A Review of Blockchain Consensus Algorithm

Manas Borse, Parth Shendkar, Yash Undre, Atharva Mahadik, and Rachana Yogesh Patil

Abstract The advent of Blockchain started when a mysterious person or organization with an alias Satoshi Nakamoto published a white paper named "Bitcoin: A Peer-to-Peer Electronic Cash System." This paper introduced a digital currency with no middlemen and no central authority. This meant, no transaction taxes, secure transactions, and a uniform currency. Hence, started the expedition of Blockchain Technology. Blockchain Technology needs consensus algorithms to insert a valid block of data to the Blockchain and maintain its state. Due to the rapid developments in Blockchain Technology and it's adaptation to a plethora of wide areas (games, digital art, medical records, etc.), a study of consensus algorithms is essential to help researchers and developers to adapt a consensus algorithm according to their needs (proof of resource or majority voting).

Keywords Consensus algorithm · Blockchain · Proof of work · Proof of stake · Proof of elapsed time · Byzantine fault tolerance

1 Introduction

1.1 Blockchain Technology

Blockchain Technology is a decentralized, immutable, consensus based, distributed ledger. It is a peer-to-peer network with its nodes spread all over the world, reaching an agreement about the form and validity of transactions. Once this consensus, as we call it is reached, the transactions are stored in a block of data and linked to the previous block. This forms an unending immutable series of data blocks, hence Blockchain. There are diverse consensus algorithms which are being used today. This paper discusses the consensus algorithms.

All the parties involved in the Blockchain network has to agree upon a valid form of ledger so that the data block can be added to the block chain. The protocol that

M. Borse (✉) · P. Shendkar · Y. Undre · A. Mahadik · R. Y. Patil
Pimpri Chinchwad College of Engineering, Pune, India
e-mail: manasborse02@gmail.com

I. J. Jacob et al. (eds.), *Expert Clouds and Applications*, Lecture Notes in Networks and Systems 444, https://doi.org/10.1007/978-981-19-2500-9_31

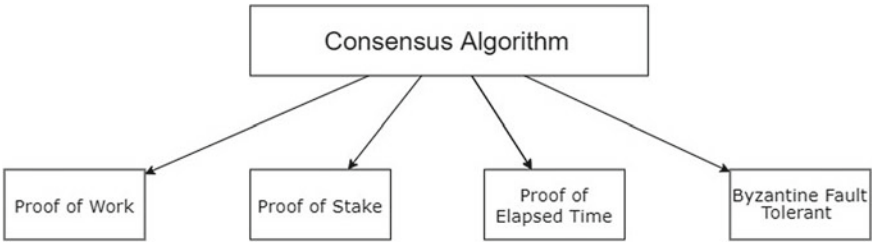

Fig. 1 Taxonomy of consensus algorithms

allows these parties to come to a "consensus" is called a consensus Algorithm. The classification of consensus algorithm is shown in Fig. 1.

2 Related Work

In this section, the existing blockchain consensus algorithms are studied and their advantages and disadvantages are analyzed.

2.1 Proof of Work Consensus Algorithm

Bitcoin is still the most influential cryptocurrency system. Its Proof of Work consensus is a system that rewards the first individual who can solve a hard math problem. This system limits the number of miners who can successfully solve the problem.

The authors of [1] gives a modification to the Bitcoin by taking advantage of the missed computational effort of miners. It would allow miners to justify their work and the network's difficulty would then decrease accordingly.

Due to the unique features of Blockchain, it has inspired a wide range of new social applications. However, its decentralized nature and its use of Proof of Work (PoW) technology can be very challenging to manage.

The algorithm can only keep trail of the network hash rate quick enough [2]. However, it cannot set the target BPT on time. We introduce a (linear predictor based difficulty control algorithm) that takes into account the relationship between the hash rate and the difficulty. It achieves better stability and flexibility in terms of BPT.

The crypto (Bitcoin) has utilized Proof of Work consensus to prevent double spending attacks [3]. However, it is not yet clear how this will affect the decentralized network's security. Gavrilovic and Ciric [4] proposes a new protocol that takes into account the computing control of each server and regulates the trouble of making a block on the base of the evaluation.

Majority of the emails traffic is spam. It is an abuse that is used for the determination of mass dissemination of unwanted messages. In [5, 6], solution needs a specific quantity of work from the recipient before the email message is sent. The extended SMTP protocol method would be evaluated through the use of the Proof of Work. assessment of the servers work and the influence of distributed spam on it will be shown. The proposed solution will be presented to help minimize server load and reduce spam traffic.

A Blockchain is an open ledger technology that enables people to verify transactions. There is a way to improve scale and transaction speed is to find an answer that provides quicker Proof of Work algorithm. In [6], parallel mining method is introduced. The proposed method involves a selection process for a manager, a reward system, and a distribution of work. It was tested using a variety of test cases.

Bitcoin, the world's first digital money, is founded on the PoW (Proof of Work) consensus procedure. Its widespread adoption has raised the bar for Blockchain Technology.

Feng and Luo [7] has also covered the various concepts of Blockchain and Proof of Work consensus algorithm along with its performance analysis.

In [3], they propose a new protocol that will allow miners to generate blocks with equal difficulty and reward them with equal opportunity. The new method will also evaluate the computing power of the nodes. Based on the evaluation, the reward for the user's incentive is also changed (Table 1).

2.2 Proof of Stake Consensus Algorithm

Over the years Proof of Stake (PoS) consensus algorithms is developed and is to be added in the systems so that a distributed ledger can be added in the system and then being processed over the whole working of the system [10, 11]. The validators do not receive any amount of reward on the blocks that have been validated by them, instead they receive networking fees as their type of reward. Hence, they can be awarded in a way that has been a true form of reward. However, the technology used or developed in this system is currently limited.

The Proof of Stake consensus algorithm's operation is based on transactions, and their validation by the validators for the transaction or it being called as node to be added in the system [12]. The nodes are the ones who make the transactions (or the amount of transactions) in the system. All nodes who wish to be validators for the next block must stake a certain amount of money [13].

The highest amount of stake which was being validated is added in the system or is being elected as the validator [14]. Then, the validator verifies all the transitions which have being taken place in the system then if the transaction which was being processed was an authentic and proved transaction, then the validator does hold the transaction as valid and it adds it or publishes it to the block [15].

Now, if the block being added by the validator is verified then the transaction is valid and then the validator gets a stake back with a reward from the transaction

Table 1 Reference papers studied of proof of work

Reference	Advantages	Disadvantages
[1]	PoE utilizes computational power and increases mining power. Miners who fail at computational tasks might get experience	High energy consumption is advantageous to nodes that accumulate computational power
[2]	The prediction-based difficulty management method provides significantly improved stability and flexibility on BPT, as it's based on the link between hash rate, difficulty, and BPT	Author prove that the prediction-based difficulty control technique cannot be implemented using smoothed BPT as a calculating method
[3]	This ensures that all miners have an equal chance of success. In addition, based on the evaluation, the reward for the user's incentive is modified	Miner can easily attack against blockchain
[4]	The suggested approach reduces spam traffic and server strain while having no negative impact on legitimate email users' experience	It takes more processing time
[5]	In comparison to the present system, preliminary data suggest that proof of work scalability has improved by 34%	There is a chance to get incorrectly evaluated by a reputation system
[6]	Extensive testing shows that our method detects Sybil attacks with a high detection rate and a low communication and computation cost	Due to the wireless communication characteristics, a solution is difficult to achieve
[7]	CryptoNight, which uses scratchpads of various sizes, is the most equitable proof of work algorithm	Each algorithm is affected differently by the size of the accessible memory region
[3]	This ensures that all miners have an equal chance of being successful. Furthermore, based on the evaluation, the reward for the users incentive is changed	a potential mining pool exhibits symptoms of centralization
[8]	It demonstrates that mining industry has a propensity for centralization, which is incompatible with the basic concepts of cryptocurrencies	The anticipated value influences the reward once it has been adjusted for the rate is obtained
[9]	The paper proposes a proof-of-useful-randomness method that can improve energy efficiency	A single iteration in PoUR might take longer than a typical PoW iteration

Table 2 Reference papers studied of proof of stack

Reference	Advantages	Disadvantages
[10]	They demonstrated the use of blockchain technology in the healthcare system as well as the system's applications	Complication in reading and studying the data
[11]	They introduced Bazo which is improved network to meet the demands of Internet of Things networks	It is complex to implement in real world scenarios
[12]	The system measures user's particular skill and ranks him according to his skill used	Risk of any user uploading fraud data is relatively high in it
[13]	It has offered resistance to the security threats while recording the transactions of the data	Cannot be used on multilevel platforms
[14]	This system has been used to improve consensus within it by scaling vote according to validator's profile	Profile reading takes a considerate amount of time
[15]	Studied weighted voting in the distributed ledger and created an algorithm for better implementation of distributed ledger	Security risk is high
[16]	They used picturable signatures to construct a blockchain which can protect from LRSL attacks	System is complex to design

processed or the block verified. If the block being processed is not verified, then the validator will lose the stake and will get a negative review for the transaction or the addition of the certain block. It will result in his negative ranking and will hold him in a low position of the validators [16] (Table 2).

2.3 Proof of Elapsed Time

The properties that make Blockchain innovation incredible, like data integrity and flexibility to vindictive nodes, rely principally upon the decision of consensus protocol used to facilitate the network. The essential development of Blockchain innovation is to use these algorithms in completely decentralized, open networks [17]. Consensus can be thought of as an entity whose sole purpose is to eliminate uncertainty by giving everyone a fair chance to make their requests append into the Blockchain network [18].

Now, PoET is nothing but a lottery-based consensus algorithm that gives a fair chance to every validator to publish its data in the block [19].

In a way, conventional PoW can be likened to a lottery, with the likelihood of winning being proportional to the amount of computing effort that is involved. Any node can be the first to solve a problem and distribute a block yet the possibility of winning is directly related to computational speculation [20]. This irregularity prevents any one side from consciously influencing the square composition. Instead of spinning its computational wheels, PoET assigns each node an irregular stand-by time-examined from a spectacular appropriation, produced by code operating inside a "trusted execution environment." All validators collect exchanges into candidate blocks, and when the node's stand-by period expires (and no other square has been distributed efficiently at this height), it publishes its candidate block and advertises to the network. When more than one block is published at the same moment, a percentage of time spent waiting up is used to calculate the predicted fork, with the chain with the shortest overall stand-by time being preferred [21, 22].

For several reasons, PoET stands out as a good one to study in terms of power and accessibility, it is one of the best algorithms, with its most essential use in Bitcoin [23]. It is also devoid of digital money, making it a viable solution for industry use cases where trades aren't always monetary. Finally, it is extremely parameterizable, in contrast to the Bitcoin convention, which has remained mostly dormant since its inception and gives few tools for updating. The selection of block interval, the amount of time that elapses between sending progressive squares to the chain, is significant among these lottery-style consensus bounds [24, 25] (Table 3).

2.4 Byzantine Fault Tolerance

In this paper [26], research on PBFT is done to improve its system flexibility, high communication overhead, bad behavior of leader node. This is done by simultaneous joining and leaving of nodes, by admitting valid nodes and limiting messages, and by election of trusted leader node, respectively.

Scalability is a major problem [27] of BFT algorithm; and hence, this paper aims to address this issue. The proposed solution is a Multi-layer BFT algorithm which effectively decreases latency and improves scalability.

This paper [28] suggests that a reputation-based model should be adopted to evaluate consistency and validity of information provided by nodes. This reputation-based model, according to this paper should be able to make BFT more secure and reliable.

In this paper [29], transactions are classified into categories, namely equal and unequal transactions, unequal transactions are categorized into common and troubled transactions. Now, only these troubled transactions are subjected to the BFT algorithm to improve scalability.

A group of leader nodes is selected to improve consensus accuracy and to minimize network communication cost [30].

SBFT makes use of a mixture of 4 ingredients: the usage of creditors and getaway signatures to lessen verbal exchange, the usage of a constructive rapid path, lowering

Table 3 Reference papers studied of proof of elapsed time

Reference	Advantages	Disadvantages
[17]	The execution upholds dependable gathering of any ideal responsibility. REM might be seen as recreating the conveyance of distribution of block-mining intervals related with PoW, however, REM does as such with PoUW, and hence wipes out squandered CPU exertion	Study shows that no single algorithm can be utilized to accomplish various information prerequisite and it not relies upon prevalence of that algorithm
[18]	DC-PoET was able to achieve a higher throughput	There is still room to improve the protocol's efficiency by more smartly and dynamically creating the blockchain overlay network
[19]	Use of Blockchain in IoT strengthens innovation with emphasis on recognition of customers	Blockchain conveniently stores transactions and device Id's without a central server. However, the ledger must be kept on the nodes themselves, and it will inevitably increase in size thus reducing the efficiency
[20]	Adapts to a fairer means to achieve an agreement on who will get to publish their block	An infiltration in the Blockchain system can be expected if the attacker succeeds in generating blocks with the help of compromised nodes
[21]	PoET reduces the computational work load although being a lottery-based consensus like PoW	This algorithm can still be broken by corrupted SGX
[22]	After undergoing the tests, the throughput was able to cap on 2300 tx/s. This is yet another milestone achieved as it beats the results acquired for hyperledger fabric	Requirements for further proficiency observed achieve
[23]	The TEE handles the confidentiality of data and integrity while dealing with the computation aspect	An infiltration in the blockchain system can be expected if the attacker succeeds in generating blocks with the help of compromised nodes
[24]	Blockchain avoids data loss in reference to failure of centralized database. Also, blockchain provides more secure means to attain a transaction	A proper need to be implemented to make this process fool-proof
[25]	Because this consensus is executed in TEE provided by SGX devices, it is supposed that cheating with the work of the two above functions is very difficult	An infiltration in the blockchain system can be expected if the attacker succeeds in generating blocks with the help of compromised nodes

customer verbal exchange, and making use of redundant servers for the short path [31].

This paper [32] aims to improve transaction's throughput and decrease the time required for implementation of requests in a personal Blockchain. The tactics controlling Block Proposal Verification are carried out simultaneously in place of strolling chronologically.

To evaluate distinctive consensus algorithms primarily based totally on particular parameters consisting of crash fault tolerance, verification speed, throughput (TPS), scalability [33]. In case of semi-closed permissioned networks of more than one firms, PBFT is recommended.

The aim of this article consists in allocating the Hyperledger Fabric and understand all information on Hyperedger Frameworks to decide whether its usefulness is justified in practice [34]. They have observed that the Hyperledger Fabric is an enormous and dynamic project and it has huge range of use cases (Table 4).

Table 4 Reference papers studied of byzantine fault tolerance

Reference	Advantages	Disadvantages
[26]	More secure, fault tolerant	Nodes cannot join and exit freely
[27]	Faster can tolerate more number of nodes	No improvements in security, no change in leader node selection system
[28]	Increases the average transactions per second by 15% and decreases latency by 10%	Scaling problem is not solved
[29]	Faster than PBFT, showed 61.25% performance improvement when compared to BFT of Hyperledger Besu	No change in leader node selection system
[30]	The process of consensus and validation between different organizations will have stability and speed. This can be applied in data management and value creation	Scalability problem still remains
[31]	In a large scale deployment, this modification of PBFT can work effortlessly	Election of primary node is same
[32]	Throughput is increased and latency is decreased	Election of primary node is same
[33]	Verification speed, throughput (TPS) is better in PBFT	Scalability needs improvement compared to other algorithms
[34]	Hyperledger fabric is planned to be used for corporate right from the start. These are the maximum lively projects, and the network collected across the platform keeps to grow	It has got a complex architecture It is not much network fault-tolerant

3 Challenges/Findings

3.1 Proof of Work

Since Proof of Work algorithm in its current form has few vulnerabilities like Selfish mining attack, Eclipse attack, 51% attack, Scalability, Electricity dependency, and wastage. An attacker may use these techniques to break through system. So, there is a huge scope to improve this algorithm by using some techniques and modifications or using it in combination with other algorithms PoS (Proof of Stake) etc.

The traditional PoW accounts for about 90% of the total market in digital cryptocurrencies [35], as well as dominating the Blockchain based applications. In spite of its merits and wide utilize in practice, the conventional PoW also has been appeared to be greatly energy-expensive. An enormous chunk of this electricity utilization is due to the computational inefficiency of conventional PoW algorithms. This serious energy waste is considered one of the greatest drawbacks of traditional PoW algorithm.

Eclipse attacks are an extraordinary sort of cyberattack where an attacker makes a fake environment around one node, or client, which permits the attacker to control the affected node into wrongful activity [36].

3.2 Proof of Stake

As a result, the Proof of Stake (PoS) consensus algorithm can be used to implement a variety of system procedures found which are advantageous to the product it is used in to deliver security and trust.

This is gathered and handed to the entity that will create the new block. Finally, the impracticality of the 51% attack: in order to launch an attack, the attacker must have or have 51% of the stake in the cryptographic system in the network, which will cost the attacker a toll and, as a result, will be rather expensive for him. Decentralization is the primary benefit or use of existing PoS systems.

Some may call it as an advantage and some may call it as a disadvantage for the system. But it will be verified in the coming years. Explaining it, it says that the validator with massive amount of stake or more positive reviews will get the first preference while validating a block over some validators who are not as experienced as the above validator. The positives of this are that the system will generate a verified block and trust will be high if the validator with more positive reviews and experience has verified the block in the process. But, in the negative side it will make more hard for the new validators to be in the process as the above validator will get all the necessary means for validating a block in the process.

3.3 Proof of Elapsed Time

Since PoET (Proof of Elapsed Time) uses Intel SGX as a TEE, an attacker that can corrupt a single SGX-enabled node can win every consensus round and break the system completely. So, there is a huge scope to improve this algorithm by using it in combination with other algorithms PoUW (Proof of Useful Work), PoS (Proof of Stake), etc., or by modifying the existing algorithm.

The stale block will happen at whatever point the briefest stand-by time and another stand-by time contrast by not exactly the engendering deferral of the network. This outcome in reduction of network throughput fundamentally as the network size increments, different variables held steady.

3.4 Byzantine Fault Tolerance

BFT has some definite limitations.

1. Scalability.
2. Election of trusted primary/leader node.
3. Fault Tolerance.

Some modified algorithms solve its scalability issue and some make the election of leader node/nodes much efficient. No improvement in existing BFT completely removes its limitations. So, there lies a scope to find a modified BFT algorithm which improves its limitations.

A multi layered PBFT approach can be followed to improve scalability. Fault tolerance can be increased by reducing client communication from $f+1$ to 1. A reputation-based approach can be followed to nominate a leader node. Excess servers can be maintained for better resilience and performance.

4 Conclusion

The blocks in the Blockchain are linked together using a cryptographic hash value. Nodes in the blockchain system are protected from attack by the consensus protocol, which also maintains the integrity of the network. It's no secret that Blockchain consensus protocols have been the subject of many different ideas. Focusing on Blockchain, this study presents a comprehensive examination of prior forms of distributed ledgers. A more reliable, scalable, and cost-effective network can be created by leveraging the permissioned, permission-less, and consortium Blockchain consensus protocols.

References

1. S. Masseport, B. Darties, R. Giroudeau, J. Lartigau, Proof of experience: empowering proof of work protocol with miner previous work, in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (IEEE, 2020), pp. 57–58
2. K. Zheng, S. Zhang, X. Ma, Difficulty prediction for proof-of-work based blockchains, in *2020 IEEE 21st international Workshop on Signal Processing Advances in Wireless Communications (SPAWC)* (IEEE, 2020), pp. 1–5
3. R. Nakahara, H. Inaba, Proposal of fair proof-of-work system based on rating of user's computing power, in *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)* (IEEE, 2018), pp. 746–748
4. N. Gavrilovic, V. Ciric, Design and evaluation of proof of work based anti-spam solution, in *2020 Zooming Innovation in Consumer Technologies Conference (ZINC)* (IEEE, 2020), pp. 286–289
5. S.S. Hazari, Q.H. Mahmoud, A parallel proof of work to improve transaction speed and scalability in blockchain systems, in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (IEEE, 2019), pp. 0916–0921
6. P.R. Yogesh, Backtracking tool root-tracker to identify true source of cyber crime. Proc. Comput. Sci. **171**, 1120–1128 (2020)
7. Z. Feng, Q. Luo, Evaluating memory-hard proof-of-work algorithms on three processors. Proc. VLDB Endow. **13**(6), 898–991 (2020)
8. H. Alsabah, A. Capponi, Pitfalls of bitcoin's proof-of-work: R&D arms race and mining centralization. Available at SSRN 3273982 (2020)
9. E.U.A. Seyitoglu, A.A. Yavuz, T. Hoang, Proof-of-useful-randomness: mitigating the energy waste in blockchain proof-of-work (2021)
10. S.R. Niya et al., Adaptation of proof-of-stake-based blockchains for IoT data streams, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE, 2019)
11. G. Pattewar, N. Mahamuni, H. Nikam, O. Loka, R. Patil, Management of IoT devices security using blockchain—a review, in *Sentimental Analysis and Deep Learning*, pp. 735–743 (2022)
12. N. Nair, A.K. Dalal, A. Chhabra, N. Giri, Edu-coin: a proof of stake implementation of a decentralized skill validation application, in *2019 International Conference on Nascent Technologies in Engineering (ICNTE)* (IEEE, 2019), pp. 1–4
13. D. Tosh et al., CloudPoS: a proof-of-stake consensus design for blockchain integrated cloud, in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (IEEE, 2018)
14. S. Leonardos, D. Reijsbergen, G. Piliouras, Weighted voting on the blockchain: improving consensus in proof of stake protocols. Int. J. Network Manage. **30**(5), e2093 (2020)
15. P. Gaži, A. Kiayias, A. Russell, Stake-bleeding attacks on proof-of-stake blockchains, in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (IEEE, 2018)
16. S. Deore, R. Bachche, A. Bichave, R. Patil, Review on applications of blockchain for electronic health records systems, in *International Conference on Image Processing and Capsule Networks* (Springer, Cham, 2021), pp. 609–616
17. A. Pal, K. Kant, DC-PoET: proof-of-elapsed-time consensus with distributed coordination for blockchain networks, in *2021 IFIP Networking Conference (IFIP Networking)* (IEEE, 2021), pp. 1–9
18. L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, On security analysis of proof-of-elapsed-time (PoET), in *International Symposium on Stabilization, Safety, and Security of Distributed Systems* (Springer, Cham, 2018), pp. 282–297
19. R.Y. Patil, M.A. Ranjanikar, A new network forensic investigation process model, in *Mobile Computing and Sustainable Informatics* (Springer, Singapore, 2022), pp. 139–146
20. F. Zhang, I. Eyal, R. Escriva, A. Juels, R. Van Renesse, {REM}: resource-efficient mining for blockchains, in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pp. 1427–1444 (2017)
21. A. Corso, Performance analysis of proof-of-elapsed-time (PoET) consensus in the sawtooth blockchain framework, Doctoral dissertation, University of Oregon, 2019

22. B. Ampel, M. Patton, H. Chen, Performance modeling of hyperledger sawtooth blockchain, in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)* (IEEE, 2019), pp. 59–61
23. V. Costan, S. Devadas, Intel SGX explained. IACR Cryptol. ePrint Arch. **2016**(86), 1–118 (2016)
24. C. Saraf, S. Sabadra, Blockchain platforms: a compendium, in *2018 IEEE International Conference on Innovative Research and Development (ICIRD)* (IEEE, 2018), pp. 1–6
25. G.T. Nguyen, K. Kim, A survey about consensus algorithms used in blockchain. J. Inf. Process. Syst. **14**(1), 101–128 (2018)
26. X. Zheng, W. Feng, Research on practical byzantine fault tolerant consensus algorithm based on blockchain. J. Phys: Conf. Ser. **1802**, 032022 (2021). https://doi.org/10.1088/1742-6596/1802/3/032022
27. W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, M.A. Imran, A scalable multi-layer PBFT consensus for blockchain. IEEE Trans. Parallel Distrib. Syst. **32**(5), 1146–1160 (2021). https://doi.org/10.1109/TPDS.2020.3042392
28. K. Lei, Q. Zhang, L. Xu, Z. Qi, Reputation-based byzantine fault-tolerance for consortium blockchain 604–611 (2018)
29. J. Seo, D. Ko, S. Kim, S. Park, A coordination technique for improving scalability of byzantine fault-tolerant consensus. Appl. Sci. **10**(21), 7609 (2020)
30. Y.-A. Min, The modification of pBFT algorithm to increase network operations efficiency in private blockchains. Appl. Sci. **11**, 6313 (2021). https://doi.org/10.3390/app111463131
31. G. Golan Gueta et al., SBFT: a scalable and decentralized trust infrastructure, in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 568–580 (2019). https://doi.org/10.1109/DSN.2019.00063
32. H. Samy, A. Tammam, A. Fahmy, B. Hasan, Enhancing the performance of the blockchain consensus algorithm using multithreading technology. Ain Shams Eng. J. (2021)
33. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun, A review on consensus algorithm of blockchain, in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2567–2572 (2017). https://doi.org/10.1109/SMC.2017.8123011
34. M. Krstić, L. Krstić, Hyperledger frameworks with a special focus on hyperledger fabric. Vojnotehnicki glasnik **68**, 639–663 (2020). https://doi.org/10.5937/vojtehg68-26206
35. R.Y. Patil, S.R. Devane, Network forensic investigation protocol to identify true origin of cyber crime. J. King Saud Univ. Comput. Inf. Sci. (2019)
36. D. Sivaganesan, Performance estimation of sustainable smart farming with blockchain technology. IRO J. Sustain. Wirel. Syst. **3**(2), 97–106 (2021)