AN EVALUATION OF BLOCKCHAIN CONSENSUS ALGORITHMS

Dr. Shambhu Bhardwaj*

*Associate Professor,
Department of Computer Science, Faculty of Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: shambhu.bhardwaj@gmail.com

DOI: 10.5958/2249-7137.2021.02626.4

ABSTRACT

Cryptocurrencies have exploded in popularity, and underlying them is an innovative technology known as blockchain: a distributed digital ledger in which bitcoin transactions are recorded once they have been validated. Many clients or "validators" inside the cryptocurrency's peer-to-peer network verify transactions within a ledger using one of many different consensus methods for addressing the issue of dependability in a network containing multiple faulty nodes. The Proof of Work (PoW) and Proof of Stake (PoS) algorithms are the most commonly used consensus algorithms; however, there are additional consensus algorithms that employ alternate PoW and PoS implementations, as well as hybrid implementations and even entirely new consensus methods. We compare and contrast traditional consensus algorithms with some of its contemporaries that are presently in use in contemporary blockchains in this article. Our investigation focuses on the algorithmic steps performed by each consensus algorithm, as well as the algorithm's scalability, the manner by which validators are compensated for their time spent confirming blocks, and the system's security concerns. Finally, we discuss our findings as well as some potential future trends in blockchain consensus algorithms.

KEYWORDS: *Blockchain, Consensus Algorithms, Consensus, Cryptocurrency, Network.*

1. INTRODUCTION

A blockchain is an open, distributed ledger that can efficiently and permanently record transactions between two parties. The most well-known example is Bitcoin, which was developed in 2008 by a person or group operating under the pseudonym "Satoshi Nakamoto"[1]. The aim of the initial Bitcoin whitepaper was to enable the development of a peer-to-peer form of electronic currency, allowing online payments to be transferred directly from one party to another without going through a banking institution. This is accomplished in Bitcoin's implementation by time stamping every transaction on the peer-to-peer (P2P) network and hashing them into a growing chain of transaction blocks[2]. Validators, or "miners," do the hashing. Validators are peers in the network that contribute in the production of new blocks. All transactions inside the chain are trusted as genuine if no one validator or group of validator controls more than 25% of the computer power required to hash these blocks.

Particular the possibility for an infinite number of validators in any given P2P network, consensus methods are required for any collaboration between them. The Proof of Work (PoW) method used by Bitcoin is the most commonly used of these; however, there are a variety of alternative ways for a network to reach agreement, including the algorithms discussed later in this paper.

1.1. The Consensus Problem:

In distributed computing, consensus is a challenge in which nodes within the system must come to an agreement despite the existence of defective processes or misleading nodes[3].

1.1.1. The Byzantine Generals Problem:

The Byzantine Generals Issue is a communication breakdown problem. To put it another way, how can each node (also known as a general) in a system be confident that the data it receives is accurate[4]. The scenario of n Byzantine generals ready to assault a fort is presented in the original problem. Each general has the choice of attacking the fort or retreating; however, all generals must agree on the same plan of action, since a half-hearted assault would be catastrophic. To make things worse, the generals are separated by a great distance and can only communicate via messengers, who may or may not deliver their messages, and some of these generals are traitors who will deliberately try to mislead the others.

1.1.2. Byzantine Fault Tolerance (BFT):

When nodes may produce arbitrary data, Byzantine Fault Tolerance (BFT) is a category of replication algorithms that aims to address the issue of achieving consensus[5]. BFT can ensure a system's safety (the probability that something bad will happen in the system) and liveness (the chance that something good will happen in the system) if no more than $\lfloor (n-1) \div 3 \rfloor$ replicas are defective throughout its lifespan, where n is the total number of replicas in the system. BFT can tolerate up to 33% of nodes that aren't working. In order to guarantee safety and liveness in a system, up to (3f + 1) replicas are often needed, where f is the total number of defective replicas contained inside such system; however, at least one known BFT implementation is able to decrease this to (2f + 1) necessary replicas.

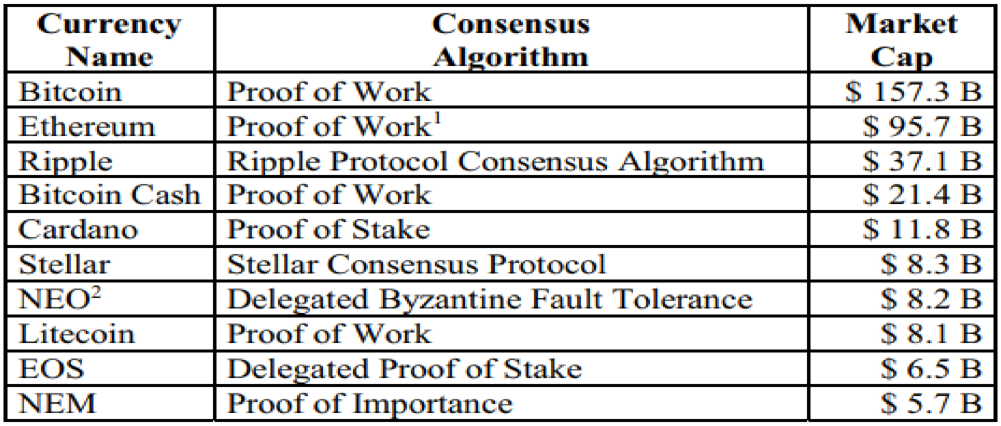
1.1.3. Delegated Byzantine Fault Tolerance (dBFT):

Delegated Byzantine Fault Tolerance (dBFT) is a variation of regular Byzantine Fault Tolerance. This fault tolerance method, described in the NEO whitepaper, divides clients in a P2P system into two categories: bookkeepers and regular nodes[6]. Ordinary nodes do not participate in the consensus process; instead, they vote (thus the name “delegated”) on which bookkeeping node to endorse. The successfully chosen bookkeeper nodes are subsequently included in the consensus process. A random bookkeeper node is chosen at random to broadcast its transaction data to the whole network in this procedure. At least 66 percent of the other bookkeepers believe that the transaction data is correct, and it is permanently committed to the blockchain, and a new cycle of consensus is begun with a bookkeeper chosen at random.

Because there are now over 1,500 active cryptocurrencies that are actively traded on the worldwide market, and because a new coin may be produced at any time, a cryptocurrency's market cap determines its “high-profile” in this context. Despite the fact that crypto currency market prices are always fluctuating, this ranking scheme was found to be the most equitable in sorting the currencies and the algorithms that power them.

1.2. High-Profile Consensus Algorithms:

TABLE 1: TOP TEN CRYPTOCURRENCIES BY MARKET CAP (IN BILLIONS) AS ON 23-09-2018



Currency Name	Consensus Algorithm	Market Cap
Bitcoin	Proof of Work	$ 157.3 B
Ethereum	Proof of Work[1]	$ 95.7 B
Ripple	Ripple Protocol Consensus Algorithm	$ 37.1 B
Bitcoin Cash	Proof of Work	$ 21.4 B
Cardano	Proof of Stake	$ 11.8 B
Stellar	Stellar Consensus Protocol	$ 8.3 B
NEO[2]	Delegated Byzantine Fault Tolerance	$ 8.2 B
Litecoin	Proof of Work	$ 8.1 B
EOS	Delegated Proof of Stake	$ 6.5 B
NEM	Proof of Importance	$ 5.7 B

1.2.1. Proof of Work (PoW):

According to the Bitcoin whitepaper, the PoW method operates by looking for a value that has a hash beginning with a number of zero bits when hashed. This is done by appending a nonce (doing work) to the original value until the resulting hash has the required amount of zero bits. Once this nonce is discovered and the proof of work is fulfilled, the block cannot be altered without repeating all of the work for that block and all subsequent blocks.

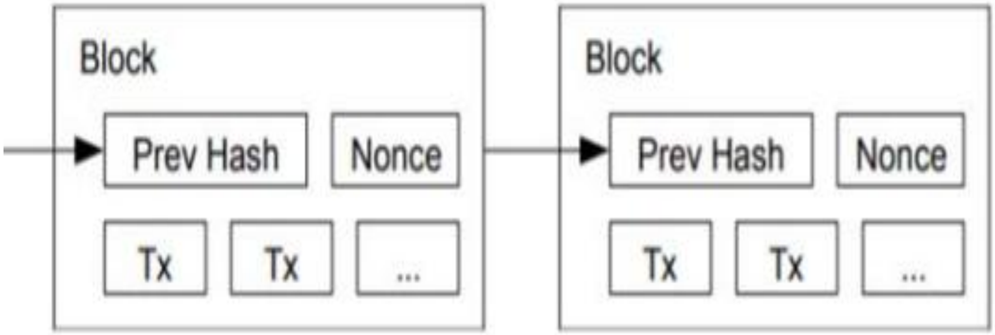


Figure 1. Visualization of two blocks within a PoW Blockchain

With the exception of the initial block produced by the system (the “genesis block”), all blocks contain a hash that consists of the preceding block's hash plus the nonce needed to generate the requisite zero bits, as shown in figure 1. The genesis block is an exception since it has no prior block to reference: its hash is all zeros.

1.2.2. Ripple Protocol Consensus Algorithm (RPCA):

The Ripple Protocol Consensus Algorithm (RPCA), as its name suggests, is a consensus algorithm utilized solely by the Ripple cryptocurrency and was created especially to solve latency problems that other algorithms have. According to the whitepaper, RPCA performs the following functions:

- Prior to a new consensus round, each server collects all valid transactions and places them in a public list known as the “candidate set.”
- Each server compiles all candidate sets discovered on its “Unique Node List,” which is a collection of other Ripple servers to whom the server has access.
- In a sequence of one or more rounds, each server votes on the validity of each transaction.
- In the final round, any transactions that get at least 80% “yes” votes are recorded to the public ledger and the ledger is closed.

1.2.3. Proof of Stake (PoS):

Proof of Stake (PoS) is a hybrid system in which PoW is used for currency minting and PoS is utilized for the majority of network security[7]. The age of each currency is taken into account in a PoS system in the form of “coin-days.” This idea is easily illustrated with an example: ten coins held for ten days equals 100 coin-days. When these coins are used in a transaction, their age is depleted and reset to zero. Unlike in a PoW system, where the chain with the greatest work is considered the main chain, in a PoS system, the chain with the maximum consumed coin age is considered the main chain. A validator pays himself (and therefore consumes his coin age) for the privilege of minting a new block for the network under the PoS method. The system determines the goal amount that a validator must contribute in order to mint a new block under the following conditions:

$\text{proofhash} < \text{coins} \times \text{age} \times \text{target}$

1.2.4. Stellar Consensus Protocol (SCP):

The Stellar Consensus System (SCP) is a decentralized consensus protocol in which nodes in the network do not have to trust the whole network but may select which nodes to believe. The notion of a “quorum slice,” which was originally established by this protocol, refers to a collection of nodes that trust each other[8]. A quorum slice is a subset of a quorum that convinces one specific node of agreement, while a quorum is a collection of nodes sufficient to achieve an agreement. SCP begins with a “nomination procedure,” in which fresh, candidate values are proposed for agreement. Each node that gets these values will vote for one of these values, resulting in one value receiving the majority vote. The “ballot protocol” is deployed once the nomination procedure has been properly completed. During this phase, nodes begin voting on whether or not to commit or cancel the values chosen in the previous phase. If a group of nodes cannot come to an agreement, the value is transferred to a higher-valued ballot and voted on again.

1.2.5. Delegated Proof of Stake (dPOS):

Stakeholders choose to elect any number of witnesses to produce blocks in a Delegated Proof of Stake (dPOS) system[9]. The roster of witnesses is shuffled at each maintenance interval, and each witness is given a chance to produce a block at a set rate of one block every n seconds, where n is determined by the implementation. Witnesses are compensated for each block produced; but, if they fail to produce a block after being elected, they may be voted out in subsequent elections. Blocks are generated every three seconds by authorized producers on the EOS blockchain, and the list of those producers is randomized every 21 blocks. If a producer has not generated a block in the last 24 hours, they are removed from consideration until they inform the blockchain of their desire to resume block production.

2. LITERATURE REVIEW

Traditional consensus algorithms are compared and contrasted by Bach et al. with some of their contemporaries now in use in modern blockchains [10]. Their research focuses on each consensus algorithm's algorithmic processes, the system's scalability, how validators are rewarded for their time spent confirming blocks, and the algorithm's security issues. Finally, they explain their results as well as possible prospective blockchain consensus algorithm tendencies.

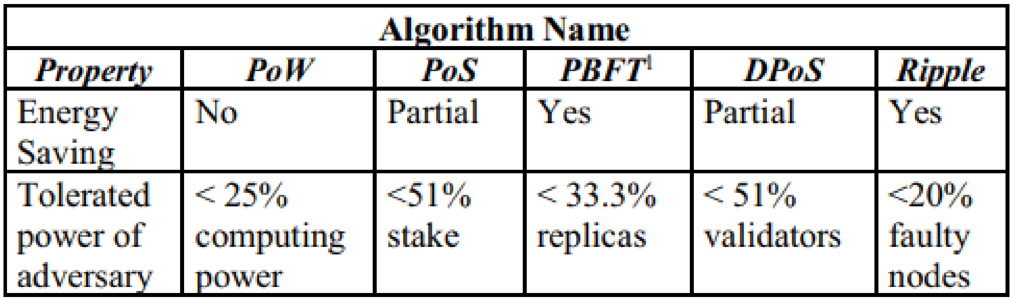
Nguyen et al. provide an overview of Blockchain consensus methods that have been investigated and are currently being utilized in a variety of well-known applications [3]. According to them, the problem of transforming a low-trust centralized ledger maintained by a single third-party to a high-trust decentralized ledger held by multiple organizations, or verifying nodes, has been solved by Blockchain. A major addition to Blockchain's work is the consensus mechanism, which defines how all nodes in the validating network agree to add a new block. There are two types of blockchain algorithms. The first is proof-based consensus, in which nodes joining the verifying network must show that they are better prepared to do the adding task than the others. Voting-based consensus is the second kind of consensus, which requires network nodes to exchange their results of verifying a new block or transaction before making a final decision.

3. DISCUSSION

3.1. Comparisons:

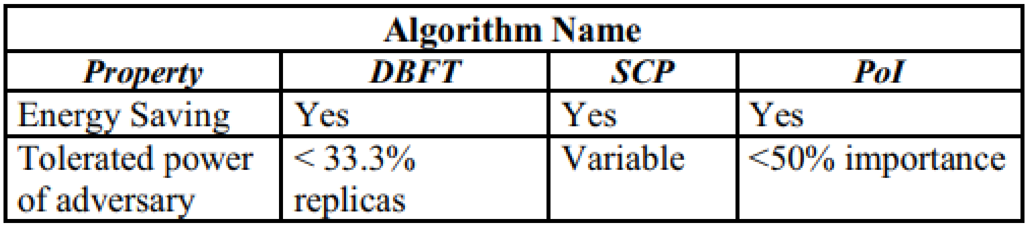
According to Zheng et al., Table 2 provides a simple comparison of different methods [11]. Because it is difficult to offer exact figures regarding how much energy each implementation uses owing to complicating variables such as processor efficiency and type, energy saving is only provided a general yes-no-partial answer. Table 3 provides information about algorithms that the authors did not include in their work.

TABLE 2: CONSENSUS ALGORITHM CHARACTERISTICS: PART I



	Algorithm Name				
Property	***PoW***	***PoS***	***PBFT***[1]	***DPoS***	***Ripple***
Energy Saving	No	Partial	Yes	Partial	Yes
Tolerated power of adversary	< 25% computing power	<51% stake	< 33.3% replicas	< 51% validators	<20% faulty nodes

TABLE 3: CONSENSUS ALGORITHM CHARACTERISTICS: PART II



	Algorithm Name		
Property	***DBFT***	***SCP***	***PoI***
Energy Saving	Yes	Yes	Yes
Tolerated power of adversary	< 33.3% replicas	Variable	<50% importance

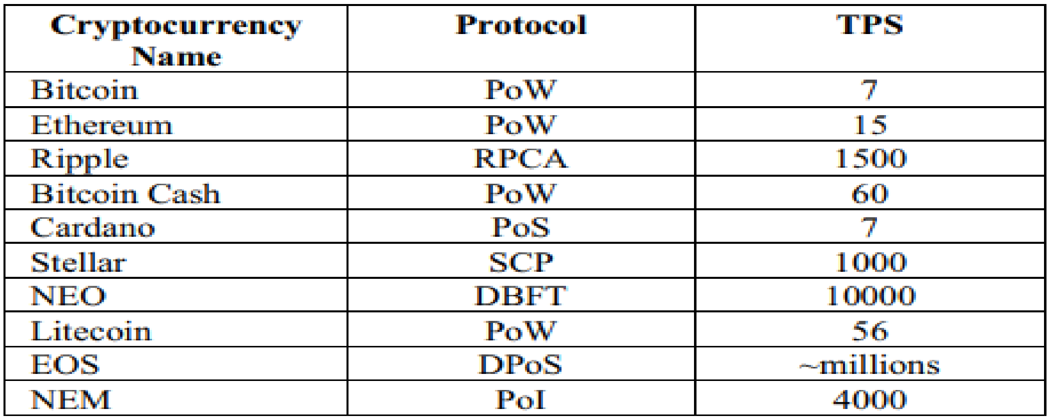
3.1.1. Security:

Tolerated adversary power is defined in Tables 2 and Table 3 as the amount of control an attacker must have over the network in order to effectively attack it. For example, in order to fabricate transactions using the PoW method, an attacker would need to possess at least 25% of the processing power in the system. To fabricate transactions using the PoS algorithm, an attacker would need to possess at least 51 percent of the network's stake. When it comes to attacker potential, the Stellar Consensus Protocol is an anomaly. Because of SCP's usage of quorum slices, a client may select which other clients it trusts. This implies that an attacker might theoretically gain control of a significant part of the network but still be unable to alter the blockchain inside a limited number of trusted groups. On the other hand, rather than the whole quorum, an attacker may influence the quorum slices inside the network. In any of these hypothetical situations, there is no simple answer.

3.1.2. Scalability:

The theoretical maximum number of transactions per second (TPS) that a cryptocurrency can achieve is listed in this section. As shown in Table 4, while the algorithm that underlies a cryptocurrency ultimately dictates the maximum TPS that can be achieved, there is still some variance between networks that use the same protocol.

TABLE 4: TRANSACTIONS PER SECOND FOR SELECTED CRYPTOCURRENCIES



Cryptocurrency Name	Protocol	TPS
Bitcoin	PoW	7
Ethereum	PoW	15
Ripple	RPCA	1500
Bitcoin Cash	PoW	60
Cardano	PoS	7
Stellar	SCP	1000
NEO	DBFT	10000
Litecoin	PoW	56
EOS	DPoS	~millions
NEM	PoI	4000

3.2. Limitations:

The difficulty in obtaining correct transaction per second statistics for each blockchain network, as well as energy consumption estimates for the less popular blockchains, are the most apparent drawbacks of this study (i.e. not Bitcoin or Ethereum). TPS statistics were often derived from third-party sites covering the subject, or, in the case of the NEM network, from marketing materials. These figures are not entirely reliable and should only be used to get a sense of what a network may be capable of in theory.

4. CONCLUSION

The Proof of Work method, which is by far the most common consensus algorithm in use across cryptocurrencies, will ultimately be replaced by newer, more efficient algorithms, according to the early results in this paper. The Ethereum network, which has been preparing a transition to Proof of Stake for at least the past year, is the most visible example of this. If Ethereum completes its shift to a PoS system, an in-depth comparison of the new system to the existing one would be an excellent starting point for future study. If the transfer fails, a more in-depth examination of RPCA and SCP may be undertaken, since both protocols seek to provide a worldwide network.

REFERENCES

1. P. K. Kaushal, A. Bagga, and R. Sobti, “Evolution of bitcoin and security risk in bitcoin wallets,” 2017, doi: 10.1109/COMPTELIX.2017.8003959.
2. P. Waelbroeck, “An Economic Analysis of Blockchains,” CESifo Work. Pap. Ser., 2018.
3. G. T. Nguyen and K. Kim, “A survey about consensus algorithms used in Blockchain,” J. Inf. Process. Syst., 2018, doi: 10.3745/JIPS.01.0024.
4. J. Wang, “A simple Byzantine Generals protocol,” J. Comb. Optim., 2014, doi: 10.1007/s10878-012-9534-3.
5. T. Distler, C. Cachin, and R. Kapitza, “Resource-Efficient Byzantine Fault Tolerance,” IEEE Trans. Comput., 2016, doi: 10.1109/TC.2015.2495213.
6. Y. Hu, Y. Xiong, W. Huang, and X. Bao, “KeyChain: Blockchain-based key distribution,” 2018, doi: 10.1109/BIGCOM.2018.00027.
7. N. Houy, “’It will cost you nothing to ‘kill’ a proof-of-stake crypto-currency,” Econ. Bull., 2014, doi: 10.2139/ssrn.2393940.
8. D. Mazieres, “The Stellar consensus protocol: A federated model for Internet-level consensus. url:https://www.stellar.org/papers/stellar-consensusprotocol.pdf,” Stellar Dev. Found., 2016.
9. X. Fan and Q. Chai, “Roll-DPos: A randomized delegated proof of stake scheme for scalable blockchain-based Internet of Things systems,” 2018, doi: 10.1145/3286978.3287023.
10. L. M. Bach, B. Mihaljevic, and M. Zagar, “Comparative analysis of blockchain consensus algorithms,” 2018, doi: 10.23919/MIPRO.2018.8400278.
11. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” 2017, doi: 10.1109/BigDataCongress.2017.85.