How to Cite:
Kanagasankari, S., & Vallinayagi, V. (2022). A comparative analysis of consensus algorithms in the health care sector using block chain technology. *International Journal of Health Sciences*, *6*(S1), 11702–11716. https://doi.org/10.53730/ijhs.v6nS1.7863

A comparative analysis of consensus algorithms in the health care sector using block chain technology

S. Kanagasankari
Research Scholar, Registration No: 21111262282001, Department of Computer Science, Sri Sarada College for Women (Autonomous), Tirunelveli-627011, Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012, Tamil Nadu, India
Email: Kanagasankari1975@gmail.com

Dr. V. Vallinayagi
Research Head & Associate Professor, Department of Computer Science, Sri Sarada College for Women (Autonomous), Tirunelveli-627011, Tamil Nadu, India
Email: vallinayagimahesh@gmail.com

***Abstract*---**As Blockchain is a distributed digital ledger system, it focuses on various sectors such as bitcoin, the banking sector, the corporation sector, the real estate and the healthcare sector. Each block in the blockchain contains the hash value, timestamp and transaction data of their previous block. The consensus algorithms plays a major role in the blockchain framework. This consensus algorithm maintaining the safety and efficacy of blockchain. The consensus protocols determines how the agreement to add the updated block to all nodes in the network works. Every consensus protocols has its own set of performance and scalability features. It is essential to technically compare each consensus mechanism by highlighting their strengths and weaknesses. Consensus algorithms in blockchain can be divided into two types. They are Proof based consensus and voting based consensus. The Proof based consensus shows that they are more qualified than others to do mining work. Voting-based consensus explains that nodes are needed in a blockchain network to exchange decisions for mining a new block or transaction before reaching a final conclusion. Their effectiveness can be enhanced by manipulating the suitable consensus algorithm in the blockchain. Blockchain technology is recently implement in many domains, especially for healthcare Industry. In this review article outlines some of the consensus algorithms needed for the healthcare sector. First we explain an overview on blockchain technology, blockchain architecture, and classification of blockchain and challenges of blockchain in healthcare sector. Next, we have

elaborated on the various consensus protocols applicable to the health sector. Finally, we have analyze and discussed the performance, throughput and scalability of consensus protocols in the healthcare sector.

***Keywords*---**Blockchain, Consensus, Healthcare, Proof-based Consensus, Voting-based Consensus.

Introduction

Transactions made in blockchain technology are called as blocks. In many databases this is also called a chain. This block is stored on a network by peer-to-peer nodes. The area where the block is stored is referred to as the digital ledger. Blockchain technology is a decentralized technology. It is a ledger distributed through the ends connected to the chain. Blockchain is often used in many industries because of its open source, decentralized, immutable, autonomy, transparent and anonymity parameters [Asad Ali Siyal et al., 2019].Blockchain technology has been required for a wide range of security features such as managing e-data generated by the Healthcare sector, Banking Services and Cybercrime. Transactional cost, performance and security issues can be addressed through decentralization within blockchain. All the nodes in the blockchain are equal rank. These nodes reach a consensus by pursuing a policy of majority domination using pre-agreement of rules [Du Mingxiao et al., 2017].

What is Blockchain?

Blockchain is a basically a peer-to-peer network transaction system. It provides secure functionality without the need for reliable third parties. All transactions are made on a decentralized ledger database shared between multiple nodes that make up the blockchain network. Each time a new transaction occurs on the blockchain, the record of that transaction is added to each participant's ledger. Distributed database managed by several contributors is known as Distributed Ledger Technology (DLT). Transactions on the blockchain are recorded with an immutable cryptographic signature called a hash [Bikramaditya Singhal et al., 2018].

Blockchain Architecture

There is no centralized information in the blockchain architecture. It's really impossible to hack a blockchain. The blockchain architecture supports a growing list of ordered records called block. Each and every block carries a timestamp and a link to the previous block.

- *Node* - the computer that presents in the blockchain architecture. Each blockchain node contain independent copy of the entire blockchain ledger.
- *Transaction* - Database verified by blockchain participants. It acts as a constant guarantee of financial transaction or smart contract.
- *Blocks*-Transactions made in blockchain technology
- *Chain* — A ordered of blocks.

- *Miners* — Nodes that check blocks before adding them to the blockchain architecture.
- *Consensus* — A set of rules and agreements for performing blockchain operations.

How Blockchain works?

The initial transaction is called as genesis block. This transaction is stored in first block of the chain. Other transactions are checked for two reasons, before being accepted. One is verification done by some other node in the same chain. Another one is digital signature of the sender. To complete the copying process it will be linked to a valid transaction block and distributed to other nodes. Making transactions in this way can cause some confusion if each node tries to broadcast its blocks updates. In order to avoid this state, an agreement must be reached between the nodes to determine which block will be connected and through which node, using a consensus algorithm [Bela Shrimali et al., 2021].

Importance of Consensus

Reliable blockchain networks immune from two problems. One is double spending problem and another one is byzantine generals. However, if the attacker is able to gain 51% of the network power, these issues can successfully destroy the blockchain network. Therefore, the consensus algorithm should be carefully designed to avoid such an attacks.

Challenges

There are some issues and challenges faced by Blockchain technology [Ahmed Afif Monrat et al., 2019]. To meet these challenges, we more concentrate to improve the consensus algorithms that are the basis of Blockchain technology.

- *Scalability:* The system is not yet able to accommodate a large-number of users at once.
- *Security*: 51% of attacks on the network are one of the security vulnerabilities of the network.
- *Energy Consumption*: The amount of energy consumption are wasted during the mining process in blockchain.

Classification of Blockchain

The blockchain classified into the depending on the generally managed data, the availability of such data and what actions the user can take. These include:

- Public
- Private
- Consortium

Public, Private and Consortium Blockchain

A public blockchain is an unrestricted, permissionless distributed ledger system. Anyone with Internet access can log in to this blockchain platform and become

part of the blockchain network by becoming an authorized node. It is usable for mining and exchanging crypto currencies. Consensus practices such as Proof of Work, Proof of Stake and Delegated Proof of Stake etc. are used in the public and decentralized blockchain network [Leila Ismail et al., 2019]. However, there are two other categories of blockchain they are private blockchain and consortium blockchain. A private blockchain is controlled by centralized network. This Private Blockchain determines who can interact with blockchain and who can view recorded information. Private Blockchain is an authorized system that operates only on a closed network. These are usually used only within an organization or organization. Only register members will participate in the Private Blockchain network. Private Blockchain are in use as a public blockchain. But these are small and have a limited network [Marko Hölbl et al., 2018].A federation blockchain is a distributed ledger controlled by several entities. Each node operate the network node and also each node participates in the consensus Private and consortium blockchain are used by organizations that aim to use the blockchain framework. The Consortium blockchain are used in a variety of key sectors including healthcare, insurance and financial departments. These have not been done equally because blockchain themselves have different implications for different consensus mechanisms, accessibility, security and sustainability. Not all blockchain types apply equally to every application case. Although public blockchain are safe, they do not fit well with the company because of their transparency. Table 1 shows the classification of public, private and consortium types of blockchain characteristics.

Table 1

Comparison of public, private and consortium blockchain characteristics

Attributes	Public	Private	Consortium
Consensus Process	Permissionless	Permissioned	permissioned
Consensus persistence	Independent Organization	Single Organization	Group of Organization
Centralized & Decentralized	Decentralized	Centralized	Decentralized
Types of consensus	Proof-based	Voting-based	Voting-based
Consensus Algorithms	Pow, PoS, DPoS, PoI, LpoS	PoET, PBFT	PBFT, PoS, Stellar, RAFT, Tendermint, Ripple
Energy Consumption	High	Low	Low
Use Cases	Cryptocurrency	Supply chain	Healthcare

Blockchain in Healthcare Sector

Blockchain technology can be used to manage patient electronic data and sharing their data. Data sharing is an essential for updating clinical data for rapid follow-up. Further through data exchange and data sharing patients are remotely

identified and referred to them by appropriate physicians [Arlindo F et al., 2018]. Consensus protocols in blockchain have been used in the healthcare industry for the past few years as an application for providing electronic health data related to patient safety. The private type of blockchain is based on a relatively closed environment where node identities are known. Private Blockchain solves complex applications more efficiently than the public blockchain based consensus mechanism because of the distributed consensus algorithm and smart contract [Yue Hao et al., 2018]. The consensus mechanism in the distributed system can resolve the node trust and problems on the principle of decentralization. This consensus algorithm achieves a balanced position on the block chain network nodes. This consensus mechanism in the blockchain technology structure has a direct impact on the overall performance of blockchain as the main mechanism of blockchain. Figure1 shows how the consensus protocol works in blockchain. The network admin provides sensitive e-data with patient consent to healthcare providers. Then the e-data of the recommended patient is transmitted on a decentralized P2P network with multi-node. When a transaction takes place between two nodes, the other nodes will check the transaction with some kind of proof or voting based algorithm. Then a new block is created and authenticated by all consensus nodes in the network. Finally, the new block is created and the existing blockchain is added.

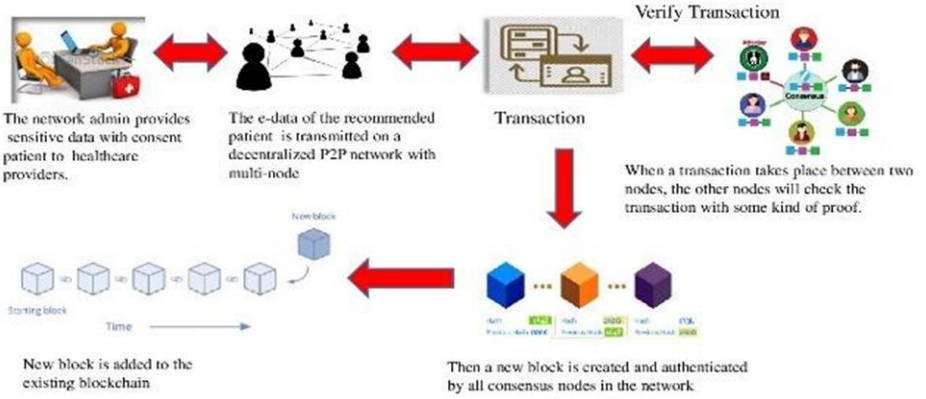

Fig1-Blockchain Consensus Mechanism

Blockchain Consensus Algorithm in Healthcare Industry

Consensus mechanisms permit distributed systems to work together and remain secure. According to a crypto-economic system, a consensus mechanism is used to prevent certain types of economic attacks. By dealing with consensus the attacker can control 51% of the network. Consensus mechanisms are designed to make "51% attack" unviable. Different mechanisms are designed to fix this security problem.

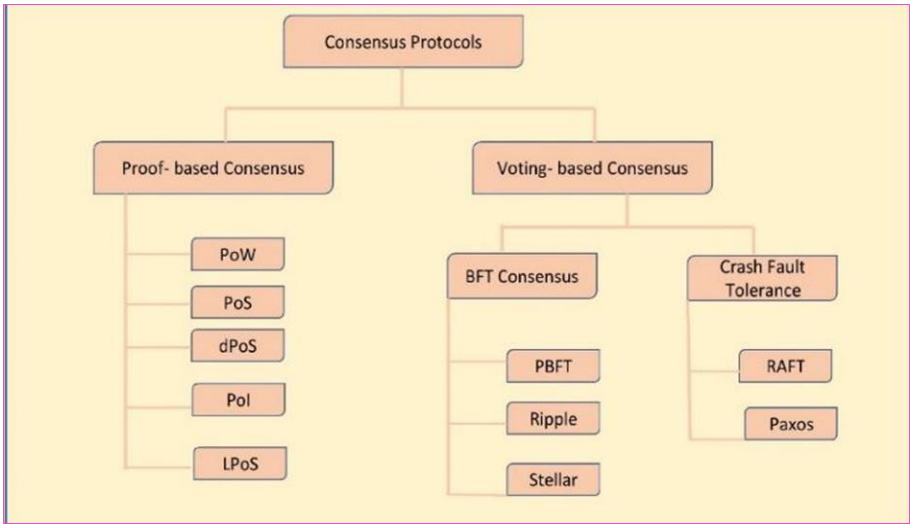

Fig-2 Recent Development of Consensus Protocols for Blockchain

Because there is a consensus protocol in blockchain, every transaction is considered to be completely secure, reliable and good framework. Consensus algorithm is a method by which all peers in the blockchain network reach a consensus on the current state of the distributed ledger. In this way blockchain networks gain reliability. Each new block added to the blockchain by consensus protocol ensures that a version of the trust accepted by all nodes in the blockchain. Consensus mechanism work individual for each domain. Some domains require less computational power, while others require quick transaction. The consensus method describes the method required to achieve total agreement between network nodes during the block verification process. This consensus mechanism aims to provide mining equality. If all nodes in the blockchain network provide the same output, that consensus protocol is defined as secure and valid according to the publishing rules. This is also called the stability of the shared state. A consensus protocol ensures real- time liveliness. All the right nodes participating in consensus process will eventually create a value .Blockchain technology uses only one of the most common consensus algorithms, for example, it uses one of the consensus mechanisms, such as Proof of Work, Proof of Stake or Delegated Proof of Stake. All of these mechanisms are aimed at ensuring that participant's dispose of identical copies of distributed database files .Some selected consensus methods used in the public, private and consortium blockchain are illustrated. These consensus protocols are widely used in the healthcare sector to protect patients' e-data and resolve issues [Partha Pratim Ray et al.,2021]. In blockchain consensus algorithms are divided into two main components: one is proof-based consensus algorithm and another one is voting-based consensus algorithm [Sunny Pahlajani et al., 2019].Figure2 illustrates the recent development of consensus protocols for blockchain.

Proof based Consensus Algorithm

Various consensus practices such as Proof of Work, Proof of Stake and Delegated Proof of Stake are used in the public and decentralized blockchain network. The prototype work of consensus algorithm PoW is proposed by Nakamoto. Till date so many proof- based algorithms have been proposed. PoW, PoS are the basis for other consensus algorithms. The basic premise of the proof-based consensus algorithm is to acquire the right to add a new block to the node chain that creates enough resource at multiple nodes joining the network [Giang-Truong Nguyen et al., 2018].

Proof of Work

The Proof of Work consensus algorithm is the most commonly used consensus method. This mechanism solving a computationally challenging problem in order to create new blocks. The problem is solving by approximating the value for nonce [Zibin Zheng et al., 2017]. It is added into the hash module. The difficulty level is met during further reviewing. If a miner finds a solution, the miner creates a block and broadcasts the nonce to the network, finalizing block. Evidence of working using a consensus protocol verifies each transaction. Thus, the blockchain network protects the transaction against double- spending mechanism. Transactions are finalized and approved by the miners after confirmation. If someone tries to copy a transaction it will show that it is counterfeit on the network and it will not be accepted. You cannot spend twice, with a transaction approved. The PoW consensus protocol is widely used in the public types of blockchain network. Opportunities for the use of PoW consensus protocol in the healthcare sector are moderate [Partha Pratim Ray et al., 2021].

Proof of Stake

Proof of Stake divides users into blockchain shares. Each node may be a miner holding a certain number of shares of blockchain. The Proof of Stake assumes that the user with more stake is less likely to hit the network. Each node assigns a certain amount of their stakes when they become miners. The network will hold that amount to ensure that the user is trustworthy. Low computational power is sufficient for this consensus algorithm. Proof of Stake has minimal energy consumption compared to Proof of Work. The Proof of Stake does not trigger a flow between the nodes to solve the next block. Instead of a competition between the nodes to solve the next block, a node Proof of Stake helps to select a node by lottery. The speed of block formation and transaction confirmation is usually very fast as only one block is made in each round of PoS mechanisms. In PoS 51% attack is virtually impossible [M. Bartoletti, S. Lande et al., 2017]. It contains low to moderate energy consumption.so that, in public types of blockchain network we propose POS mechanism could be used as a best solution to apply for e-healthcare sectors [Haider Dhia Zubaydi et al., 2019] Mehrdad Salimitari et al., 2019].

Delegated PoS

Delegated Proof of Stake is the popular evolution of the Proof of Stake concept whereby users of the Internet to select representatives to verify the next block. Those who have too many tokens in this mechanism do not have the authority to confirm or verify transactions [YuanyuanSun et al., 2021]. All token owners select a group of delegation to perform this task. The advantage of the centralized feature of DPoS over the mechanism of PoS is that the scalability is higher as the rate of verification and transaction is higher. This makes quick transaction, but costs more to centralize. There is a protocol for detecting and votingfor a malicious representative it consumes significantly less energy than PoW. Further, this mechanism can handle a higher number of transactions compared to Proof of Work mechanism. Due to its stake-weighted voting system, DPoS is often considered as a digital democracy. We can use it to manage patient sensitive data as it handles less energy consumption and huge number of transactions.

Voting- based Consensus Algorithm

The consensus mechanism of voting-based is desirable in the private blockchain where the nodes are known. Before appending a block to a blockchain, the results must be exchanged on the network through a vote-based consensus mechanism. To implement a voting-based consensus algorithm, the nodes in the verification network must be familiar and adaptable. Thus, they can exchange the message easily. This is the main difference between the proof-based and voting-based consensus algorithms. In a voting-based consensus algorithm, all nodes in the network, except maintaining the ledger, must verify transactions or blocks together. They will interact with others before they decide to add the proposed blocks to their chain [Sunny Pahlajani et al., 2019]. Consensus mechanism based on voting can be classified into two types.

- Byzantine fault tolerance-based consensus: crashing nodes and subverted nodes.
- Crash fault tolerance-based consensus: crashing nodes

Byzantine Fault Tolerance

Byzantine Fault Tolerance is considered as a feature of a distributed network to achieve consensus even if certain nodes in the network fail to respond or respond with incorrect information. The main purpose of Byzantine fault tolerance is to protect against influence of the faulty nodes through the use of collective decision making. It is derived from Byzantine Generals Problem.

Practical Byzantine Fault Tolerance

Practical Byzantine fault tolerance proposed by Castro and Liskov is used for Hyperledger Fabric. PBFT voting- based consensus algorithm contains are two kinds of nodes. One is leader node, the other is some validating peers. These peers will activate some rounds in the chain to add a block. Customers initially send transaction requests to their respective verification peers. Peer transactions

received from those are forwarded to other peers, including the leader. Once the number of transactions reaches a threshold called the batch size, the leader node will order the transactions according to the time they created and place them as a block. Then there are three phases in PBFT are executed. First in the pre-production phase the leader will send his proposed block to other peers. Then next in the preparation phase and the commit phase they double check to make sure it is the block received from the leader. If any node receives the blocks, after the preparation phase they will be the same as those stored locally. In this method, all the nodes have to participate in the voting process. In order to add the next block, two-thirds of the nodes may reach a consensus when agreeing to that block. The secure, immutable and trustless network of blockchain parameters can procedure PBFT mechanism to fragment the systems and generate better insights, improve efficiency and support. We propose that this would be very useful for the e-healthcare sector as it has low tolerance against malicious nodes [Sivleen Kaur et al., 2021]. This consensus protocol enables transaction requests at high speed, but the resulting overhead of communications restricts their scalability [Shikah J. Alsunaidi et al., 2019] [M. Vukolić et al., 2016].

Stellar Consensus Protocol

The Stellar Consensus Protocol is the popular evolution of PBFT. It contains two steps. The First one is nomination protocol next one is ballot protocol. This consensus mechanism provides micro finance services on the blockchain platform. In initial stage, nomination protocol is executed. During this stage, new values called candidate values are proposed in the agreement. These values are sent to all the nodes in the quorum and each of them will vote for one of the candidate values. Next, ballot protocol is initiated. This ballot protocol involves a federated voting to either accept or abort the obtained values in the nomination protocol. Finally, voting for the current slot is finalized and aborted ballots are discarded. In the stellar consensus protocol differs from other blockchain platforms. Stellar consensus method eliminates need to rely on the entire mining system to verify transactions. Stellar achieves a transaction processing time of about 3 to 5 seconds and increase the speed of network operations by approx. 1000 per second. So that, this mechanism is very helpful for the healthcare sector due to transaction time and speed of network operations.

Ripple

Ripple was proposed to solve the problem of light delays caused by synchronous communication between nodes. In this decentralized system, every miner uses a subset network at trusted nodes in a large network to achieve consensus. There are two kinds nodes in a network. The first one is server node and the other one is customer node. The server node is responsible for the consensus protocol. The customer node has the ability to convert only funds. Each server has a unique node list. There is a UNL (Uniform Node List) within each server. When determining whether to place the transaction on the ledger, the server queries the nodes in the UNL. When 80% of the nodes in the UNL agree to a transaction,

consensus is reached. For a node, the ledger will endure correct as long as the faulty nodes in UNL is less than 20% [Zibin Zheng et al., 2017].

Crash Fault Tolerance

Crash Fault Tolerance (CFT) can be a good solution when any one component of the system fails. There may be different organizations, divisions or groups that control the individual components of the system. These may have different goals. CFT cannot reach a consensus if any company acts maliciously.

Paxos

Paxos algorithm solves the problem of uniformity in a good way. The main goal of this algorithm is to select a single value in the network fault. In this the nodes of the network are divided into three types. They are proposers, acceptors and the learners. Everyone who learns the consensus value in the network, is a learner. Initially, the proposer develops a proposal number plan with the proposal. This proposal number know a prepare message and send to the acceptors. Each acceptor compares the currently received proposal number value with the proposal number of all the proposers and accepts the proposal if the number currently received proposal number is higher than the number received then it accepts the proposal otherwise drops it. Next a vote is being held based on the majority decision. The proposer checks the rejection of the proposal by a majority of the acceptors. If this is true, the proposer will update this number with the up-to-date proposal number. Otherwise, the proposer further checks whether the majority of the acceptors have already accepted the values. If it is true the proposer value cannot be accepted. Otherwise, the proposer sends the accepted message [Vishal sharma et al., 2020].

RAFT

In the RAFT algorithm, each node is assigned states such as leader, candidate and follower. This algorithm, which is proposed to manage copied records, plays a strong role in the network. The leader node is responsible for ordering transactions. RAFT does not create a block without transactions. Thus, it differs from other consensus methods. Leader node is selected by voting rules. If the existing leader fails, the leader selector performs a random timeout for each server. One or more candidate nodes are trying to become a leader. If a candidate node receives a majority of votes the nominee will serve as a leader until it expires [Anastasios Alexandridis et al., 2021]. RAFT is suitable algorithm for private/consortium blockchain. This algorithm improves the level of security through constant changes for members as a service. While their protocols are similar to BFT algorithms, only up to 50% of crash faults can be tolerated [Mehrdad Salimitari et al.,2019] [Mohammad Dabbagh et al., 2021].This algorithm is suited in real life implementation and comprehension.

Analysis and Discussion of Various Consensus Algorithm

Consensus algorithms plays a key role in the implementation of blockchain. The consensus protocols mentioned above are used in various blockchain implementation. The comparison of consensus protocols discussed above in terms of performance is in table2.In this table2 shows all the above consensus protocols mentioned are compared to check the compatibility of the healthcare sector.

Node Identity

The proposed consensus algorithms such as PBFT, and Raft mentioned above should verify the identity of the nodes participating in the mining process. These consensus algorithms are suited for the private or consortium Blockchain networks. Algorithms like PoW, PoS and DPoS, Stellar and Ripple are more suitable for public blockchain network, because the nodes are join the networks freely.

Mining Capability

The key point in the blockchain is the mining method used. The mining system has a significant impact on power consumption, performance and security. PoW mine solves the difficult puzzle. It increase network security, but consumes a lot of computing power. So that this algorithm works is very less. The mining process in PBFT depends on the transmission of multiple broadcast messages between nodes that overhead network communications [Shikah J. Alsunaidi et al., 2019].

Energy Consumption

The most energy consuming algorithm is PoW. Selecting a miner in this way depends on the speed at which we solve the puzzle. For that you need to do subsequent calculations to get the target hash value. As a result, a certain amount of electrical energy is consumed. But PoS, DPoS have use them less electrical energy consumption compared to PoW. Because amount of calculations is lower. Algorithms that do not perform mining functions such as PBFT and RAFT significantly conserve electrical energy.

Performance, Throughput and Scalability
When considering any of the consensus protocol for blockchain in healthcare, network performance, transaction throughput and scalability should be considered.
• *Performance*
Performance is the measurement of the amount of data that moves from one end point to another. Networking performance and bandwidth are calculated based on the distribution level of the consensus nodes in the blockchain. Performance for a private consortium platform can be in the thousands of blocks per second. The healthcare sector data used in blockchain limited. Measurements will vary based on data in the healthcare industry. Collections

containing EHR and patient clinical data contain large amounts of data. During each transaction, performance may decrease as new blocks are added. Excluding large data such as diagnoses, medications and images, specifications and only adding their data sets can help keep performance consistent.

- *Throughput*

All consensus algorithms express transaction throughput based on the blocks added to the blockchain per second. This transaction throughput depends on the consensus algorithm that applies. This leads to confirmation of the validity of the transaction and also it specifies how the nodes interact and the stability of each copy of the shared ledger. The amount of e-data provided by the design, scope and healthcare sector these are all the important factors affecting transaction performance. Current data trends focus on providing what healthcare providers need.

- *Scalability*

Blockchain's are great with light weight Meta data, source and transaction information. The data for each confirmed block should be reflected at each node. Each node stores a complete copy of the shared ledger, it represents the sum of all the data in all blocks from the beginning of the chain. The scalability is always consideration in software implementation. The ability to rearrange all the information collected will be challenging, as it grows. So, starting with the right dataset from the beginning will improve the measuring ability. Prototype design is required for the performance, throughput and scalability of blockchain technology. It's having clear solution to the problem and shape the elements such as what information which stakeholders needs to solve the problem.

Table 2
Different Consensus Algorithm Performance

Consensus Algorithms	Accessibility	Scalability	Throughput	Latency	Energy Consumption	Healthcare Sector aptness
PoW	Public	Strong	Weak	Strong	Strong	Moderate
PoS	Public & Private	Strong	Weak	Moderate	Less than PoW	Strong
DPoS	Public & Private	Strong	Strong	Moderate	Weak	Moderate
PBFT	Private	Weak	Strong	Weak	Moderate	Strong
Stellar	Public	Strong	Strong	Moderate	N/F	Moderate
Ripple	Public	Strong	Strong	Moderate	N/F	Moderate
RAFT	Private & Consortium	Moderate	Strong	Weak	Strong	Strong

*NA-Not Found

Conclusion

Blockchain technology would be a great solution to the problems facing the health care sector such as the lack of patient-centered proper approaches, the inability to integrate diverse systems, maintenance and protection of sensitive patient's medical data. The excellent framework in the blockchain technology

enables the healthcare sector to improve. Blockchain technology solves the following problems faced by the healthcare industry, such as providing patient's electronic data to other stakeholders in the network without their consent, unregistered medical services and data errors. These systems are very dominant in creating a consensus algorithm in the blockchain. We can innovate in blockchain by creating variations in processes and new technologies. The consensus protocols in blockchain varies according to the organization and their computational speed, performance and patient electronic data safety. Each of these consensus protocols differs in dealing with attacks. According to this study, a systematic review has been conducted on the various consensus algorithm required for the healthcare sector.

Declarations of competing interest

The authors declare no conflict of interests.

Acknowledgements

We would like to thank the reviewers for their precious comment.

References

Asad Ali Siyal., Aisha Zahid Junejo.,Muhammad., Zawish.,Kainat Ahmed., Aiman Khalil., & Georgia Soursou (2019). Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. *Cryptography, 3*(1), 3; https://doi.org/10.3390/cryptography3010003.

Du Mingxiao., Ma Xiaofeng., Zhang Zhe., Wang Xiangwei., & Chen Qijun (2017). A review on consensus algorithm of blockchain. IEEE, pp.2567-2572, https://doi.org/10.1109/SMC.2017.8123011

Bikramaditya Singhal., Gautam Dhameja., & Priyansu Sekhar Panda (2018).Beginning blockchain: a beginner's guide to building blockchain solutions. ISBN: 9781484234440, Apress, Berkeley, CA,.

Bela Shrimali., & Hiren B. Patel (2021). Blockchain state-of- the-art: architecture, use cases, consensus, challenges and opportunities. Journal of King Saud University-Computer and Information Sciences, In Press.,

Ahmed Afif Monrat., Olov Schelén., & Karl Andersson (2019).A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE, Vol.7, pp. 117134 – 117151, DOI: http://dx.doi.org/10.1109/ACCESS.2019.2936094.

Leila Ismail., & Huned Materwala (2019). A review of blockchain architecture and consensus protocols; use cases, challenges, and solutions, Symmetry, 11(10), 1198; https://doi.org/10.3390/sym11101198.

Marko Hölbl., Marko Kompara., Aida Kamišali´c., & Lili Nemec Zlatolas (2018). A systematic review of the use of blockchain in healthcare, *Symmetry, 10*(10), 470, : https://doi.org/10.3390/sym10100470.

Arlindo F. da Conceic¸ao., Flavio S. Correa da Silva., Vladimir Rocha., Angela Locoro., & Joao Marcos M. Barguil (2018).Electronic health records using blockchain technology. arXiv preprint arXiv:1804.10078.

Yue Hao., Yi Li., Xinghua Dong., Li Fang., & Ping Chen (2018).Performance analysis of consensus algorithm in private blockchain. IEEE, https://doi.org/10.1109/IVS.2018.8500557.

Partha Pratim Ray.,Dinesh Dash., Khaled Salah.,& Neeraj Kumar (2021).Blockchain for IOT- based healthcare: background, consensus,platforms,and use cases. IEEE,Vol.15, Issue: 1, pp.85-94, DOI: https://doi.org/10.1109/JSYST.2020.2963840.

Sunny Pahlajani., Avinash Kshirsagar., & Vinod Pachghare (2019). Survey on private blockchain consensus algorithms. IEEE, 1st International Conference on Innovations in Information and Communication Technology (ICIICT) DOI: 10.1109/ICIICT1.2019.8741353

Giang-Truong Nguyen.,& Kyungbaek Kim (2018).A survey about consensus algorithms used in blockchain. Journal of Information Processing Systems, Vol. 14, pp. 101-128., https://doi.org/10.3745/JIPS.01.0024

Zibin Zheng., Shaoan Xie., Hongning Dai., Xiangping Chen., & Huaimin Wang (2017). An overview of blockchain technology :architecture, consensus, and future trends. IEEE, 6th IEEE International Congress on Big Data, 10.1109/BigDataCongress.2017.85

M. Bartoletti., S. Lande., &A. S. Podda (2017).A proof-of-stake protocol for consensus on bitcoin subchains. International Conference on Financial cryptography and Data security, Springer, vol. 36, pp. 568–584., DOI: http://dx.doi.org/10.1007/978-3-319-70278-0_36

Haider Dhia Zubaydi., Yung-Wey Chong., Kwangman Ko., Sabri M. Hanshi., & ShankarKaruppayah (2019). A review on the role of blockchain technology in the healthcare domain. Electronics, 8(6), 679; DOI: https://doi.org/10.3390/electronics8060679

Mehrdad Salimitari., & Mainak Chatterjee (2019).A survey on consensus protocols in blockchain for IOT networks. Networking and Internet Architecture (cs.NI); Cryptography and Security (cs.CR), DOI: https://arxiv.org/abs/1809.05613v4

YuanyuanSun.,,BiweiYan., YanYao., & JiguoYu (2021).DT- DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. Elsevier, Vol.187, pp.371-376., DOI: https://doi.org/10.1016/j.procs.2021.04.113

Sivleen Kaur., Sheeta Chaturvedi., Aabha Sharma., & Jayaprakash Kar(2021).A research survey on applications of consensus protocols in blockchain. Security and communication networks, Vol.2021, DOI: https://doi.org/10.1155/2021/6693731

Shikah J. Alsunaidi., & Fahd A. Alhaidari(2019). A survey of consensus algorithms for blockchain technology. IEEE, International Conference on Computer and Information Sciences (ICCIS), DOI: https://doi.org/10.1109/ICCISci.2019.8716424

M. Vukolić (2016).The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. International Workshop on Open Problems in Network Security, Springer, pp.112–125.

Vishal sharma., & Niranjan lal (2020).A novel comparison of consensus algorithms in blockchain. Advances and Applications in Mathematical Sciences, Volume 20, Issue1,pp.1-13.

Anastasios Alexandridis., Ghassan Al-Sumaidaee., & Rami Alkhudary (2021).Making case or using raft in healthcare through hyperledger fabric. IEEE , 978-1-6654-3902-2/21/$31.00 ©2021

Mohammad Dabbagh., Kim-Kwang Raymond Choo., Amin Beheshti., Mohammad Tahir.,& Nader Sohrabi Safa (2021). A survey of empirical performance evaluation of permissioned blockchain platforms: challenges and opportunities. Elsevier, Vol.100, DOI: https://doi.org/10.1016/j.cose.2020.102078