Paper ID: 211

A Review of Blockchain Consensus Mechanisms: State of the Art and Performance Measures

Thanushya Thanujan#, R. A. C. P. Rajapakse, and Dilani Wickramaarachchi

Department of Industrial Management, Faculty of Science, University of Kelaniya, Sri Lanka.

#thanushyal@esn.ac.lk

Abstract: Blockchain is an emerging digital technology for creating decentralized systems which disrupts the digital world with its complex and robust architecture. It has a range of application domains; from cryptocurrencies to decentralized software applications which are commonly known as DApps. The consensus mechanism is the core of Blockchain technology. Reaching a common agreement among the nodes of a decentralized distributed network is a vital but challenging process in consensus mechanisms. Consensus mechanism enables adding a new block to the blockchain making it transparent, trustworthy and immutable. This paper presents a systematic review of existing mainstream consensus mechanisms to highlight their strengths, impulsions and limitations, and the evolution of consensus mechanisms. On the basis of their canonical properties, each consensus mechanism is having its own performance characteristics. The performance of a consensus mechanism is determined in various criteria such as throughput, mining power, energy consumption, fault tolerance, and more. However, there is no fixed common scale yet to measure the performance. At present a particular consensus mechanism is adopted by an application domain purely based on subjective criteria including trial and error. Therefore selecting the most appropriate consensus mechanism in a particular application domain requires a systematic set of guidelines to be developed. By exploring the existing literature on various consensus mechanisms and their performance characteristics, this paper facilitates the researchers to identify the most appropriate consensus mechanism for a given application domain.

Key Words: blockchain, consensus mechanisms, decentralized applications, DApps.

Introduction

The blockchain technology has developed substantially since its first notable application in 2008 which is widely known as bitcoin (Nakamoto, 2009). After invention of Bitcoin the evolution of blockchain could be divided into three main phases.

Phase one (2008 - 2013) describes the transactions of bitcoins, phase two (2013-2015) the smart contracts implemented on Ethereum(Buterin,2014) platform and, phase three (Since 2015) the development of Decentralized Applications using smart contracts which are known as DApps (Cai et al., 2018). As these applications grow with complexity there is a growing demand to attain agreement between distributed network nodes in order to make the corresponding blockchain transparent, trustworthy and immutable. Therefore consensus mechanisms are considered as one of the most vital elements in blockchain based systems.

In literature numerous consensus mechanisms have been proposed such as Proof of Work(PoW), Delayed Proof-of-Work(DPoW), Prime Number Proof of Work (Prime Number PoW), Proof of Stake (PoS),

Delegated Proof of Stake (DPoS), Leased Proof of Stake (LPoS), Proof of Stake Velocity (PoSV), Proof of Burn (PoB), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance(PBFT), Delegated Byzantine Fault Tolerance(DBFT), Federated Byzantine Agreement(FBA), Raft and a few more. Among them Proof of Work (PoW) ultimately has become the widely-used consensus mechanism in these days, mainly since it has been used in the bitcoin system. The core objective of all consensus mechanisms are same but in terms of implementation and performance characteristics, there are quite a lot of differences.

Apparently, meticulous security and performance analysis of most of the consensus protocols are still not published in top venues. However, the challenge of choosing the most appropriate consensus mechanism has surged in the Decentralized Applications (DApps) era of the blockchain technology. Moreover, since research on the consensus mechanisms is still not very much matured, clear guidance for the selection of an appropriate consensus mechanism has not been made available. Determining and analysing the potentiality of the mainstream consensus mechanisms will help the researchers to select the most appropriate consensus mechanism for their Decentralized Applications (DApps).

In this research work, a background study of the blockchain technology was conducted with special attention to various consensus mechanisms. With the aforementioned objective in mind, prevailing mainstream consensus mechanisms were analysed in terms of their strengths and weaknesses in different performance attributes as a systematic review. Accordingly, information has been reorganized to guide selecting a problem specific, consensus mechanism based on the expected outcome.

The rest of the paper is organized as follows. In the section- II, a background study is presented with the evolution of blockchain technology. A review of existing literature on consensus mechanisms is presented in section III, followed by a discussion in section IV on the similar work published already with comparisons of existing consensus mechanisms and the outcome of this study is presented. Finally, section V discusses the result and limitations of this study and section VI concluding the remarks.

Background Study

The blockchain architecture has been evolving over the past couple of decades in terms of application and performance characteristics. Particularly with the futuristic conceptualization of DApps, the architecture of blockchain has drastically changed and the role of the underlying consensus mechanism has become highly variant but important. Hence, it is important to understand the evolution of the blockchain architecture prior to any discussion on the role of consensus mechanisms.

A. Evolution of Blockchain Technology

1) Blockchain 1.0 (Bitcoin): Bitcoin is considered as the first decentralized digital cryptocurrency and it was the first application of blockchain technology. Apart from conventional currencies and other digital currencies, bitcoin is distinguishable based on some key features (CoinDesk, 2020) such as, decentralization of transactions (transactions maintained by peer to peer network), limited supply (total number of bitcoin limited to 21 million), pseudonymity (transactions are secured with public/private key addresses instead of personal identity) and immutability (validated transactions cannot be revoked). Central to the bitcoin system was a consensus mechanism called Proof of Work (PoW), which was the core technology used to ensure the transparency, immutability and

security of transactions being recorded in a chain of blocks. The Proof of Work (PoW) consensus mechanism generates and validates a new immutable block to the existing chain of blocks by solving a complex puzzle.

2) Blockchain 2.0 (Ethereum): Ethereum is an open source decentralized blockchain based platform proposed by Vitalik Buterin in 2013. His white paper (Buterin,2014) – "A Next Generation Smart Contract & Decentralized Applications Platform" - was published and documented in late 2013. Even though ethereum is also another cryptocurrency, the blockchain architecture behind ethereum was recognized for its ability to facilitate smart contracts, which are software-based functionalities that go beyond transactions in bitcoin system. The concept of smart contracts, in other words, has made ethereum a software architecture that could be used to create transparent, decentralized and fault tolerant software applications. Proof of Work (PoW) and Proof of Stake (PoS) are the most used consensus mechanisms in Ethereum. Proof of Work (PoW), similar to bitcoin, was the very first consensus protocol used in ethereum. However, it was seen later some attempts to shift to a different consensus mechanism called Proof of Stake (PoS). While Proof of Work (PoW) required solving a complex mathematical puzzle to generate and validate a new block, which consumed much computational energy, the Proof of Stake (PoS) consensus mechanism facilitated the creation of a new block by staking the wealth of the generating node.

3) Blockchain 3.0 (The Future): With promising success of smart contract based applications, blockchain has thrived across many industries. Going beyond cryptocurrency and smart contracts, the next generation of blockchain technology tries to resolve the contemporary problems such as scalability, security, privacy and transparency which are found in various industries through an improved version of decentralized applications called DApps. Blockchain 3.0 could be considered as an improved version of blockchain 2.0 (Ethereum) and the DApps could be considered as its core.

B. The Blockchain Architecture

Blockchain architecture reveals all the substantive technical aspects behind blockchain. In blockchain the collection of transactions or digital information are recorded in chronological order in a block, which is linked with other similar blocks as a chain and secured using cryptography. SHA-256 cryptographic hashing algorithm is used to create a hash value for a block at the moment that particular block is generated. Each block in a blockchain has the hash value of the previous block in a way the blocks are linked and form as a chain. Each block is referencing to only one parent, but until the fork situation is resolved, it might have more than one child temporarily. A block can be identified in a blockchain by its cryptographic hash and block height. The very first block in the blockchain is known as the genesis block.

Structure of a block – Block is a data structure, which bundles the transactions and broadcast to all the nodes in the distributed decentralized network. A block contains a block header along with recorded transactions. Block header is a Metadata which helps to verify and validate the block.

The block header is made up with three sets of Metadata (Antonopoulos et al., 2017). First, previous block hash, which is 32 bytes in size, and it refers to the previous block or parents hash in the chain. Second is a set of Metadata, each with size of 4 bytes, namely 1). Difficulty target, which is a parameter defined by a hash below a given target, 2). Timestamp, which is the creation time of a

particular block and 3). Nonce, which is "number only used once" added with hash to meet the difficulty. Third, the merkle root, which is a 32 bytes size binary hash tree that summarizes all the recorded transactions in a particular block.

Once the transaction is initiated, it is stored in the transaction pool until it become confirmed. Minors, who attempt to create new blocks by solving the mathematical puzzle, on the network choose transactions from the transaction pool and form them into a new block, which they just mined. The validity of a new block added to the blockchain comes from a process known as consensus. In other words, a new block is chained with the blockchain only if it got the consensus of the majority of nodes attached to the respective blockchain network. Once a block is validated and added to the chain it turned to be immutable

The consensus mechanism plays a critical role in a blockchain. The traditional consensus mechanisms suffer from the drawback called 51% attack, which means the possibility of accepting a false block with majority's consensus fraudulently. Therefore, different other consensus mechanisms have been developed, particularly with the advent of smart contracts and decentralized applications, for different classes of problems. Moreover, the nature of distributed applications demands the elimination of the role of miner in the bitcoin architecture and the alternative approaches are sought after as a result.

Consensus Mechanism

A consensus mechanism is a fault-tolerant mechanism which is used to reach a common legitimate agreement between nodes in a peer-to-peer, network-based distributed decentralized system such as blockchain. For example, having a consensus mechanism enables to overcome the issue of double spending in bitcoin transactions, which means making two payments using the same digital currency.

In literature, a notable study on the evolution of consensus mechanism/s has been presented by Leila Ismail et al. They have analyzed and provided a temporal evolution of the blockchain consensus protocols, classifying them into three main categories (Ismail et al., 2019) namely 1) compute-intensive based consensus protocols (insist massive computational power based consensus mechanisms), 2) capability based consensus protocols (potency based consensus mechanisms) and 3). Voting based consensus protocols.

Compute-intensive based consensus protocols are rivalling-based protocols that consume more energy, insist exorbitant cost for resources and contamination of environment, which are seen as its principal drawbacks (Monrat et al., 2019). Capability-based consensus mechanisms diminish the energy consumption problem, though it also has notable obstacles. It depends on capability, which indicates some possession of wealth, and hence is biased to rich and also may provide a chance to nasty attackers. Voting-based consensus protocols address the issues of high energy consumption in competitive based approach and avoid wealth dominance from capability based protocols by introducing a voting mechanism to attain a consensus.

A. Proof of Work (PoW)

The concept of Proof of Work (PoW) was introduced in 1993 by Cynthia Dward and Moni Naor, when they published a science paper "Memory-Bound Functions for Fighting Spam". Later in 1999, Markus Jakobsson and Ari Juels introduced the term "Proof of Work" in their paper "Proofs of work and bread pudding protocols". After invention of bitcoin, Satoshi Nakamoto developed the PoW mechanism to confirm

transactions and add/mine new blocks to the bitcoin blockchain.

As described before, in this mechanism, to add a new block into existing chain minors are required to solve a complex puzzle (work) based on a cryptographic hash algorithm. The use of the SHA-256 algorithm expects minors guess a random number (nonce) and find the solution by using SHA256 function twice which is less than difficulty. This acts as a proof of the work done by the miner. The difficulty of the puzzle increases when the number of participants (minors) increase. After, validated all the transactions in the new block then the new block is then added to the blockchain. The person (node) who found the solution as soon as possible will be rewarded with bitcoin.

The detraction of Proof-of-Work are the threats of a 51% attack - malicious miners can seize 51% of the computing power of a network, gain so-called "domination" and get chance to won the chance , time consuming - solution comes in random selection of nonce which is time consuming process and resource consumption - to find the solution more computational power is needed

B. Proof of Stake (PoS)

In 2012, Sunny King and Scott Nadal introduced the concept of Proof of Stake (PoS) as a solution to “Bitcoin mining’s high energy consumption”. Sunny King introduced Peercoin as the first cryptocurrency to implement Proof of Stake in 2013(Cointelegraph, 2017). After the invention of ethereum, the ethereum developers were trying on the transition from Proof of Work to Proof of Stake through the Casper- test net version protocol. Casper was later upgraded into two - Casper FFG: (The Friendly Finality Gadget) and Casper CBC (The Friendly GHOST/Correct-by-Construction). Founder of ethereum explained both as - “The main trade-off between FFG and CBC is that CBC seems to have nicer theoretical properties, but FFG seems to be easier to implement” (Antonopoulos et al., 2018).

Proof of Stake (PoS) protocol is developed as an alternative to the Proof of Work (PoW). In this mechanism, instead of minors, the participants are validators. Validators are chosen the next block by stake their tokens rather than mining. Those who stake large amount will get high chance to create next block. Since the validator no need to do mining hence Proof-of-Stake consume standard energy and became environmentally-friendly protocol which is alternative to Proof-of-Work.

The two main variants of Proof of Stake (PoS) mechanisms are Leased Proof of Stake (LPoS) and the Delegated Proof of Stake (DPoS) mechanisms. The flaws of Proof of Stake (PoS) are “Nothing at stake” problem (when validators try to create all possible forks) and “long-range attacks - The attacker tries to modify the history of the blockchain by creating a fork from the block already created” (Li et al., 2017).

C. Leaseded Proof of Stake (LPoS)

In 2017, Leased Proof of Stake (LPoS) is launched by Waves. In this mechanism, any nodes can lease their balances to staking nodes to make “richer gets richer” and will be rewarded with a percentage of the payout. Leased tokens remain in the full control of the leasing node and leases can be canceled at any time.

D. Delegated Proof of Stake (DPoS)

This method is introduced by Daniel Larimer in 2014 to overcome wealth dominance. Delegated Proof of Stake (DPoS) is similar to Proof of Stake (PoS).This mechanism works under voting and election process in an attempt to validating the blocks. Rather than staking or competing, nodes are work together to build and validate a new block.

Since limited number of participants are participating, this can potentially lead to 51% attack.

E. Proof of Burn (PoB)

Proof of Burn (PoB) was proposed by Ian Stewart in 2014 as an alternative consensus mechanism to overcome the problem of excessive energy consumption in Proof of Work (PoW). In this mechanism minors instead of wasting resources, burns their coins for minig and validation process. Once the miner burns the coins to the unspendable address which is called an eater address then it cannot be recovered. This intimidates the malicious nodes in the network who try to work on an invalid block. The drawback of this consensus is the rich becoming richer.

F. Proof of Elapsed Time (PoET)

In 2016, Intel invented the Proof of Elapsed Time (PoET) consensus protocol. In this mechanism, minors will be selected based on time. Each verification node sleeps after creation of a random wait time and the node completes the waiting time first receives a chance to propose the next block. Having to depend on Intel is the major drawback of this consensus mechanism.

G. Practical Byzantine Fault Tolerance (PBFT)

In 1999 Barbara Liskov and Miguel Castro introduced Practical Byzantine Fault Tolerance (PBFT) used to solve the Byzantine General problem (Castro et al., 1999). Among nodes in the network one node selected as a leader and rest of them are backup nodes. Once the leader node receive the transaction request, the transactions are bundled into block and the block is broadcast to the backup nodes for verification. If the majority or the 2/3 of the network found exact same hash then the new block is added to the existing chain. In this consensus transaction will be approved even if some nodes are malicious (not exceed ⅓ of the overall nodes). When the number of nodes in the network increases, the system became more secure and efficient. The major threat found in this mechanism is the Sybil attack (Swathi et al., 2019).

H. Delegated Byzantine Fault Tolerance (DBFT)

Neo developed Delegated Byzantine Fault Tolerance (DBFT) in 2014 as a modified version of Practical Byzantine Fault Tolerance (PBFT), which differs only in terms of the mechanism to select the leader. Leader is selected through a voting process. In this mechanism some nodes in the network has the potential to record and verify transactions. It may create multiple malicious replica nodes. In this situation, Sybil attack may occur.

I. Hybrid Consensus Mechanisms

There is no such thing as “one consensus fits all”. Because each application domain may differ in term of subjective. Despite single consensus mechanisms in the literature, hybrid type blockchain consensus mechanisms have been proposed to obtain efficient expected output while maintaining the decentralization such as Proof of Authority (PoAuthority), Proof of Weight (PoW), Proof of Activity (PoA), Delayed Proof-of-Work(DPoW), Delegated Proof of Stake (DPoS), Proof of Space (PoSpace) and few more. The objective of the hybrid consensus mechanism is to adopt the benefits of the respective consensus and aims to mitigate each other’s weaknesses.

**Table I illustrate the evolution of consensus mechanisms. It elaborates corresponding consensus for each classification, whether it is hybrid type or not and current usages.

Table 1: Evolution of Consensus

Evolution Type		Basis	Consensus algorithms	Hybrid	Used by
Compute-Intensive based consensus protocols		Huge computational power	Proof of Work(PoW-1993)	No	Bitcoin, Ethereum, Litecoin, Dogecoin
			Delayed Proof-of-Work(DPoW)	Yes (PoW-PoS)	Komodo
			Prime Number Proof of Work (Prime Number PoW-2013)	No	Primecoin
Capability-Based Consensus Protocols		Wealth dominance	Proof of Stake(PoS-2012)	No	Ethereum (soon), Peercoin, Nxt.
			Delegated Proof of Stake (DPoS-2014)	Yes (PoS-BFT)	Bitshares, Nano, Cardano
			Leased Proof of Stake (LPoS-2017)	No	Waves.
			Proof of Stake Velocity (PoSV-2014)	Unknown	Reddcoin
			Proof of Burn (PoB-2014)	Unknown	Slimcoin
			Proof of Space (PoSpace) / Proof of Capacity (PoC)(2015)	Yes (PoW-PoS)	Spacecoin, Chia, Burstcoin
			Proof of History (PoH-2017)	Unknown	Solana
			Proof of Importance (PoI-2018)	Unknown	NEM
			Proof of Believability (PoBelievability-2017)	Yes	IOST
			Proof of Authority (PoAuthority-2017)	Yes (PoS-BFT)	Gochain, Menlo one
			Proof of Elapsed Time (PoET-2016)	No	HyperLedger
			Proof of Weight (PoW)	Yes (PoS-BFT)	Algorand
			Proof of Activity (PoA)	Yes (PoW-PoS)	Decred
Voting-Based Consensus Protocols	Byzantine Fault Tolerance (BFT)-based protocols	Voting system	Practical Byzantine Fault Tolerance(PBFT-1999)	Unknown	Hyperledger Fabric, Hyperledger Iroha, Oracle, Hydrachain, BigchainDB
			Delegated Byzantine Fault Tolerance(DBFT-2014)	Unknown	NEO
			Federated Byzantine Agreement(FBA-2018)	Unknown	Ripple, Stellar
			Combined Delegated Proof of Stake and Byzantine Fault Tolerance (DPoS+BFT-2018)	Yes (DPoS-BFT)	
	Crash Fault Tolerance (CFT)-based protocols		Raft (2014)	Unknown	Quorum
			Federated CFT-based consensus(2014)	Unknown	

Choosing a precise consensus mechanism is mandatory to consolidate Decentralized Applications. Selection of an appropriate consensus mechanism depends on several factors such as prevention of double spending, hash power, scalability, throughput, latency, energy efficiency, transaction verification, .etc.

- Double spending problem – Spending the same cryptocurrency more than once when doing digital transactions.

- Hash power – It is also called as Hash rate. It depends on the speed of the mining device. Its influences reveal, when a minor tries to compete to win a reward within a short period of time by solving a puzzle in order to try to add a new block to the existing chain.
- Scalability – Scalability depends on many factors. It influences directly to the throughput of the network and indirectly to the block size, response time and transaction fees.
- Throughput – Denotes the number successful transactions per second. It depends on block size, verification time, Block creation/ latency.
- Latency – It refers to the time interval between the transactions that are confirmed and deployed.
- Energy efficiency – It is used to determine which consensus algorithm uses how much energy from the resources.
- Transaction verification – It denotes the time a successful transaction takes for verification.

Previous Surveys and Analysis of Consensus Algorithms

When looking at the existing literature, there are quite a few surveys and comparative analysis of various blockchain consensus mechanisms could be identified. For example, (Nguyen et al., 2018) has reviewed the popular consensus mechanisms and grouped them into two major categories namely, proof-based consensus and voting-based consensus and, has presented a comparison between PoW, PoS and their hybrid forms. (Yadav et al., 2020) also have presented a comparative analysis. They have compared the consensus mechanisms based on the notion of permissioned networks and permission less networks. In another comparative evaluation of consensus mechanisms done by (Hazari et al., 2019), it has revealed that the PoW is the most widely used consensus algorithm in cryptocurrencies and the advancement of decentralization and scalability of the network is opposite to each other. Direct Acyclic Graph (DAG) resolves this issue, even though some security issues still exist.

(Cao et al,2020), have analyzed and compared PoW, PoS and DAG based blockchain in terms of the average time to generate a new block, the confirmation delay, the TPS and the confirmation failure probability. In (Ni et al., 2018), the authors have identified the gaps by mapping the security and performance characteristics of the consensus mechanisms and the challenges of integrating blockchain-based IoT (Internet of Things) applications. In their research, PoW, PoS, PBFT, PoET, DBT, Tendermint and IOTA protocols have been compared to verify which factors suit to merge with IoT systems. In (Mahood et al., 2020), the authors have identified the parameters such as blockchain type, transaction rate, scalability, adversary tolerance model, experimental setup, latency, throughput, bandwidth, communication model, communication complexity, attacks, energy consumption, mining, consensus category, and consensus finality to compare the blockchain consensus algorithms. In (Alsunaidi et al., 2019) authors have figured out the factors that affect the performance and security of the blockchain consensus algorithms.

Similar work has been done in (Bakmanet al., 2020), state-of-the-art blockchain consensus algorithms and pros and cons of each consensus mechanisms have been reviewed. They have also proposed an analytic framework that consists of four different criteria to evaluate the consensus algorithms' performance including their throughput, the profitability of mining,

degree of decentralization and algorithms' securities and vulnerabilities.

There are a few more recent comparative studies published with similar results. Table II depicts a summary of existing comparative studies in terms of security and performance.

Table 2: Comparisons of existing studies

Factors / Consensus	Prevent Double Spending	Hash Power	Scalability	High Throughput	High Latency	Energy Efficient	Fast Transaction Verification
Proof of Work (PoW)	[(Ni et al., 2018), (Hazari et al., 2019)]	[(Bakmanet al., 2020)]			[(Bakmanet al., 2020)]		
Proof of Stake (PoS)	[(Ni et al., 2018), (Hazari et al., 2019)]		[(Hazari et al., 2019)]	[(Bakmanet al., 2020)]		[(Ni et al., 2018), (Hazari et al., 2019), (Yadav et al., 2020), (Cao et al., 2020)]	[(Bakmanet al., 2020)]
Delegated Proof of Stake (DPoS)	[(Bakmanet al., 2020)]		[(Hazari et al., 2019), (Bach et al., 2018), (Bakmanet al., 2020)]	(Bach et al., 2018)]			
Proof of Elapsed Time (PoET)	[(Ni et al., 2018)]			[(Bakmanet al., 2020), (Nguyen et al., 2018)]		[(Ni et al., 2018), (Yadav et al., 2020)]	[(Bakmanet al., 2020), (Nguyen et al., 2018)]
Practical Byzantine Fault Tolerance (PBFT)	[(Ni et al., 2018), (Bach et al., 2018)]			[(Ni et al., 2018), (Bakmanet al., 2020)]		[(Ni et al., 2018), (Bakmanet al., 2020)]	[(Bakmanet al., 2020)]

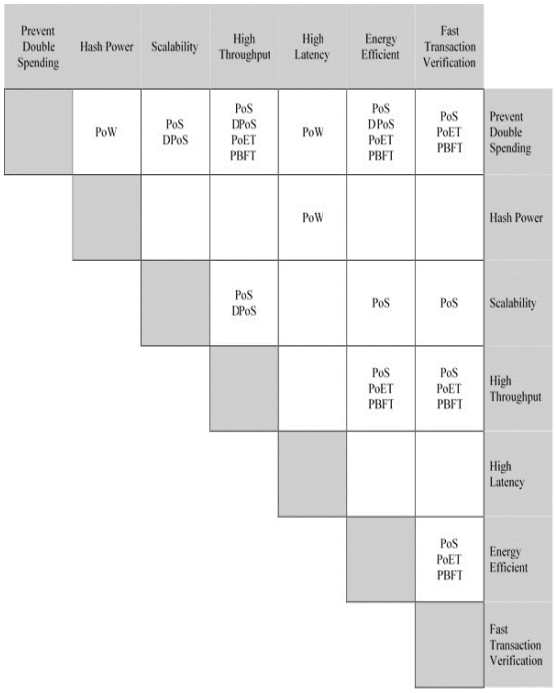

Figure 1: Reorganization of Consensus Mechanisms

Based on the results of the review of the existing comparative studies, it is possible to reorganize the existing consensus mechanisms into a grid as depicted by Figure 1. Such a reorganization is expected to help the researchers to identify the most appropriate consensus mechanism for a particular application with a given set of performance and security requirements.

Discussion

The review of existing consensus mechanism reveals that each and every consensus mechanism have different shortcomings. There is no consensus mechanism, which satisfies all the performance and security characteristics. As a solution, many hybrid consensus mechanisms have been proposed. However, the existing hybrid consensus mechanisms have not been empirically evaluated. They were compared only using theoretical aspects. Furthermore, a judicious technical study on performance analysis is needed. Identification of performance and security characteristics of existing consensus mechanism have led to select an appropriate consensus mechanism.

Conclusion

This work is expected to serve as a guideline for further understanding on blockchain consensus mechanisms and their unique security and performance characteristics. This paper, starting with a background study of blockchain technology, analyses the mainstream consensus mechanisms. The result is a reorganization of the existing consensus protocols so that, one might choose the most appropriate consensus mechanism for the application being developed considering multiple performance and security factors. Especially in the era of DApps, such a guidance is necessary since the nature of the application could vary and so as its requirements when selecting the consensus mechanism. Our future work will look in to the use of these findings to select the most appropriate consensus mechanism for a smart food supply chain in the organic food industry.

References

Alsunaidi, S. and Alhaidari, F., 2019. A Survey of Consensus Algorithms for Blockchain Technology. International Conference on Computer and Information Sciences (ICCIS), pp.1-6.

Antonopoulos, A. M. and Wood, G. D., 2018. Mastering Ethereum. 1st ed. O'Reilly Media.

Antonopoulos, A., 2017. Mastering Bitcoin. 2nd ed. O'Reilly Media, Inc.

Bach, L., Mihaljevic, B. and Zagar, M., 2018. Comparative analysis of blockchain consensus algorithms. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp. 1545-1550, doi: 10.23919 /MIPRO.2018.8400278.

Buterin, V., 2014. Ethereum: A next-generation cryptocurrency and decentralized application platform. Bitcoin Magazine, 23.

Buterin, V., Reijsbergen, D., Piliouras, G., 2020. Incentives in Ethereum's hybrid Casper protocol. International Journal of Network Management. doi:10.1002/nem.2098

CAI, W., Wang, Z., Leung, V.C., 2018. Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access 6, 53019–53033. doi:10.1109/ACCESS.2018.2870644

Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M. and Li, Y. 2020. Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks.

Castro, M., Liskov, B., 1999. Practical Byzantine Fault Tolerance. Proceedings of the Symposium on Operating System Design and Implementation 1–14. doi:10.1145/571637.571640

Chaudhry, N. and Yousaf, M,. 2018. Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. 12th International Conference on Open Source Systems and Technologies (ICOSST), pp.54-63, doi: 10.1109 /ICOSST.2018.8632190.

CoinDesk. 2020. Bitcoin 101 - Coindesk. [Online] Available at: <https://www.coindesk.com/learn /bitcoin-101/what-is-bitcoin> [Accessed 5 March 2020].

Cointelegraph. 2017. The History and Evolution of Proof-Of-Stake. [Online] Available at: <https: //cointelegraph.com/news/the-history-and-evolution -of-proof-of-stake> [Accessed 21 April 2020].

Deirmentzoglou, E., Papakyriakopoulos, G. & Patsakis, C. 2019. A Survey on Long-Range Attacks for Proof of Stake Protocols. IEEE Access, 7, 28712-28725.

Gai, F., Wang, B., Deng, W. & Peng, W. 2018. Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. Database Systems for Advanced Applications.

Guo, H., Zheng, H., Xu, K., Kong, X., Liu, J., Liu, F. & Gai, K. 2018. An Improved Consensus Mechanism for Blockchain. Smart Blockchain.

Hao, Y., Li, Y., Dong, X., Fang, L. and Chen, P., 2018. Performance Analysis of Consensus Algorithm in Private Blockchain. IEEE Intelligent Vehicles Symposium (IV), pp. 280-285, doi: 10.1109/ IVS.2018.8500557.

Hazari, S. and Mahmoud, Q., 2019. Comparative evaluation of consensus mechanisms in cryptocurrencies. Internet Technology Letters, 2(3), p.e100.

Hooda, P. Proof of Work (Pow) Consensus - Geeksforgeeks. [Online] GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/proof-of-work-pow-consensus/> [Accessed 30 May 2020].

Investopedia, 2018. Double-Spending Definition [WWW Document]. Investopedia Dictionary. URL https://www.investopedia.com/terms/d/doublespending.asp.

Ismail , Materwala,2019. Article,A Review of Blockchain Architecture and ConsensusProtocols : Use Cases, Challenges, and Solutions. Symmetry, 11(10), p.1198.

Judmayer, A., Stifter, N., Krombholz, K. and Weippl, E., 2017. Blocks And Chains:Introduction To Bitcoin, Cryptocurrencies, And Their Consensus Mechanisms. Morgan & Claypool.

Karamat, S. and Heal, J., 2020. A Brief History of Ethereum - Coin Rivet Guide to the Creation of Ethereum. [Online] Coin Rivet. Available at: <https://coinrivet.com/guides/cryptocurrencies /a-brief-history-of-ethereum/> [Accessed 15 March 2020].

Knoema. 2020. Bitcoin Price from 2009 to 2019 - Knoema.Com. [Online] Available at: <https://knoema.com/nmyfsf/bitcoin-price-from-2009-to-2019> [Accessed 5 March 2020].

Kostal, K., Krupa, T., Gembec, M., Veres, I., Ries, M. and Kotuliak, I., 2018. On Transition between PoW and PoS. 2018 International Symposium ELMAR,pp. 207-210, doi: 10.23919/ELMAR.2018.8534642.

Li, K., Li, H., Hou, H., Li, K. & Chen, Y. 2017. Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain. 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

Li, W., Andreina, S., ... Karame, G., 2017. Securing proof-of-stake blockchain protocols, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, pp. 297–315. Doi:10.1007/978-3-319-67816-0_17

Mahajan, D. 2019. A Survey Paper on Blockchain Technology. International Journal for Research in Applied Science and Engineering Technology, 7, 3564-3569.

Mahmood W, Wahab A. 2020 Survey of Consensus Protocols.SSRN Electronic Journal.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W. and Qijun, c., 2017. A review on consensus algorithm of blockchain. In: IEEE International Conference on Systems.pp.2567-2572.

Monrat, A. A., Schelen, O. & Andersson, K. 2019. A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, 7, 117134-117151.

Nakamoto, S., 2009. Bitcoin: A Peer-To-Peer Electronic Cash System. [Online] Bitcoin.org. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 20 December 2019].

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T. & Dutkiewicz, E. 2019. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access, 7, 85727-85745.

Nguyen, G. and Kim, K., 2018. A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems, 14(1), pp.101-128.

Ni, W., Abolhasan, M. & Makhdoom, I. 2018. Blockchain for IoT: The Challenges and a Way Forward. Proceedings of the 15th International Joint Conference on e-Business and Telecommunications.

Sadek Ferdous, M., Jabed Morshed Chowdhury, M., Hoque, M. and Colman, A., 2020. Blockchain Consensus Algorithms: A Survey. [Online] NASA/ADS. Available at: https://ui.adsabs.harvard.edu/abs/2020arXiv200107091S/abstract> [Accessed 26 March 2020].

Saleh, F., 2018. Blockchain without Waste: Proof-of-Stake. SSRN Electronic Journal. doi:10.2139/ssrn.3183935

Swathi, P., Modi, C., Patel, D., 2019. Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners, in: 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/ICCCNT45670.2019.8944507.

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. & Kim, D. I. 2019. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access, 7, 22328-22370.
Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), pp.1-32.

Wu, Y., Song, P., Wang, F., 2020. Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain. Mathematical Problems in Engineering 2020. doi:10.1155/2020/7270624

Xiao, Y., Zhang, N., Lou, W. & Hou, Y. T. 2020. A Survey of Distributed Consensus Protocols for Blockchain.

Xu, X., Weber, I. and Staples, M., 2020. Architecture for Blockchain Applications | Springerlink. [Online] Doi.org. Available at:

<https://doi.org/10.1007/978-3-030-03035-3> [Accessed 12 February 2020].

Yadav, A. K. And Singh, K., 2020. Comparative Analysis of Consensus Algorithms of Blockchain Technology. Advances in Intelligent Systems and Computing, pp.205-218.

Acknowledgement

This research was supported by the Accelerating Higher Education Expansion and Development Operation (AHEAD) of the Ministry of Higher Education funded by the World Bank.

Author Biographies

Thanushya Thanujan received B.Sc (Special) in Computer Science at Vavuniya Campus of the University of Jaffna and M.Sc in Computer Science at the University of Peradeniya. Since 2016 she has been working as a lecturer (Prob.) in the Department of Computer Science, Faculty of Applied Science, Trincomalee Campus. Her research interests are Blockchain Technology, Internet of Things, Graph Theory Image Processing and Network Security.

Chathura Rajapakse is a senior lecturer attached to the Department of Industrial Management, Faculty of Science, University of Kelaniya. He is an alumna of the Tokyo Institute of Technology, Japan from where he received a Doctor of Engineering degree in Computational Intelligence and Systems Science in March 2015. He also possesses a Master of Engineering degree from the same university as well as a B.Sc. (Special) degree in Industrial Management from the University of Kelaniya, Sri Lanka. He is conducting research on smart and intelligent information systems since 2009.

Dilani Wickramaarachchi is a senior lecturer attached to the Department of Industrial Management, Faculty of Science, University of Kelaniya. She is an alumna of the La Trobe University, Australia from where she received her PhD in Software Engineering in March 2015. She also possesses a Master of Science in Computer Science degree from the University of Colombo School of Computing(UCSC), Sri Lanka, as well as a B.Sc. (Special) degree in Industrial Management from the University of Kelaniya, Sri Lanka. Her research interests are in Global Software Engineering, Human learning through co-creation, Software code quality improvement, Computational thinking and Digital innovation.