EasyChair Preprint

№ 3908

Blockchain Technology's Impact in Voting, Financial Transactions and Healthcare Data Management

Leo Fuentes

July 19, 2020

Blockchain Technology's Impact in Voting, Financial Transactions and Healthcare Data Management

Leo Fuentes
COMP1001
Flinders University, South Australia

fuen0012@flinders.edu.au

Abstract

While blockchain technology has only been around for twelve years, its potential has proved that it may be one of the most fundamental technologies for the future to come. Its base characteristics and functionalities are showing experts around the globe its potential. In the last few years, blockchain technology has been emerging in multiple industries and is beginning to solve a range of existing problems.

1 Introduction

Blockchain technology was brought to life in 2008 by *Satoshi Nakamoto*. Ever since its inception, blockchain has changed data transmission between computers in both security and accessibility. Blockchain's ability to provide a secure, robust, and transparent (Davidson et al. 2016) transaction ledger (a record of transactions) is opening avenues for future application and development. Together with continuous improvements to cryptography, this technology may be the future of data storage and transmission. Already, blockchain has been recognised as an alternative to traditional systems in voting, financial transactions, and even healthcare.

2 The Form and Function of Blockchain

A blockchain is a record of information, each stored in *blocks* (Narayanan et al. 2016). Each *block* is linked through a cryptographic hash, which represents the transaction information as well as the time it occurred.

At its core, blockchain is the solution for the well-known 'Two Generals' Problem' which poses the problem of several army commanders communicating accurate information reliably (Küfner, 2018). In a public blockchain, several safety measures must be taken in order to prevent malicious activity or system malfunction. In order to do so, blockchain algorithms fully rely on a mechanism that validates the transactions (Swanson, 2015), these include proof of work and proof of stake. Using proof of work requires the participant's computer to undergo immense calculations through solving a mathematical puzzle (Pilkington, 2015). This is commonly referred as 'mining' in a crypto-currency context, in which the first computer to solve the puzzle is rewarded with part of the transaction fees (Davidson et al. 2016). On the other hand, proof of stake consists of the algorithm choosing a random participant that has accumulated sufficient reserves. This method is mostly applied to cryptocurrencies in which participants have monetary reserves (Duong et al. 2017).

3 The Problems Blockchain Solve

Blockchain is a revolutionary tool that allows for reliable and secure communication between entities, making its applications virtually endless. Currently, it is reshaping the way we think about fundamental aspects of our lives, such as voting, financial transactions, and even healthcare.

3.1 Voting

With an increasing population of eligible voters, many countries are starting to face issues with the practicality of traditional voting methods. Estonia was the first to implement electronic voting in its presidential election (Ayed, 2017). However, with the proposed e-voting system came major security breaches. The current standard voting paper-based systems contains flaws in two major areas; they rely on the honesty and validity of the people counting. Another major issue is that currently, voting is not scalable, which leads to problems in the accuracy of the votes (Ayed, 2017). Implementing blockchain technology into e-voting is becoming increasingly plausible due to its robust

security. Conducting votes electronically with blockchain is eliminating these setbacks and enabling it to complete tasks such as counting votes much faster. By design, blockchain technology is secure, however, its implementation would require a system which ensures authenticity, anonymity, accuracy, and verifiability on a large scale (Ayed, 2017). With a reliable voting system put in place, blockchain technology could change the way we vote.

3.2 Financial Transactions

Blockchain has not only provided revolutionary technology to improve voting but has shown to be extremely beneficial for peer to peer transactions. Initially, Satoshi Nakamoto created blockchain technology to be used as a transaction ledger for bitcoin, a decentralised currency (Swanson, 2015). One of the main advantages of using blockchain-based currencies (cryptocurrency) is the absence of a third-party financial institution, which operate in a centralised system (Nakamoto, 2008). Bypassing a third-party is appealing due to its efficiency. Transactions are processed significantly faster, often also alleviating the third-party's fee (Fanning et al. 2016). In addition, the implementation of a peer to peer network (decentralised system) eliminates privacy breach risks (Swanson, 2015) that may occur within a centralised system. Rather, each transaction is made public but cannot be traced back to anyone. This is a growing problem within third-party financial services - regulations such as the 'Dodd-Frank' require more transparency and reporting from ledgers.

3.3 Healthcare Data Management

Healthcare data management covers a wide range of crucial information regarding diagnosis, treatment, and any physical or mental impairments (Jothi et al. 2015). On top of this, a substantial amount of data includes that of personal or sensitive information. In many countries, healthcare is a rapidly growing industry (Jothi et al. 2015), with it, a considerable amount of confidential data is being constantly created and handled. Blockchain's ability to securely and reliably transfer information seems promising for the future of the healthcare industry in data management. Data recorded in blockchains can only be created, and not removed or altered (Dimitrov, 2019), which increases the security and confidentiality of the patient. Additionally, it is stored in a decentralised network, meaning it can be accessed much faster from any computer with the appropriate digital signature (Dimitrov, 2019), giving way to nationwide interoperability. Furthermore, this process is significantly more reliable and secure than standard centralised data storage systems. In healthcare data, blockchains can be used in a variety of ways; one of the most recognised aspects is securely storing a patient's information. Without a key or digital signature, it is practically impossible to decrypt it (Dimitrov, 2019).

4 The Future of Blockchain

The future is bright for the implementation of blockchain technology, with time, it is being implemented to an increasing number of industries. Some industries have not yet started using this due to some flaws: within cryptocurrency, if a certain group of minors has control of 51% or more of the processing power to complete the mathematical puzzle (mining), they are able to interrupt new blocks (Swanson, 2015). Although this is not practical, it will always be a threat to the reliability of blockchain technology. While this is not currently pragmatic, quantum computing's unparalleled processing power may pose a threat to blockchain's security (Stewart et al. 2018). However, quantum-resistant cryptography seems like a secure alternative for the near future (Munson et al. 2017). While these flaws are concerning, they mainly threaten financial transactions that belong to public blockchains. Whereas, private systems that require an digital signature to access are far less vulnerable (Welfare, 2019), and remain an extremely efficient way to store and transmit information securely and reliably (Dimitrov, 2019). Moreover, existing financial firms are taking interests in blockchain technology through developing privatised blockchains, which include restricted access rather than proof of work and proof of stake mechanisms. This signifies that they will have control over the transactions (Davidson et al. 2016). In some ways this goes against some of blockchain technology's core ability to provide secure and reliable *peer to peer* transactions.

It is difficult to predict what will come of blockchain technology, but it is certain that it has already shaped the way data storage and transmission are managed.

References

Crosby, M. (2016). BlockChain Technology: Beyond Bitcoin.

Davidson, S., De Filippi, P. and Potts, J. (2016). Economics of Blockchain. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2744751.

Dimitrov, D.V. (2019). Blockchain Applications for Healthcare Data Management. *Healthcare Informatics Research* 51–56. https://doi.org/10.4258/hir.2019.25.1.51.

Duong, T., Fan, L. and Zhou, H.-S. (2016). *2-Hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely*.

Fanning, K. and Centers, D.P. (2016). Blockchain and Its Coming Impact on Financial Services. *Journal of Corporate Accounting & Finance* 53–57. https://doi.org/10.1002/jcaf.22179.

Gheorghiu, V. (2017). Quantum-Proofing the Blockchain.

Jothi, N., Rashid, N.A. and Husain, W. (2015). Data Mining in Healthcare – A Review. *Procedia Computer Science* 306–313. https://doi.org/10.1016/j.procs.2015.12.145.

Küfner, R.A. (2019). *The Byzantine Generals Problem*. *Medium*. Available at: https://medium.com/nakamo-to/the-byzantine-generals-problem-1ae994eaba7e [Accessed: 19 March 2020].

Nakamoto, S. (2019). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Manubot.

Olleros, F. and Zhegu, M. (2016). *Research Handbook on Digital Transformations*. Edward Elgar Publishing.

Pilkington, M. (2015). *Blockchain Technology: Principles and Applications*. Rochester, NY: Social Science Research Network.

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M.F. and Knottenbelt, W.J. (2018). Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. *Royal Society Open Science* https://doi.org/10.1098/rsos.180410.

Swanson, T. (2015) Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.

Welfare, A. (2019). *Commercializing Blockchain*. 1st ed. John Wiley & Sons, Ltd.