in the transaction school tradition of Nobel laureates Ronald Coase and Oliver Williamson and sees the blockchain as a new type of economic institution that enhances (and competes with) the existing economic institutions of capitalism: firms, markets, commons, relational contracting, and governments.

[1] We do not consider the possibility of centralisation in Bitcoin mining power here.

3. Opportunism vs. trust

Oliver Williamson (1985) has provided a comprehensive theory of how transactions are structured and performance monitored (he defines performance monitoring as "governance"). Williamson has specified two behavioural 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: 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: 68). Williamson (1993) 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 well-understand. Adverse selection occurs where one party to a transaction has superior information to counter-parties 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 behaviour as a result of entering into a contract.

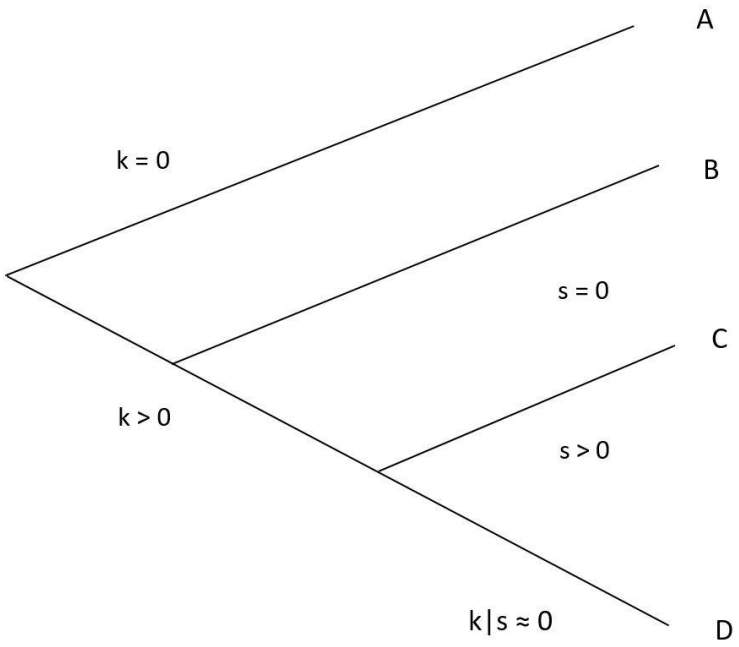
In the absence of bounded rationality or opportunism contracting becomes trivial. Comprehensive "planning" becomes viable in the absence of bounded rationality while "promise" is viable in the absence of opportunism. The implications of a lack of opportunism are quite profound – Williamson (1993: 97) 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. In this manner deviations from the Aoki contract curve would be quickly corrected.

Williamson (1993) makes the argument that if parties to a contract promise engage in co-operative behaviour 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 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's (1993) suggestion that "[t]rust is sometimes treated as an antonym for opportunism". Yet Williamson thinks this view is not quite correct and we agree. As Williamson argues calculated cooperative behaviour is not trustworthy.

Williamson illustrates his argument regarding opportunism and the control of opportunism using a diagram similar to our figure 1. In the first instance consider modes A, B, and C. In the diagram k represents an investment hazard associated with opportunism. If there were no opportunism $k = 0$. In that instance contracts can be organised by what Williamson describes as being "competition" – contractual performance is easily observed and non-compliance easily corrected. In those instances where $k \neq 0$ then the question of contractual safeguards (s) becomes important. Consider the well-known market for lemons problem, 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 occur will do so at a deep discount to true value. Of course, we well know that various mechanisms to safeguard transactions evolve ($s > 0$) ensuring that transactions do occur. These mechanisms, however, are costly and impose that cost 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 realised in a world of positive transactions costs.

Figure 1: Opportunism and Contracts



The important point being that trust as usually described by economists is a mechanism to overcome opportunism – trust in figure 1 is "s"; the solution to problem k, not the absence of problem k.

In the context of the 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 (Catalini and Gans 2016, Pilkington 2015, Yermack 2017). The suggestion being that $s_{Blockchain} < s$; all that the blockchain does is further reduce existing transaction costs. What blockchains do, however, is slightly 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. Blockchains 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. The blockchain technology incorporating proof of work (or proof of stake) 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 business models. The condition $k|s \approx 0$ is not an externality – miners are paid to validate and 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 and validate those transactions.

4. Conclusion

In the schema described above, blockchains are platforms for three-sided bargaining. Expenditure s by miners suppresses k. Miners are rewarded for their work by valuable native tokens. Transaction fees denominated in the native token provide an economic incentive for prioritising transaction validation. This has distributional consequences. What users (that is, those who send and receive transaction outputs) want and what miners want for the network can differ and need to be balanced. A fourth group - those who seek to hold cryptocurrency tokens (investors) - have different interests again.

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 industrialisation.

5. Bibliography

Berg, C, 2017, What Diplomacy in the Ancient near East Can Tell Us about the Blockchain, *SSRN Working Paper*.

Bresnahan, T. and M. Trajtenberg, 1995, General Purpose Technologies: 'Engines of Growth'?, *Journal of econometrics* 65, 83 – 103.

Catalini, C. and J. Gans, 2016, Some Simple Economics of the Blockchain, National Bureau of Economic Research.

Coase, R, 1937, The nature of the firm, *Economica*, 4(16), 386 – 405, Reproduced in R. Coase, 1988, *The firm, the market, and the law*, University of Chicago Press.

Davidson, S., P. De Filippi, and J. Potts, forthcoming, Blockchains and the economic institutions of capitalism, *Journal of Institutional Economics*.

Hodgson, G. M., 2004, Opportunism is not the only reason why firms exist: why an explanatory emphasis on opportunism may mislead management strategy, *Industrial and Corporate Change*, 13(1) 401 – 418.

Jensen, M. and W. Meckling, 1976, Theory of the firm: Managerial behaviour, agency costs and ownership structure, *Journal of Financial Economics*, 3(4), 306 – 360.

Nakamoto, S, 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, (www.bitcoin.org2008).

Pilkington, M. 2015, Blockchain Technology: Principles and Applications, In F Olleros and M Zhegu (eds.) *Research Handbook on Digital Transformations*, Edward Elgar.

Williamson, O. 1985, *The economic institutions of capitalism*, The Free Press.

Williamson, O. 1988, The logic of economic organization, *Journal of Law, Economics, and Organization*, 4(1), 65 – 93.

Williamson, O. 1993, Opportunism and its Critics, *Managerial and Decision Economics*, 14(2), 97 – 107.

Yermack, D, 2017, Corporate Governance and Blockchains, *Review of Finance* 21, 7 – 31.