Received: 18 February 2019 | Revised: 22 March 2019 | Accepted: 2 April 2019

DOI: 10.1002/itl2.100

WILEY

LETTER

Comparative evaluation of consensus mechanisms in cryptocurrencies

Shihab S. Hazari | **Qusay H. Mahmoud**

Department of Electrical, Computer and Software Engineering, University of Ontario Institute of Technology, Oshawa, Ontario, Canada

Correspondence
Shihab S. Hazari and Qusay H. Mahmoud, Department of Electrical, Computer and Software Engineering, University of Ontario Institute of Technology, Oshawa, Ontario, Canada.
Email: shihab.hazari@uoit.ca (S. S. H.) and qusay.mahmoud@uoit.ca (Q. H. M.)

The Bitcoin cryptocurrency allows entities in a peer-to-peer network to reach consensus about the state of the blockchain through a set of cryptographic algorithms and economic incentives. Bitcoin uses a proof of work system, but there are other consensus mechanisms used by other cryptocurrencies. The performance of a cryptocurrency depends on the consensus mechanism used. This paper presents the results of a comparative evaluation that has been conducted on various significant consensus mechanisms. The unique characteristics, as well as drawbacks of each mechanism, are highlighted, together with their applications. The mechanisms are also classified into major types and those types are evaluated elaborately. The paper concludes with a discussion of the open challenges related to the available solutions.

KEYWORDS
blockchain, consensus, cryptocurrency

1 | INTRODUCTION

The concept of a transaction started in approximately 6000 BC with the barter system when people used to exchange products.[1] However, such a system is impractical since different products have different values. As a medium of exchange, the concept of currency was subsequently introduced in approximately 5000 BC. Initially, currencies were made of gold, brass or silver, which later transformed into paper bills. The invention of currency introduced triple-entry bookkeeping[2] into the transaction system. Here, rather than directly making a transaction, an individual depends on a third party who is responsible for making the transaction, storing the currency and keeping a record of the transaction. This third party later evolved to become a bank or financial institution, bringing centralization to all transactions. In such a case, both parties have to trust the third party to perform the transactions. This can cause a single point of failure and disrupt the security of the transactions.

The issue of centralization (involvement of a fixed third party in every transaction) can be solved by maintaining a peer to peer network[3] among all peers. Here, a two-party can perform a transaction without the inclusion of any third party. However, such a process is not practical for the traditional currency system. As an example, a bank is not only responsible for verifying a transaction but also for storing the currency. This enables individuals to perform digital transactions without the exchange of any fiat currency. Also, without verification, there is always a chance of fraud or double spending. To solve these issues, cryptocurrencies came into play.

A cryptocurrency maintain a distributed public ledger among the users without any central authority. This ledger contains every transaction that occurs in the network. The transaction records the sender and recipient's public keys as their identity and the amount of currency to be transferred. Before performing a transaction, the sender needs to input his/her private key, similar to the basic cryptography protocol. When a transaction is initialized, it is verified by any other peer using the public ledger. After verification, it is broadcast in the network and other peers update their public ledger. Once a transaction is broadcast, it cannot be modified.

Blockchain provides a peer to peer decentralized network that brings cryptocurrency into play. Blockchain contains the fundamentals that cryptocurrencies require to perform and verify transactions. Blockchain can be classified into three main kinds[4]: private, public and federated. Almost all cryptocurrencies use public Blockchain where every node has equal authority. To maintain the consensus among the nodes in a decentralized system, a mechanism is followed by every node in the network. The security and scalability of a cryptocurrency depends on this mechanism.

The contribution of this paper is a comparative evaluation of consensus mechanisms used in 50 of the top cryptocurrencies. To this end, the rest of the paper is organized as follows. In Section 2, the consensus mechanisms are briefly discussed, along with their features, drawbacks and use cases. In Section 3, the evaluation of consensus mechanisms is presented and discussed. Section 4 concludes the paper and offers ideas for future work.

2 | CONSENSUS MECHANISMS

A public Blockchain maintains a decentralized system on a global scale. Here, thousands of peers contribute in order to verify or validate transactions. In such a powerfully changing status of the Blockchain, these openly shared ledgers require an effective, reasonable, ongoing, practical, dependable, and secure instrument to guarantee that every one of the transactions happening on the system is real and that all members concur on the status of the ledger. To ensure all this, it is very important to maintain a consensus mechanism, which is similar to the Byzantine Fault Tolerance (BFT) mechanism.[5] BFT denotes how many failures a system can consider. It allows no restrictions or cannot make any assumption on the decision taken by a single node of the system. A node has the ability to generate distinct data in this type of situation. As Blockchain has no central authority, by using such a mechanism, all or a majority of peers can settle on a decision following certain rules. As a result, all peers can maintain a common public ledger. A decentralization network must maintain the BFT mechanism. Without having that, the node can upload malicious data to the network, which can destroy the reliability of the system. Moreover, there is no central authority which can take over the control of the system to repair the damage. In this section we discuss several consensus mechanisms and present the statistics (Figure 1) of consensus mechanisms utilized in the top 50 cryptocurrencies based to market capitalization as of December 2018.[17,18]

2.1 | Proof of Work

Proof of Work (PoW), the most popular consensus protocol in cryptocurrency, first came into play with the invention of Bitcoin.[6] This consensus mechanism is used to verify and validate a transaction as well as to mine the currency. Besides Bitcoin, several other cryptocurrencies such as Litecoin, Bitcoin Cash, Monero, and Dash use the PoW for consensus. In Bitcoin, in order to perform a Proof of Work, a miner has to create transaction data with one or multiple unconfirmed transactions to create a block. A miner is responsible for verifying and validating transactions. Any peer in the network can be a miner. After creating the transaction data, the miner has to solve a cryptographic puzzle. Here, the puzzle is a hash problem with a given difficulty. This difficulty regulates how much time is required for a miner to solve a block. Along with transaction data, the miner must also take the hash of the previous block as input. In this way, every block is connected to the next block, thus forming a chain. Miners compete with each other with their transaction data to solve the puzzle for a certain block. When a miner finds a solution, s/he broadcasts it to the network and other miners then validate it. Following validation, the block is added to the network and the miner who solved that block is rewarded.

2.2 | Proof of Stake

Proof of Stake (PoS) involves the creation and validation of a new block with no competition among miners. One major difference between PoW and PoS is that in the latter, rather than mining currency, the validator receives only a transaction fee for creating a new block. This means that the amount of total currency in the network always remains fixed. Here, the validator is elected in a pseudo-random way before starting the validation. Only the elected validator can validate a subsequent block. Each time before creating a block, a validator is randomly selected. In order to be elected, the user has to put some of his/her own currency at stake. The user who puts more currency at stake has more chance of being elected. Once elected, a user can create a new block and is rewarded with the amount of currency staked along with the transaction fees. The other users receive back the amount of currency they put at stake. In Nxt, proof of stake is used to create a new block.[7]

However, in Proof of Stake, there is a bottleneck. Wealthy individuals who can put more currency at stake have a better chance of being elected. As a result, it may seem that a comparatively poor user will never be a validator. To solve such an issue, many pseudo-random algorithms have been proposed, among which the most popular are Randomized block selection

and Coin age based selection. In the Randomized block selection method, the algorithm is developed with a combination of the value of the stake and the lowest hash value of a user. Blackcoin uses this method of PoS.[7] In Coin age based selection such as Peercoin,[8] the information used in the algorithm is the amount of the stake plus the amount of time that the currency has been held at stake. The longer the currency has been held at stake, the higher the probability that it will be selected.

2.3 | Proof of Burn

The proof of Burn consensus mechanism was invented by Ian Stewart. This mechanism is used in Slimcoin.[9] Here, miners send some coins to a random invalid unknown address before creating a block. The address changes after every blocks are created. As it is an invalid address, the coin which is sent to that address is unusable or burned. This address is also known as an "eater address." Among the miners, only one is able to create the next block and receive a reward. Here, the reward includes the transaction fees and the mining coin.

The Proof of Burn algorithm inspires the long-term investment. The possibility of receiving a reward is based on the time of investment. Since every transaction in Proof of Burn is recorded, the investor who continuously invests for a long period receives more privileges towards achieving a reward. In spite of having a short-term loss, investors are able to profit through long-term investment. A drawback is as the coin is burned, an investor stands to lose considerable money before being rewarded. The mechanism does not provide any guarantee that, after a certain amount of investment, the investor will have an opportunity to mine the coin. Also, if the number of miners in the network increases, the chance of getting rewarded is diminished.

2.4 | Proof of Capacity

The proof of Capacity algorithm privileges on the capacity of a miner's storage rather than hashing power. The goal of this mechanism is to decrease the usage of computational energy, as is the case in proof of work. Instead of calculating the hash in every block, proof of capacity allows storing the list of possible solutions, even before mining the block. The miner who has more space can store more solutions, which provides the miner an advantage to solve the block. This technology was first introduced in Burstcoin.[10]

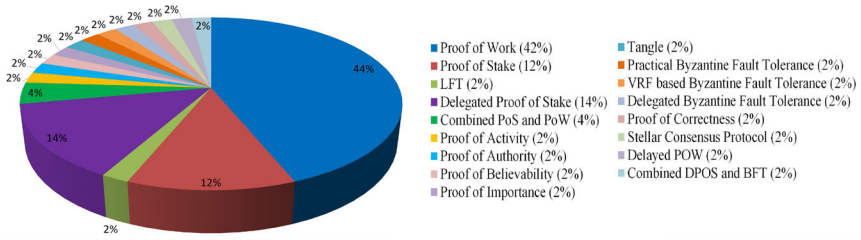
This mechanism contains two steps: plotting the hashes and mining the coins. By continuous hashing of data, using his/her id, the miner plots all possible nonce values that can contain solutions. Here, the Shabal algorithm is used for hashing. After plotting, a miner starts the mining process. During this process, the miner generates a scoop number. With that scoop, the miner calculates the deadline value of every possible nonce s/he plots. Among those deadlines, the lowest deadline is picked up by the miner. A deadline is a threshold value in seconds to counterfeit a certain block. When a miner selects a minimum deadline and no other miner is able to forge the block in the next deadline period, the miner can demand the reward and counterfeit the block. Proof of capacity is scalable and cost-efficient, as miners do not have to compete with each other by using computational power. However, it can lead to a new competition over storage space to plot more nonces.

2.5 | Tangle

Tangle is the consensus protocol used in IOTA.[11] IOTA is a cryptocurrency which is mainly developed to maintain the ecosystem among IoT (Internet of Things) devices. A major difference between Tangle and other consensus protocols is that rather than using a Blockchain network it uses a Directed Acyclic Graph (DAG) to plot the network. DAG is a unidirectional noncyclic graph-structured network that makes it possible to verify multiple transactions by different miners at the same time.

Tangle is a continuously growing ledger, in which unconfirmed transactions are known as tips. An unconfirmed transaction should be verified by at least two transactions or nodes in the network. These two nodes are randomly selected by the Markov Chain Monte Carlo (MCMC) technique. To verify the transaction, a small Proof of Work, such as hashcash, is needed. However, verifying by two nodes is not enough to complete the transaction. The new node also needs to confirm at least two new unconfirmed transactions to complete the original transaction. Therefore, to complete an individual's transaction, a node has to verify other incomplete transactions. This maintains decentralization in the network and every participant makes an almost equal effort to maintain consensus.

Tangle does not require a transaction fee. Since each participant has almost the same contribution based on the transaction amount of individuals, no fees or rewards are required. Also, scalability increases with the network growth. With more participation, more transactions can be verified at the same time. However, the network still requires a significant amount of energy consumption as a small proof of work needs to be conducted in order to verify a transaction.



Proof of Work		Delegated Proof of Stake	Proof of Importance	Practical Byzantine Fault Tolerance
Aeternity	DigiByte	BitShares	NEM	Zilliqa
Augur	Dogecoin	Lisk	**Proof of Stake**	**Delegated Byzantine Fault Tolerance**
Binance Coin	Ethereum	Nano	Cardano	Neo
Bitcoin	Ethereum Classic	Tezos	EOS	**Delayed POW**
Bitcoin Cash	Litecoin	Waves	Holo	Komodo
Bitcoin Diamond	Maker	Tron	OmiseGO	**Combined PoS and PoW**
Bitcoin Gold	Monero	Huobi	Qtum	0x
Bitcoin SV	Ravencoin	**Combined DPOS and BFT**	Steem	HC
Verge	Tether	AOA	**Proof of Correctness**	**VRF based Byzantine Fault Tolerance**
Bytecoin	**LFT**	**Proof of Activity**	XRP	Ontology
Chainlink	ICON	Decred	**Stellar Consensus Protocol**	**Tangle**
Dash	**Proof of Believability**	**Proof of Authority**	Stellar	IOTA
Zcash	IOST	VeChain		

FIGURE 1 Consensus mechanisms of the top 50 cryptocurrencies based on market capitalization (using coinmarketcap.com data as of Dec 2018)

2.6 | Proof of Importance

Proof of Importance (PoI) is an advanced consensus mechanism similar to PoS which was first used in NEM cryptocurrency.[12] To eliminate the drawback of the rich becoming richer, which exists in PoS, the proof of importance mechanism introduces some new regulations, including a score-based protocol known as the proof of importance score. A participant with a higher score has an increased possibility of being selected as a validator. This score is calculated according to three factors: vesting, transaction partner and number and size of transactions in the previous 30 days.

The participant who invests more coins in the network receives a higher PoI score. The number of harvest coins should be at least 10 000. The score also increases with the size and number of transactions. More transactions bring an increased possibility of being a validator. Also, these transactions should be net transfer. If two or more users perform the same transaction among themselves, the PoI score will not change.

2.7 | Practical Byzantine Fault Tolerance

The Practical Byzantine Fault Tolerance (PBFT) is a real- world replication of BFT consensus mechanism. In general practice, in the case of cryptocurrency, a group of individuals is predefined to validate the transactions in a PBFT model.[13] When a new transaction arises, the predefined group receives the transaction and reaches a consensus. Among the nodes, one node is considered as a leader node and other nodes as a backup node. To reach a consensus, the nodes heavily communicate with each other. They also need to verify that no data has been modified during the transmission. In a PBFT model, at least 2/3 of the overall nodes need to reach the consensus to take a decision. It does not matter if 1/3 of the overall nodes are malicious. The transactions are processed in four steps. First, a client requests a transaction to the leader. The leader then broadcast the transaction to the backup nodes. In the third step, the backup nodes verify the transaction and notify the customer. The client waits up to a certain number of same replies. This certain number should be more than the number of malicious nodes which the system can allow. The leader node may change after a certain period and also if the supreme majority numbers of backup nodes decide if the leader is malicious. In Zilliqa cryptocurrency PBFT is implemented.[13] The delegated byzantine fault tolerance (DBFT) is a slightly modified version of PBFT. In Neo, DBFT is used as the consensus mechanism.[12]

2.8 | Other consensus mechanisms

Various other consensus mechanisms are used in different cryptocurrencies. One of the significant mechanisms is proof of correctness which is used in Ripple.[14] Here the servers collect the unconfirmed transactions and make them public as candidate sets. Those candidate sets are voted by all servers based on their veracity. The candidate sets, which exceed a predetermined threshold vote count, will proceed to the next round. The process continues until a set receives at least 80% votes of the servers and then that set is added to the ledger. Proof of authority[15] is used in Ethereum's Kovan Network. It is similar to PoS mechanism. However, the possibility of becoming a validator depends on the reputation of a candidate, not the amount of stake. Proof

TABLE 1 Comparative evaluation of consensus mechanisms

Consensus mechanisms	Proof of Work	Proof of Stake	Hybrid or combined PoW and PoS	Byzantine Fault Tolerance	Tangle
Energy consumption	Wastes considerable energy	Less energy consumption	Uses a significant amount of energy	Less energy consumption	Uses a significant amount of energy
Advanced hardware requirement	Required	Not required	Differs in different mechanisms	Not required	Required, but less than PoW
Centralization	Decentralized	Partially centralized	Partially centralized	Centralized	Decentralized
Double spending attack	Theoretically possible	Difficult	Possible, but less serious than PoW	Not applicable	Difficult
Scalability	Not scalable	Scalable	Partially scalable	Scalable	Scalable
Memory requirement	Significant, due to public ledger	Significant, due to public ledger	Differs in different mechanisms	Less than PoW or PoS	Less than PoW or PoS
Security	Attack is possible with 51% hash power, which is impractical in the real world	Removes 51% attack threat	Removes 51% attack threat	May have a single point of failure	Network can be attacked with 34% hash power

of believability[16] is a consensus mechanism which is used by IOSToken. Here, the validators are selected by their past behavior and contribution record.

3 | EVALUATION OF CONSENSUS MECHANISMS

The verification process, the security of the network, validation time and the cost of processing all depend on the consensus mechanism followed by a cryptocurrency. Comparative evaluation of consensus mechanisms is presented in Table 1. Most of the cryptocurrencies place the greatest emphasis on security and decentralization. As a result, more cryptocurrencies use Proof of Work as a consensus protocol. Because of its validation process, the next most popular consensus mechanism is Proof of Stake.

Based on their techniques and characteristics, different consensus mechanisms can be divided into five major groups: Proof of Work; Proof of Stake; a hybrid or combination of both PoW and PoS; Byzantine Fault Tolerance with different versions; and Tangle. Proof of Work, which is an established decentralized and secure protocol, requires a significant amount of computational energy in order to create a block. Also, all cryptocurrencies that follow PoW algorithm are facing scalability issues. As a solution, PoS came into play with an easier validation process and with lower energy consumption. However, the PoS mechanism faces centralization issues. It is assumed that only a few investors in the future will control the cryptocurrencies under the PoS mechanism. As a result, the hybrid or combined mechanisms of PoW and PoS were created. These hybrid mechanisms differ from one another. The PoW emphasizes the decentralization and security of the network while the PoS emphasizes scalability and energy consumption. Thus, the combined mechanisms consist of both the pros and cons of the PoW and PoS. However, both mechanisms face storage issues since, due to centralization, all peers need to save the continuous public ledger. The Byzantine Fault Tolerance related mechanism solves most of the drawbacks of both the PoS and PoW. However, it is centralized. As a consequence, this mechanism is mostly used in private or permissioned blockchains rather than in a public Blockchain. The major difference between Tangle and other mechanisms is that Tangle does not use a Blockchain network but uses DAG to grow the network. Thus, the validation process in Tangle is different from others.

4 | CONCLUSION AND FUTURE WORK

Consensus mechanisms are designed to prioritize either decentralization or efficiency. It is challenging to reach a decision in a purely distributed system compared to a centralized system, especially when there are no economic incentives. In Blockchain, if decentralization increases, efficiency decreases. If we try to increase efficiency, the network somehow becomes centralized. Although it would appear that DAG solves both scalability and decentralization, it brings a significant security threat.

A comprehensive evaluation reveals that, in spite of scalability and energy consumption issues, PoW is the most popular cryptocurrency mechanism. Cryptocurrencies prioritize decentralization over energy consumption. Hybrid solutions attempt to overcome this issue by maintaining decentralization.

For future work, we plan to evaluate the performance of the various consensus mechanisms and study their impact on the scalability of blockchain systems.

ORCID

Qusay H. Mahmoud https://orcid.org/0000-0003-0472-5757

REFERENCES

1. Flesher DL. Barter bookkeeping: a tenacious system. *Account Hist J*. 1979;*6*(1):83-86. https://doi.org/10.2308/0148-4184.6.1.83.
2. Fraser IAM. Triple-Entry Bookkeeping: A Critique. *Account Bus Res*. 1993;*23*(90):151-158. https://doi.org/10.1080/00014788.1993.9729872.
3. Duke D. The peer-to-peer threat. *Netw Secur*. 2007;*2002*(12):4.
4. Zibin Z, Xie C, Dai H. *An overview of blockchain technology: architecture, consensus, and future trends*. *2017 IEEE International Congress on IEEE Big Data (BigData Congress)*. Honolulu, HI, USA: IEEE; 2017:557-564.
5. Lamport L, Shostak R, Pease M. The byzantine generals problem. *ACM Trans Prog Lang Syst*. 1982;*4*(3):382-401.
6. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten E. *Sok: research perspectives and challenges for bitcoin and cryptocurrencies*. *2015 IEEE Symposium on Security and Privacy*. San Jose, CA, USA: IEEE; 2015:104-121.
7. Nguyen G-T, Kim K. A survey about consensus algorithms used in blockchain. *J Inform Proc Syst*. 2018;*14*(1):101-128.
8. King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, White Paper. Amsterdam, The Netherlands: Stichting Peercoin Foundation; 2012. https://decred.org/research/king2012.pdf. Accessed October 29, 2018.
9. P4Titan. Slimcoin: A peer-to-peer crypto-currency with proof-of-burn. http://www.doc.ic.ac.uk/ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_whitepaper.pdf; 2014. Accessed September 18, 2018.
10. Larsson T, Thorsen R. Cryptocurrency Performance Analysis of Burstcoin Mining. http://urn.kb.se/resolve?urn=urn:nbn:se:hv:diva-12883; 2018. Accessed October 3, 2018.
11. Kusmierz B. *The First Glance at the Simulation of the Tangle: Discrete Model. IOTA Foundation*; 2017. https://assets.ctfassets.net/r1dr6vzfxhev/2ZO5XxwehymSMsgusUE6YG/f15f4571500a64b7741963df5312c7e7/The_First_Glance_of_the_Simulation_Tangle_-_Discrete_Model_v0.1.pdf. Accessed October 18, 2018.
12. Mihaljevic B, Zagar M. *Comparative analysis of blockchain consensus algorithms*. *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Opatija, Croatia: IEEE; 2018:1545-1550.
13. Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery. *ACM Trans Comput Syst*. 2002;*20*(4):398-461.
14. Chase B, MacBrough E. Analysis of the XRP Ledger consensus protocol. *arXiv preprint arXiv:180207242*. 2018. https://arxiv.org/pdf/1802.07242.pdf. Accessed November 20, 2018.
15. Tedeschi P, Piro G, Murillo JAS, et al. Blockchain as a service: securing bartering functionalities in the H2020 symbIoTe framework. *Internet Technology Letter*. 2018;*2*(1):e72.
16. DeLisle B. An Introduction to Iostoken: A Blockchain for the Internet of Services. Cryptoslate; 2018. https://cryptoslate.com/introduction-iostoken-blockchain-internet-services/. Accessed November 11, 2018.
17. Cryptocurrency Market Capitalizations, CoinMarketCap; 2019. https://coinmarketcap.com. Accessed December 02, 2019.
18. Cryptocurrency Charts, Cryptocurrency Charts Live, Cryptocurrency News, Cryptocurrency Charts, Info.binance.com; 2019. https://info.binance.com/en. Accessed December 02, 2019.

How to cite this article: Hazari SS, Mahmoud QH. Comparative evaluation of consensus mechanisms in cryptocurrencies. *Internet Technology Letters*. 2019;2:e100. https://doi.org/10.1002/itl2.100