Consensus Algorithms Blockchain: A comparative study

Siham Hattab , Imad Fakhri Taha Alyaseen
Dept of Compute Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia
siham.hattab@hotmail.com
Dept of Compute Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia
imadf@iium.edu.my

***Abstract*— A blockchain is a Distributed Ledger Technology that has been defined as a "distributed, shared, encrypted database that serves as an irreversible and incorruptible repository of information. Blockchain can be defined as a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable and updatable only via consensus or agreement among peers. In blockchain platforms, each transaction in the public ledger is verified by consensus of the majority of the system participants in a** transparent **and secure way. The consensus algorithm refers to the process of attaining an unified agreement on the state of the network in a decentralized way and to facilitate the verification and validation of information being added to the blockchain. This paper aims at providing a comparison between most of the recent consensus algorithms regarding the scalability of the algorithm; the type of blockchain, node identity, the performance of the algorithm (in terms of throughput & latency) and Adversial Tolerance and to deliver a solid basis for discussions about current statistics. In this research, we also presented a new category of the Blockchain consensus algorithms, which consist of three groups as follows; the proof based on Hardware, the proof based on stake, and the proof based on voting.**

***Keywords*—** Blockchain, Consensus algorithm, performance, scalability.

I. INTRODUCTION

Blockchain is a technology which emerged in recent years, firstly it was employed within Bitcoin's cryptocurrency as a public ledger[1]. It is essentially a decentralized and distributed data structure, replicated over a peer-to-peer (p2p) network[2]. Blockchain consists of consecutive chained blocks, each one linked with the previous, containing records that has to reach a consensus before the contract is enacted [1][3][4].The consensus is a way to ensure the nodes on the network verify the transactions and agree with the order and existence on the ledger[5][6]. In the case of applications like cryptocurrency, this process is critical so as to prevent double spending or other invalid data being written to the underlying ledger, which is a database of all the transactions [7][8]

The most widely used consensus algorithms are the Proof of Work (PoW) algorithm[1],the Proof of Stake (PoS) algorithm[9] [10] as well as Practical Byzantine Fault Tolerance (PBFT) algorithm[11];however, there are also other consensus algorithms which utilize alternative implementations of PoW, PoS and PBFT, as well as other hybrid implementations and some altogether new consensus strategies[12][13][8].There are newer consensus mechanisms coming up every now and then, all of which are hoping to achieve the objectives of collaboration, egalitarianism and inclusion[14][12].Consensus is used to create a more equal and fair society for users in the decentralized network from all around the world[15]. In this research, to design the comparative study based on selected factors, we present a new category of the Blockchain consensus algorithms, the classification consists of the following main groups (see fig1)as follows; The first group is the proof based on Hardware which is by using computing power to translate into Hashing Power for the network ,this group includes POW, POET and POC. The second group which includes POS, POI and LPOS is Proof Based on Stake, in the PBS networks, the validator chosen depends on the percentage of the asset (stake) owned or staked by a validator. The third group is proof based on voting, where the member nodes have the right to vote who will be the leader and validators, and the block with the highest votes will be validated in which it will be a unique block, in this group we selected the most popular consensus algorithm which are; PBFT, DBFT and FBA.

The remaining part of this paper is organized as follows: The current section is section one, followed by section two which represents this research terminology definitions. Section three describes the research methodology and

section four present the outcomes of this research. Finally, section five presents the conclusion.

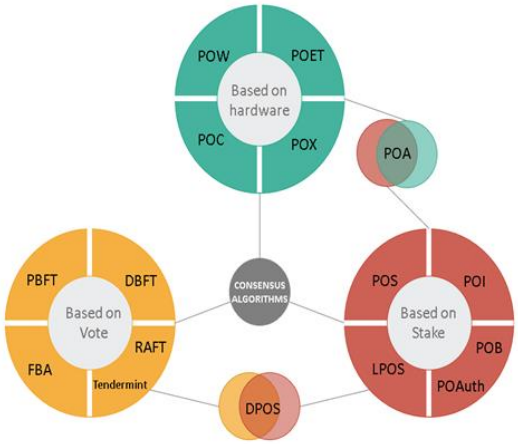

Fig. 1 The classification of Consensus algorithms based on algorithm architecture.

II. CONSENSUS ALGORITHMS

A blockchain protocol is a common term for consensus methods. These methods are different systems that are implemented to reach consensus and validate transactions within a blockchain network[11] . As defined earlier, the consensus algorithm plays a crucial role in maintaining the safety and efficiency of the blockchain. Using the right algorithm may bring a significant increase to the performance of blockchain application. Table 1 shows most of today's blockchains consensus algorithm.

Table I list of well-known consensus algorithms (CA)

Abbreviation	Name of CA	Abbreviation	Name of CA
POW	Proof of work	PoET	Proof of Elapsed Time
POS	Proof of stake	POI	Proof of Importance
DPOS	Delegate Proof of stake	POC	Proof of capacity
LPOS	Leased Proof of stake	POAuth	Proof of Authority
PBFT	Practical Byzantine fault tolerance	POX	Proof of exercise
DPFT	Delegate Byzantine fault tolerance	DAG	Directed acyclic graphs
FBA	Federated byzantine agreement	UNL	Unique node lists
POB	Proof of burn	-	Ripple
POA	Proof of activity	-	RAFT

In this research, we propose a comparison between nine (09) consensus algorithms; Proof of work, proof of stake, Proof of Elapsed time, Proof of Importance, Proof of capacity, Leased Proof of stake, Practical Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance, Federated byzantine fault tolerance through six (06) factors: the type of blockchain, identity of nodes, scalability, throughput, latency and adversarial tolerance.

Different consensus methods use different protocols to ensure that the correct consensus is reached, and that no malicious nodes can get good nodes to agree on incorrect transactions. To formalize our comparison of the presented consensus algorithm, we summarize their most important properties to present a new category. The classification can be roughly divided into the following main groups as illustrated in Figure 1. First, proof based on Hardware which requires the nodes joining the verifying network using hardware to perform some computational task to show that they are more qualified than the others to do the appending work. For this group, we will focus on some well-known ones (Proof of work, Proof of Elapsed time and Proof of capacity) that are currently used in the blockchain platforms.

Proof of work (abbreviated to PoW) is the first consensus algorithms which are used in the blockchain technology era[1], it is the computation of a cryptographic hash function with some degree of difficulty [16].In POW, miners use Hashcash (SHA-256) to solve computationally difficult math problems in order to add blocks onto the blockchain[13]. The process of intensive computations was developed to confirm the legitimacy of a transaction or avoid a phenomenon called Double-spending[7]. Since it is challenging for a single attacker to solve the difficulty for all the modified blocks before the honest nodes in the network .The proof of work concept is as follows: after the Transactions are accumulated together in the form of blocks, the Miners confirm the transactions within the blocks as legitimate, after that the miner tries to solve a mathematical problem known as the proof-of-work problem [17].A reward is then given to the first miner who solve the problem, finally Verified transactions are stored in the public blockchain Network. Another consensus algorithm in which is under proof-based on hardware is proof of Elapsed Time, PoET is often used on the permissioned blockchain networks. PoET was introduced to address the problems of high-power consumption and latency in the PoW-based consensus protocols and to improve the efficiency of the mining process by following a fair lottery system[18], where every single node is equally likely to be a winner. PoET is similar to the proof of work[12] but with significantly lower energy (resource) consumption. According to this protocol, the miner node, which presents the least waiting time is selected to mine the next block; the timer is different for every node. Every user in the network is assigned a random amount of time to wait from a trusted function in a general-purpose processor, and the first user who finished the waiting gets to Produce the next block to the

network[19].The third consensus algorithm is Proof of capacity. POC is designed for public distributed ledger[20], Proof of capacity emerged as one of the many alternative solutions to the problem of high energy consumption in proof of work (POW) .This algorithm allows the validators in the network to use their usable hard drive space to increase miner's chances of producing the next block, instead of using the mining device's computing power as in the proof of work algorithm or the miner's stake as in the proof of stake algorithm[21].

The second group is stake-based consensus, these algorithms favor using one's overall holdings or "stake" instead of energy consumption as an indication that effort was used to verify a transaction (nodes are required to use their coins (stake) to verify a transaction in the network) as this group includes: Proof of stake, proof of importance and leased proof of stake.

Proof-of-Stake (PoS) algorithm is designed to overcome the disadvantages of PoW (high energy consumption)[9]. PoS is a different way to validate transactions and achieve the distributed consensus. Instead of unnecessary computation requirements of proof of work and competing with others, the node that will mine the next block is chosen based on its proportional stake in the network which is its wealth in terms of that cryptocurrency. In PoS, users who chose to be validators have to stake (stake is the coins that a user owns in order to participate in validation) some part of their coins or tokens, in order to have a chance at verifying transactions in a block. Usually, in the PoS system, once the block is validated, the validator will be rewarded a certain amount of cryptocurrency for their work (transaction fees).

Proof of Importance (PoI) is a consensus algorithm which is a variation of Proof of Stake. In PoI, instead of considering only nodes' stake for solving the next block, it takes into account other factors including node's productive network activity, which means that Proof of importance not only relies on how much stake a user has in the system, but it also monitors the usage and movement of tokens by the user to establish a level of trust and importance[22]. Another consensus algorithm is Leased proof of stake. Leased proof of stake (LPoS) is another consensus algorithm which came to improve the degree of scalability and transaction throughput of the proof of stake protocol as this algorithm give the user the right to leased their coins to other trusted nodes. The larger the amount that is leased to all trusted node, the higher the chances of that node will be selected to produce the next block, If the node has validated the next block, the user would receive some part of transaction fees that are collected by the node[12][15].

In the third group, all the nodes in the network would have to verify the transactions or blocks as they will communicate with others, before deciding to append their proposed blocks to their chain or not and this group includes: PBFT, DBFT, FBA.

Practical Byzantine Fault Tolerance (PBFT) is considered as the first practical solution to achieve consensus that overcomes Byzantine failure and has been executed in several modern distributed computer systems, including some blockchain platforms. PBFT Network comprises of a leader and validating peer nodes whereby the block creation process is executed through three phases: pre-prepares, prepare and commit phases. In PBFT, a client sends a request to the leader node to invoke a service operation, peers receive the transactions from the leader node, validate them (here, the validation is run through multiple rounds to reach consensus) then broadcast them to other peers including the leader, the leader node will order the transactions by their created time, putting them into a block. Once 2/3 of the nodes have the same hash, the new block will be published.

Another algorithm under voting-based proof is Delegate Byzantine Fault Tolerance (DBFT),DBFT combines the characteristics of dPoS and PBFT to solve the low performance drops of the latter as this algorithm splits clients within a P2P system into two groups: one is the book-keeping nodes which are generated through voting by the entire network users, book-keeping is responsible for the consensus communication with other book-keeping nodes to generate new blocks; the other is the ordinary nodes, which does not participate in the consensus, but can verify and accept new blocks. The book-keepers are elected just like in DPoS whereby the leader node will be elected and all the transactions in the network will be sent to it. After the evaluation of received transaction by the book-keepers, it will be sent to all other book-keepers. When the latter book-keeper receives the transaction results, these results are again sent to the leader node as the block will be crated if 2/3 of the book-keepers agree.

A Federated Byzantine Agreement (FBA) is a form of Byzantine fault tolerance as it is used also to improve the throughput, network scalability, and low transaction costs and Stellar was the first cryptocurrency to successfully implement FBA. This algorithm, require for each validator to decide which other validators they trust, and their list of trusted validators is called their quorum slice (quorum slice is its subset that helps a node in its agreement process)[23]. The quorum slices of each validator connect the whole network together to create a quorum, or network-wide consensus on a transaction to reach an agreement. Without the need for one centralized authority to decide on the validator list, users can spin up a validator and participate in consensus if any other participating validator adds them to their quorum slice.

III. COMPARISON STRUCTURE

In this research, our comparison structure consists of three essential steps: listing the most popular consensus mechanisms (selected algorithms) and the factors for the comparison, then the classification of these algorithms based on the algorithm architecture and comparative study design. Figure 2 shows the proposed structure for analysing and comparing the consensus mechanisms.

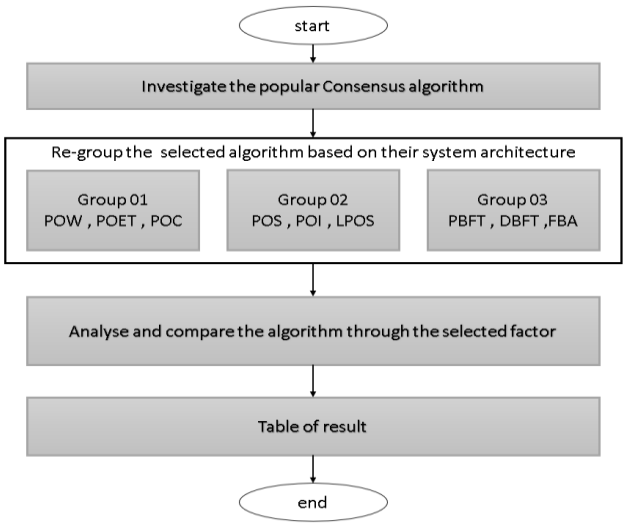

Fig. 2: Comparison structure

As mentioned before, the objectives of this research are to conduct a comparative study for the nine (09) consensus algorithm of blockchain. After emphasizing on the three categories that are mentioned earlier and highlighting the definition of the essential characteristic of the three-consensus categorized group, the type of Consensus algorithms should be sufficient to provide the desired level of blockchain. In contrast, not all the Consensus algorithms are perfect; for example, Proof of work is the first Blockchain algorithms introduced in satoshi Nakamoto[1]. It has a lot of perks, but it also comes with a lot of flaws. In this part, we will try to investigate what are the main flaws of Consensus algorithms in each group. Finally, we will

discuss the strengths and weaknesses of the candidates' algorithms in fundamentals factors of the study, then highlight the best algorithm in each group which have less drawback.

TABLE IICOPMARISIONS OF THE SELECTED CONSENSUS ALGORITHM FOR GROUP OF PROOF BASED ON HARDWARE.

Factors	POW	POET	POC
Type of Blockchain	Public Blockchain	public and private Blockchain	Public Blockchain
Node identity	Unknown nodes	untrusted nodes and open	Unknown nodes
Scalability (# of nodes)	thousands of nodes. (depends on computational power)	Unlimited nodes	thousands of nodes. (depends on disk space)
Scalability (# of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)
Performance (throughput)	nearly (7) Tx/sec	High throughput	7,000 tx per second
Performance (latency)	10 min per block	Low latency (not measured)	4 min per block
Tolerated power of an adversary	51% computing power	Unknown	50% of the space.

PoW is designed for non-permissible public distributed ledger and the high computation requirement by the protocol, and also guarantees high security. A malicious user needs 51% of the computing power, which is near impossible, considering the computational difficulty level of the protocol. PoW-based blockchain offers good node scalability with poor performance, whereas PoET-based blockchain offers good performance for unlimited numbers of nodes. POC requires approximately 30 times less power than an AISC based miner, making it the most energy-efficient of the mining protocols. However, it requires more P2P interactivity than PoW, which leads to network congestion, although, the algorithm lacks security analysis and is vulnerable to different security attacks but there is a risk of creating malware that uses hard drive space for mining purposes without the user's knowledge. Unlike other permissioned consensus protocol, PoET reaches consensus while maintaining the anonymity of the participants. This method yields a throughput higher than the PoW with a low latency compared to POC.

PoS eliminates the unnecessary computation requirements of proof of work as this algorithm is depending upon nodes with the highest amount of stake which makes the blockchain less private and centralized. PoS have a high scalability only with very limited network throughput but in contrast, LPoS throughput and scalability of number of consensus nodes are better compared to POS and POI. LPoS tries to solve the centrality problem in PoS by enabling the nodes with low coins balance to participate in block verification by adding a leasing which lead to low latency with only 60 second per block.

TABLE III COPMARISIONS OF THE SELECTED CONSENSUS ALGORITHM FOR GROUP OF PROOF BASED ON STACKE.

Factors	POS	POI	LPOS
Type of Blockchain	Public Blockchain	Public and private blockchain	Public blockchain
Node identity	Unknown nodes	Unknown nodes	unknown nodes (hallmarked nodes)
Scalability (# of nodes)	thousands of nodes. (depends on own stake)	thousands of nodes. (depends on who has more than 10,000xem)	thousands of nodes. (depends on own stake)
Scalability (# of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)
Performance (throughput)	better than pow (Approx. 13.3Tx / sec)	4,000 Tx/sec	hundreds of transactions per second
Performance (latency)	15 second per block	20 second per block	60 second per block
Tolerated power of an adversary	51% of all stake	50% importance	51% of all stake

PoI like other PoS-based methods, also depends on stake concepts and their activity in users accounts, this algorithm produces high throughout and offer low latency compared to LPOS, a block in POI is added to the blockchain by 20 seconds with the capability of processing 4000 transactions per second. In PoS algorithm, an attacker would need to control at least 51% of the stake (as in, total currency) in the network to forge transactions.

TABLE I V COPMARISIONS OF THE SELECTED CONSENSUS ALGORITHM FOR GROUP OF PROOF BASED ON VOTING

Factors	PBFT	DBFT	FBA
Type of Blockchain	Public or Private Blockchain	Private Blockchain	Public or private Blockchain
Node identity	Permissioned . Known node	Permissioned. Known node	Unknown node
Scalability (# of nodes)	Limited node	7-9 nodes	Unlimited node (any one can enjoy to quorum slice)
Scalability (# of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)
Performance (throughput)	2,000 Tx/s	10,000 Tx/s	10,000 Tx/s
Performance (latency)	10 second	15-20 second	10 second
Tolerated power of an adversary	33.3% replicas	33.3% replicas	33.3% replicas

PBFT is not the best choice for non-permissible, public blockchains due to their limited scalability (its high network overhead makes it un-scalable for large networks) and comparatively low tolerance towards malicious activities. However, PBFT has high throughput, low latency, and low computational and it's optimized to have high-performance. DBFT has many desirable features similar to that of PBFT,as DBFT and PBFT require 2/3 of the validation peers to agree on the next block's contents before submitting. The only difference is in how the votes are counted, but, its average latency for block creation is 15-20 seconds which is slightly better than PBFT. FBA is a modified version of the PBFT algorithm, where it doesn't require maintaining a membership list. This method is decentralized and is open to the public which allows everyone to participate in the consensus protocol as it has a very low latency with high throughput with 10k tx/s better than the precious algorithms in terms of scalability of a number of consensus nodes and clients. In this group, FBA blockchains feature an entirely decentralized identity management, in contrast, the PBFT and DBFT approach is a centralized identity management, which requires every node to know the entire set of its peer nodes participating in consensus, as these features make FBA very attractive for blockchain developers.

IV. RESULT AND DESCUSSION

Every type of blockchain in the network need a different consensus algorithm to fit for the various blockchain platforms and to make sure to achieve blockchain reliability. In this paper, we proposed the new classification for consensus algorithms based on their architecture to make a comparison and analyze these algorithms. In particular, we focused on the currently used consensus algorithms and some factors, these factors include node identity, scalability in terms of a number of consensus nodes and clients, tolerated power of the adversary, performance in terms of latency and throughput. Each of these consensuses has addressed some of the limitations including throughput, latency, computational overhead, network overhead, and scalability. However, none of them have been successful in addressing all the limitations to an acceptable degree. Finally, for the most demanding blockchain applications, it would be interesting to move from unnecessary computation requirements (based on hardware) to the BFT protocols. In general, implementing consensus in hardware may yield impressive performance.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] A. Sari, "The Blockchain: Overview of 'Past' and 'Future,'" no. December 2017, 2018.
[3] D. Patel, J. Bothra, and V. Patel, "Blockchain exhumed," ISEA Asia Secur. Priv. Conf. 2017, ISEASP 2017, 2017.
[4] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, 2018.
[5] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain : Comparative Analysis , Challenges and Opportunities," pp. 54–63, 2018.
[6] A. Kareem, "Algorithms And Security Concern In Blockchain Technology : A Brief Review," no. 1436182, 2018.
[7] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," J. Inf. Process. Syst., vol. 14, no. 1, pp. 101–128, 2018.
[8] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 2017 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017, 2017.
[9] S. King and S. Nadal, "Peercoin-Paper," 2012.

[10] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2 Pavel," Self-published, 2014.
[11] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin, and M. Takemiya, "YAC: BFT Consensus Algorithm for Blockchain," 2018.
[12] M. Salimitari and M. Chatterjee, "A Survey on Consensus Protocols in Blockchain for IoT Networks," 2019.
[13] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks," 2018.
[14] L. M. Bach, B. Mihaljevis, and M. Žagar, "Comparative Analysis of Blockchain Consensus Algorithms," pp. 1545–1550, 2018.
[15] A. Wahab, "Survey of Consensus Protocols," pp. 1–12, 2018.
[16] J. R. Christopher, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," 2016.
[17] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A Review on Consensus Algorithm of Blockchain," pp. 2567–2572, 2017.
[18] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On Security Analysis of Proof-of-Elapsed-Time (PoET)," 2017.
[19] R. Kochhar, B. Kochar, J. Singh, and V. Juyal, "Blockchain and Its Impact on Telecom Networks Blockchain and Its Impact on Telecom Networks," no. August, 2018.
[20] R. S. Seán Gauld1*, Franz von Ancoina, "The Burst Dymaxion," 2017. .
[21] T. Larsson, "Cryptocurrency performance analysis of Burstcoin mining," 2018.
[22] Y. Lai, "Technical Reference," Imid 2009, no. 159679, pp. 1069–1072, 2009.
[23] A. Baliga, "Understanding Blockchain Consensus Models," Whitepaper, no. April, pp. 1–14, 2017.