Blockchain: Evolution of Trust in Crypto-Economies

Husain Khambaty

RMIT University, Melbourne

Abstract

As blockchain helps to decentralise different ledgers in various industries, it is necessary to understand and critique the principles on which blockchain is based whilst also evaluating on how the implementation does assist in helping replace trust with mathematical evidence. This literature review will analyse multiple sources and provide an in-depth overview of blockchain as a decentralised distributed trust architecture.

Keywords: blockchain; decentralised; crypto-economy;

Contact: info@husainkhambaty.com | https://husainkhambaty.com

Introduction

In today's economy, when considering economic exchanges of any form, institutions play an important role as a third-party to manage ledgers, help provide and enforce trust and mediate when required to provide a fair outcome. The fundamental qualities of a ledger is that it possesses clarity, consistency and consensus thereby recording identity, property, contract and value *(Davidson, S., Filippi, P.D., Potts, J. 2018, p 642)* along with time and location. A ledger helps record transactions as a consequence of economic actions. This implies that trust is another fundamental quality that a ledger needs to possess. When a ledger is centralised or governed by a central authority, trust is the highest, however it comes at a significant cost both in terms of overhead processes, regulation and enforcement. Hence trust is required yet expensive to manufacture and maintain.

With implementing blockchain and decentralising the ledger and using a 'trustless' architecture, one is able to lower the cost of trust and substitute a trusted third-party with public verification and consensus for auditing *(Davidson, S., Filippi, P.D. & Potts, J. 2018, p 643).*

This literature review will attempt to appraise the Blockchain technology by discussing the evolution of ledgers, necessity and industrialization of trust, role of institutional crypto-economies and how Blockchain is helping replace trust to record and validate transactions.

What is Blockchain?

Blockchain was initially revealed in a paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" by an unknown author (or a group of authors) using the pseudonym "*Satoshi Nakamoto*" in 2008. The primary aim was to build a decentralised version of digital currency that would enable people to spend without relying on a financial institution.

In theory, a blockchain is an open decentralised and distributed ledger system that records transactions between two parties in a permanent way without the need of a third-party intermediary. A blockchain comprises a list of records also known as blocks that are mapped to each other using cryptographic implementations. Each block contains information about the previous block stored in a hash format, a timestamp and transactional data.

Blockchains are decentralised, immutable, provide traceability with privacy, trust and reliability. Blockchains are not limited to digital currencies but extend to any ledger systems. Other use cases apart from finance include healthcare, transportation, aviation, insurance, supply chains, healthcare, etcetera.

Decentralised and distributed ledgers

Ledgers are an old approach for recording who owns what and who has agreed to what, and helps to record anything of value *(Berg, C, Davidson, S, & Potts J 2018. p. 642)*. By definition it is "A book for keeping notes, especially one for keeping accounting records" *(Berg, C., Davidson, S. & Potts, J. 2018. p. 3)*. It helps to provide an authoritative account at a point in time. The evolution of ledgers from books where methods such as double-book keeping systems enabled a distributed consensus yet were quite susceptible to alterations and therefore were only trusted as long as the authorities were trusted.

There are typically three analytic categories of ledgers: an *actual ledger*, a *general ledger*, and a *perfect ledger (Berg, C., Davidson, S. & Potts J 2018. p. 5)*. An actual ledger is an existing real world ledger that is present either in physical or digital form. A general ledger is a theoretical construct or an idea that all transactions are mapped to a ledger while a perfect ledger is the ideal standard for comparison that is not bounded by technology, economic, social or political limitations. Ledgers help to confirm ownership, identity, status or authority *(Berg, C., Davidson, S. & Potts, J. 2017, para 5)* — they basically help map economic and social relationships.

As cited by *Perepa, B & Brakeville, S. (2018)*, the challenges with ledgers are that they are inefficient, costly and subject to misuse and tampering. Moreover the lack of transparency and possibility of corruption and fraud results in disputes. This often results in reversing transactions to resolve issues and is a costly affair alongwith the risk that contributes to missed business opportunities. This is where a distributed ledger helps to provide an efficient, tamper-proof, immutable and transparent system to address the issues of a traditional centralised ledger system.

A decentralised ledger is a database that is shared and replicated in real-time and synchronized among other peers of a network. This ledger helps to record all transactions and the members govern the network and agree on a consensus to update the records.

The Importance of Trust

Trust plays a vital role in any mode of economic interaction *(Potts, J Novak, M. & Davidson, S 2018 p2),* and that reputation is one of the solutions to trust problems (*Klien, 1997*, *cited by Berg, C, Davidson, S, Potts, J 2020)*. Traditionally trust was derived from reputation, relationships or references from people we trust. However in these conditions, the mechanisms and institutions that enforce trust and restrain any breaches end up adding on to the cost of trust. Davidson, S., Berg, C. & Potts, J (2018, cited by *Berg, C., Davidson, S. & Potts, J 2020*) estimated that trust accounted for 35 percent of US employment (using 2010 data) to generate, maintain and enforce and the figure extrapolated to the global scale would be about USD $29 trillion — trust is quite costly to create and maintain. To reduce the cost of trust, it is important to revolutionise trust thereby creating "industrialised" trust. This is where blockchain or a distributed ledger technology has the potential by providing another form of trust or a form of "trustless" trust.

Blockchain as a trust mechanism

Based on *Nair, M & Sutter, D (2018, p 534 - 536)* — Blockchain helps provide a publicly verifiable information distributed ledger that is a crucial first mechanism that leads to the creation of trust. In addition, open entry and decentralised network of miners acts as a second mechanism to help create trust. Lastly, the open-source nature of the blockchain code and decision-making process plays the third mechanism to create trust where anyone can read the code and a consensus is required within senior independent developers to make changes to the code thereby reducing any malice or opportunistic behaviour.

As noted by *Berg, C., Davidson, S. & Potts, J. (2019)*, proof-of-work[1] type distributed ledger helps to industraliase trust by creating a three-sided market consisting of buyers, sellers and miners, where miners secure the network by providing computing power and energy. The proof-of-work is a consensus protocol that transforms expensive work into trust. Moreover with the industrialisation of trust, a V-form organisation is introduced that is outsourced and vertically integrated that is tied together by distributed technology. The distributed organisation would consist of a group of independent companies *(Berg, C, Davidson, S, Potts, J 2020, p. 7)* that utilise distributed ledger technology to coordinate and audit transactions done previously by corporate offices.

Blockchain uses mathematical cryptography, open source software, computer networks and incentive mechanisms *(Berg, C, Davidson, S, Potts, J 2018, p 643)* to replace trust. A blockchain is nothing but a decentralised and distributed database that is secured using cryptography and incentivised using crypto-economic means. By using a public distributed ledger system, one is able to lower the cost of trust and substitute a trusted third-party with public verification and consensus for auditing *(Davidson, S., Filippi, P.D. & Potts, J. 2018, p 643)*. Blockchain helps to build and use ledgers securely and effectively and make use of consensus without the requirement of centralised trust. Blockchain uses consensus protocols to help solve complex mathematical puzzles to add a transaction to a block and create new blocks. In order to modify a past block, an attacker would have to redo the proof-of-work of the block and all the blocks after it thereby increasing the complexity with the increase in number of blocks *(Nakamoto, S., 2008)* and hence the probability of a slower attacker catching up diminishes exponentially over time. Hence proof-of-work or any consensus protocol helps to replace trust with mathematical and/or cryptographic puzzles to record transactions or change.

[1] Proof-of-work is one type of consensus protocol. There are several others such as proof-of-stake, proof-of-space and proof-of-elapsed-time. *See* https://www.section.io/engineering-education/blockchain-consensus-protocols

Evolution of modern capitalism

The 2009 Nobel laureate in economics, *Oliver Williamson* has argued that 'people produce and exchange in markets, firms or governments depending on the relative transaction costs' *(Berg, C., Davidson, S. & Potts, J. 2017, para. 24)*. Williamson provides a key to understanding which institutions manage which ledgers and why based on his transaction cost approach. Institutions such as governments manage ledgers or privilege or authority such as databases of citizenships, tax, social security and property ownership. Firms also maintain ledgers such as employee records and access, suppliers and customers, assets and debts; thereby implying that firms are a group of contracts.

Blockchain can help governments and firms to make their ledgers more reliable and efficient, and improve reconciliation in near real-time. The immutability and transparency can help governments implement tamper-proof ledgers while also providing the people more visibility into their data. However blockchain also competes against institutions in a decentralised and distributed manner and can help to replace institutions.

Institutional cryptoeconomics

The purpose of economics is to study the production and distribution of scarce resources alongwith the factors that underpin the production and distribution *(Berg, C., Davidson, S. & Potts, J. 2017, para. 32)*.

Institutional economics focuses on understanding the evolution and role of institutions in shaping economic behaviour. It helps to understand the economy that is based on rules such as laws, property rights, regulations and social norms; and as mentioned by *Ostrom (2015)* these rules are used to determine who is eligible to make decisions, what actions are allowed or restricted, what aggregation rules will be used, what procedures must be followed, what information must or must not be provided, and what payoffs will be assigned to individuals dependent on their actions. These are the rules that are used, monitored, and enforced when people make decisions on their actions.

Institutional cryptoeconomics helps to study the institutional economics of blockchain and the cryptoeconomy *(Berg, C., Davidson, S. & Potts, J. 2017, para. 35)* where the economy is a system to coordinate exchange of value. In traditional institutional economics we take rules into consideration while in institutional cryptoeconomics we focus on ledgers. Institutional cryptoeconomics helps us take a peek at the new blockchain revolution and provide us an understanding at what level will blockchain disrupt the economy. It is interested in the rules that govern ledgers, social, political and economic institutions.

As described by *Davidson, S., Filippi, P.D. & Potts, J. (2018, p 654),* blockchain based distributed ledger technology adds an additional category to *Williamson's (1985) 'economic institutions of capitalism'* called decentralised collaborative organisation (DCO). A DCO is an organisation but not hierarchical, resembles a market due to the token system however is not a market due to the predominant nature of activity being produced and not exchanged, and the governance resemblance of a nation state due to the mutual agreement of all members who participate in it, with automatic execution of rules through smart contract enforcement *(Atzori 2015, cited* by *Davidson, S., Filippi, P.D. & Potts, J. 2018, p 654)*.

As blockchain is a new technology and not every ledger is a best use case for blockchain, it is interesting to observe how different implementations will impact the real world in the political and economic front especially when we have deep-rooted established powerful institutions *(Berg, C., Davidson, S. & Potts, J. 2017, para. 40)* that already provide these ledger systems.

Conclusion

In conclusion blockchain helps to replace trust with the means of an open, distributed and decentralised ledger system to help maintain a system of record for any purposes and secured using cryptographic means and a consensus protocol between unknown entities spread out across the globe and connected by the internet. The system of record is immutable and encrypted that assists with the objective to replace central authorities or institutions that help to create and maintain this trust with a decentralised secure ledger which in turn helps to reduce the cost of trust. In addition institutional cryptoeconomies play a significant role in analysing the impact of blockchain on the current economy from a social, political and economical context.

References List

Nakamoto, Satoshi 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System* <https://bitcoin.org/bitcoin.pdf>

Berg, C., Davidson, S. & Potts, J. 2017, AUS. *The Blockchain Economy: A beginner's guide to institutional cryptoeconomics*. <https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4>

Davidson, S., Filippi, P.D., Potts, J. 2018, AUS. *Blockchains and the economic institutions of capitalism* <https://primo-direct-apac.hosted.exlibrisgroup.com/permalink/f/aqirjb/TN_cdi_hal_shs_oai_HAL_hal_01850927v1>

Davidson, S., Novak, M & Potts, J 2018, AUS. *The Cost of Trust: A Pilot Study* <https://ssrn.com/abstract=3218761>

Berg, C., Davidson, S. & J. Potts. 2018, AUS. *Outsourcing vertical integration: Distributed ledgers and the V-form organisation*. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3612419>

Berg, C., Davidson, S & Potts, J 2019, AUS. *Blockchain Technology as Economic Infrastructure: Revisiting the Electronic Markets Hypothesis. Frontiers in Blockchain.* <https://www.frontiersin.org/articles/10.3389/fbloc.2019.00022/full>

Berg, C., Davidson, S & Potts, J 2020, AUS. *Trustless architecture and the V-form organisation* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3612419>