OPEN ACCESS

International Journal of Innovations in Science & Technology

IJIST
P ISSN : 2618-1630
E ISSN : 2909-6130
Recognized Journal

Original Article

Critical Review of Blockchain Consensus Algorithms: challenges and opportunities

Muhammad Tahir[1], Muhammad Sardaraz[1*], Usman Aziz[1]

[1]Department of Computer Science, COMSATS University Islamabad, Attock Campus, Attock, Pakistan.

* **Correspondence:** Muhammad Sardaraz (sardaraz@cuiatk.edu.pk).

Citation | U. A. Muhammad Tahir, Muhammad Sardaraz, "Critical Review of Blockchain Consensus Algorithms: challenges and opportunities," Int. J. Innov. Sci. Technol., Special Issue pp. 52-64, 2022

Received | June 2, 2022; **Revised** |June 22, 2022; **Accepted** |June 28, 2022; **Published** |June 30, 2022.

DOI| https://doi.org/10.33411/IJIST/2022040505

Blockchain is a distributed ledger in which transactions are grouped in blocks linked by hash pointers. Blockchain-based solutions provide trust and privacy because of the resistance to the inconsistency of data and advanced cryptographic features. In various fields, blockchain technology has been implemented to ensure transparency, verifiability, interoperability, governance, and management of information systems. Processing large volumes of data being generated through emerging technologies is a big issue. Many researchers have used Blockchain in various fields integrated with IoT, i.e., industry 4.0, biomedical, health, genomics, etc. Blockchain has the attributes of decentralization, solidness, security, and immutability with a possibility to secure the system design for transmission and storage of data. The purpose of the consensus protocols is to keep up the security and effectiveness of the blockchain network. Utilizing the correct protocol enhances the performance of the blockchain applications. This article presents essential principles and attributes of consensus algorithms to show the applications, challenges, and opportunities of blockchain technology. Moreover, future research directions are also presented to choose an appropriate consensus algorithm to enhance the performance of Blockchain based applications

Keywords: Blockchain; consensus algorithms; performance evaluation; IoT; big data.

Acknowledgment.
We acknowledge that our work is not published by someone else. We would like to thank all our colleagues, and we are also thankful to all the authors who contributed to this research.

Conflict Of Interest:
The author(s) declare that the publication of this article has no conflict of interest.

Project details.
Nil

Author's Contribution. All of my co-authors contributed to this research in the form of data collection, write-up, and improvement.

Introduction

Blockchain is an emerging paradigm of distributed computing. The paradigm is revolutionizing lives from the transactions of money to the use of machines. Technology helps in proving one's identity. In the near future, Blockchain will bring more advancement in the field of computing technologies. Blockchain is a distributed database, shared and integrated among all contenders in a network. Blockchain technology has progressed in a variety of areas and is growing rapidly. Blockchain has many applications such as data exchange, record keeping, online access to data and data protection, etc. Moreover, it can be used in a variety of financial services, such as digital assets, wire transfers, and online payments, with the capability of payments without the involvement of intermediaries [1], [2]. The technology can also be applied to other areas, including smart contracts[3], utilities[4], Internet of Things (IoT)[5], reputation systems[6], security services[7], vehicular networks[7], and healthcare[7]. Thus, the research community has started to realize the potential of blockchain technology beyond financial applications.

Consensus is the key element of the Blockchain that ensures integrity among validators. For a Blockchain system, consensus algorithms guarantee that all nodes in the network agree on a consistent state of the Blockchain. Blockchain can be regarded as fundamental technology providing foundations for economics and businesses[8]. Blockchain can be defined as a ledger where information can be appended, offering an absolute decentralization[9], [10]. The information stored in this ledger cannot be changed, tampered with, or deleted. Blockchain networks are mainly discriminated against by their attributes to other networks. These attributes are tamper-resilience, transparency, open access, and disintermediation[11]. These attributes lay the foundation of numerous spotlight applications that need security and integrity of data[12], [13]. Blockchain mainly finds applications in Bitcoin, where the users are facilitated with the transactions of digital currency, and there is no need for a third party to validate these transactions. Blockchain is mainly categorized as public or permissioned[14]. As the names suggest, a public Blockchain is one where everyone can contribute to the network. But only a couple of processes may be excented in a second, thus reducing the efficiency and performance. In a permissioned Blockchain, only authorized or selected users can participate in appending the information in a blockchain, and they decide what information to be added. Permissioned Blockchain claims advantages over public Blockchain, like the capability to partition the segments where validation of a transaction is done by a specific group of nodes. Other merits are the trustworthiness of nodes, use of consensus algorithms, and promising far more throughput[15].

In this paper, we discuss the basic standards and qualities of the consensus protocols to demonstrate the applications and difficulties of different consensus algorithms. In addition, future research directions are also highlighted to select a suitable consensus protocol for the development of Blockchain-based systems.

Structure of Blockchain

Blockchain is referred to as a peer-to-peer network where transactions are shared and maintained by all peers. These peers are individuals or groups anywhere in the world. Blockchain promises the possibility of a dramatic reduction in the cost of transactions carried out. In Blockchain, the ledger is stored redundantly on several nodes in the network. If at one place a record or entry is modified, it must be modified in all copies on all nodes. When a transaction is done, all the values and assets are exchanged, and transactions are stored in a ledger permanently. There is no need for third parties to check and validate the data. If the transaction is shifted to Blockchain, the transaction can be carried out within seconds and is verified and secured autonomously. Figure 1 shows the simplified structure of Blockchain. A block in Blockchain contains a hash, hash of the previous block, data, timestamp, and other information. The nature of data in a block is dependent on the service of blockchain applications such as a record of a transaction, contract record, or record of IoT-related data. When a transaction is carried out, a code is hashed with that transaction and sent to every node. As there could be thousands or millions of transactions needed to be stored in a block of every node, for this purpose, a final hash value is issued using the Merkle tree function.

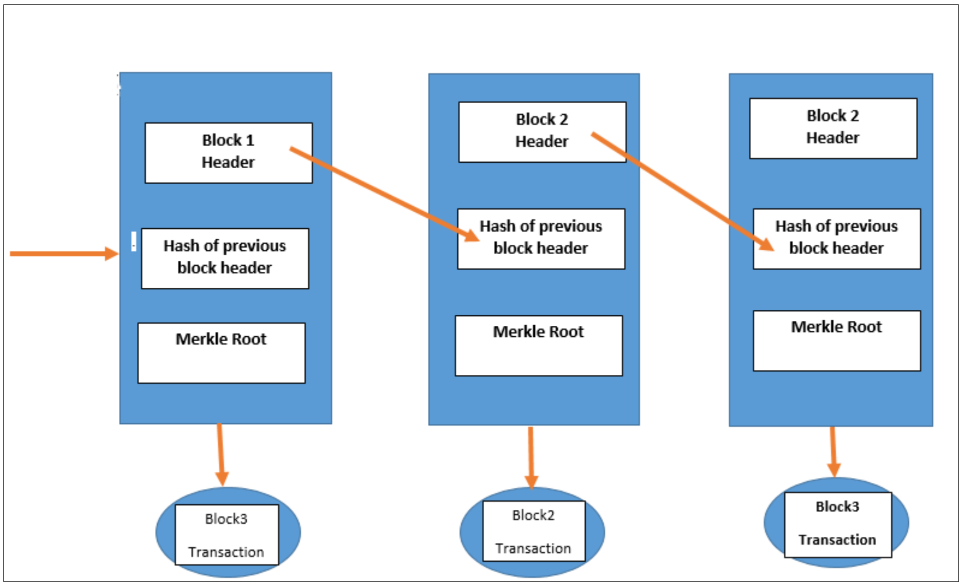

Figure 1. Structure of Blockchain.

The functionality of Blockchain: The principles of Blockchain are as follows.

- Blockchain is an open access platform, and no single entity or organization regulates Blockchain. Everyone can access the database and complete history. Partners in a transaction can see, check, and verify the record of the transaction owned by another partner.
- There is no central authority to establish contact between two nodes. There is direct peer-to-peer communication among nodes. Every node can store information and share it with other nodes freely.
- Every transaction taking place at every node has a unique value consisting of more than 30 characters long alphanumeric addresses to be identified in a blockchain network. Transactions are carried out via these unique addresses. Other nodes can see the transaction and values associated with them having access to the system. Nodes are free to keep their secrecy or show their identity to other nodes.
- Records in Blockchain are irreversible as one record, when updated with some account, is linked to all previous records, hence forming a chain. Numerous approaches[16] and algorithms are implied to make sure that the coming record is stored in the database permanently in chronological order and is accessible to all users or nodes in the network.
- Transactions in Blockchain are programmed and restricted to computation logic. It gives users the liberty to define rules and algorithms to carry out transactions among other nodes in the network automatically.

The major processes of Blockchain are as follows[17][18].

- The sender takes a new record of data and broadcasts it to other nodes in a blockchain network.
- Receiver checks and authenticates the data. If data is found correct, then it is stored in a block of the receiver.
- Every node in the blockchain network runs the Proof of Work (PoW), Proof of Stake (PoS), or other consensus algorithms to submit its block to Blockchain.

A Consensus algorithm is executed. After that, the block is added to the Blockchain. Every node in Blockchain accepts this block. Then the chain is extended based on that block.

Categorization of Blockchain:

Existing blockchain systems can generally be divided into three types: public Blockchain, private Blockchain, and consortium Blockchain [19][20]. All these types of blockchains can be enumerated from multiple perspectives.

- Determination of Consensus: In public Blockchain, every node is eligible to participate in the Consensus. In contrast, a set of selected nodes are used to validate the block in the consortium blockchain. At the same time, the private Blockchain is administrated by an association that can conclude the ultimate agreement.
- Centralization: The key variation between the three types of blockchains is that the public Blockchain is not centralized at all, the consortium is moderately centralized, and the private Blockchain is completely centralized because it can be controlled by a particular entity.
- Access permission: Operations performed in a public blockchain appear to be public. Whereas in a private Blockchain, the administrators are authorized and can decide which transaction is to be added to the Blockchain.
- Immutability of data: It is nearly not possible to process the public Blockchain because transactions are stored on distinct nodes of the distributed system. However, the blocks could be inverted or manipulated if majority groups or prevailing organization desires to manipulate the Blockchain.
- Efficiency: Because Blockchain of the public type has a large number of nodes, it takes more time to transmit blocks to all nodes. Given the security of the network, the limitations on the public Blockchain are intended to be stricter. Therefore, the performance is compromised, and the waiting time tends to be high. With a smaller number of validators, the working of the Blockchain could be more efficient than in private and consortium Blockchain.
- Agreement: In the consensus process of the public Blockchain, anyone from anywhere can participate. Unlike public blockchains, consortium and private blockchains require permission. A node must be certified to take part in the process of the Consensus for private or consortium Blockchain.

Since public Blockchain is open, it attracts many users and communities. Consortium blockchain can be used for many applications like multi-organization systems and multi-peer setup of Hyperledger Fabric. Currently, Hyperledger Fabric is developing blockchain frames for commercial purposes. Ethereum has also provided tools for building consortium blockchain. As for private Blockchain, many companies still use it for efficiency and verification.

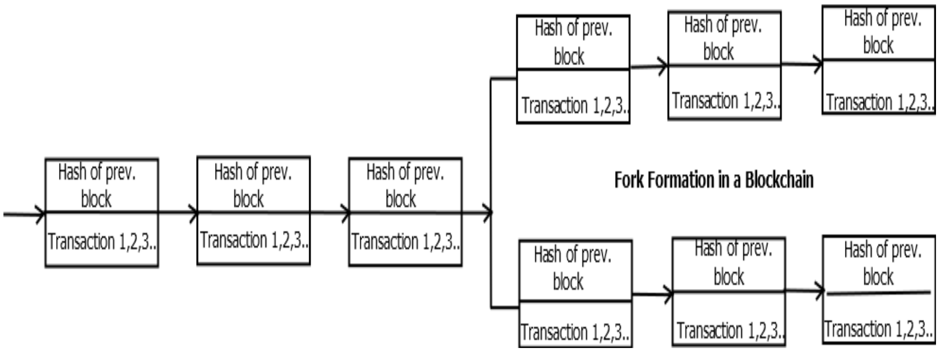

Figure 2. Demonstration of the fork in Blockchain

Forks in Blockchain:

When two miners get two unusual blocks built in the corresponding preceding block, a fork in the Blockchain may occur. This is solved by the PoW consensus protocol. Research shows that the probability of fork formation increases when the block size increases and the gap between the blocks decrease; this is probably due to the delays in the propagation of blocks in blockchain network. Delayed miners may seek to undermine blocks that are no longer in use or not the latest one[21]. Figure 2 shows the demonstration of the fork in a blockchain.

Consensus Algorithms in Blockchain

Consensus is the key element of Blockchain that describes how it works and ensures integrity among validators. Depending on the type of Blockchain, there exist different consensus mechanisms[22]. Various consensus algorithms are used in Blockchain to bring consistency in reaching an agreement among the users. Many review articles cover consensus algorithms with different aspects and parameters[23]–[32]. Consensus in a distributed system is a challenge. For blockchain framework, consensus protocols guarantee that all blocks in the system are in concurrence with a reliable state of the Blockchain. Emerging technologies produce abundant data that needs to be stored and transacted safely from decentralized databases. Recently, there has been remarkable interest in utilizing the applications of Blockchain for the delivery of safe and secure data in healthcare, biomedical, and e-health data sharing[33]. Authors in [34] proposed a framework for the selection of consensus protocols. The framework works on defined criteria and priorities by using multi decision-making system. A fault-tolerant consensus algorithm for Blockchain is proposed [35]. The protocol is based on Practical Byzantine Fault Tolerance (PBFT) to ensure the reliability and efficiency of the consensus protocols. A framework for the theoretical comparison of consensus algorithms is presented in [36]. Experimental evaluation is performed to validate the framework. Authors in [37] developed a framework for Central Bank Digital Currency Evaluation and Verification (CEV) to verify and recommend technical solutions. One module of the proposed framework consists of a consensus algorithm. An efficient consensus algorithm for consortium blockchain is proposed in [38]. The framework is based on DAG supervised to ensure consensus efficiency. Authors in [39] proposed a modification in the Istanbul Byzantine Fault Tolerance voting-based algorithm that provides choices for different business use cases. Another study is based on the acceleration of consensus algorithms using delayed feedback[40]. Another efficient and reliable protocol is proposed in [41] with the properties of fairness, public verifiability etc. Authors in [42] improve the PoW protocol by including several proof rounds. Another framework for hybrid consensus protocol for IoT based healthcare system is presented in to resolve the trustworthiness issues [43][44]. A comparative analysis of some consensus protocols is given in Table 1.

Table 1. Comparison of consensus protocols.

The goal of the consensus layer is to let the blocks reach an agreement. Different types of consensus mechanisms exist that depend on the type of Blockchain.

Parameters	PoW	PoS	DPoS	PoET
Transaction rate	Low	High	High	Medium
Tolerated	< = 25%	< 51%	< 51%	Unknown
Latency	High	Low	Low	Normal
Type of Blockchain	PL	P/PL	P/PL	P/PL
Resource consumption	High	Medium	Low	Low

The most commonly used consensus algorithms are PoW and PoS [45]; however, other consensus algorithms also practice different implementations of PoW and PoS. Since

Blockchain has become a powerful independent technology, the consensus mechanisms have also evolved independently, according to the requirements of the Blockchain platform and applications[46].

Proof-of-Work Model (Ethereum):

Ethereum is a popular blockchain platform that deals with designing smart contracts[46], [47]. The virtual machine of this platform is known as Ethereum Virtual Machine (EVM). This is used for the execution of smart contract code on the nodes of Ethereum. Ethereum platform provides permissionless and public networks. Cryptocurrency used by Ethereum is known as Ether. The purpose of this is to pay for the resources of the network as well as it is used for security like anti-spamming and DDoS protection measures. Ethereum is a general-purpose, open-source, blockchain-based distributed computing platform that can support any kind of application. Ethereum records all transactions on the Blockchain, and any entity can validate this record with the help of the Ethereum network[48]. The PoW model is also used by Ethereum. EthHash provides speedy authorization by using Application Specific Integrated Circuits (ASICs). ASICs perform very high rates of hashing operations. Entities like large organizations can make mining pools and provide a very high hashing rate that permits handling a very large amount of computational Power for operating the Blockchain network. Two approaches have been used by EthHash to oppose mining centralization. The first approach uses memory hardness. This allows the computer to circulate data in memory[49][50]. General-purpose computer hardware is also developed to accomplish expressively but cannot attain efficiently on ASICs. Another technique known as Greedy Heaviest Observed Subtree (GHOST) comprises the head of the newly bereaved chunks called uncles. An orphan block is a block that contains a temporary fork created from the main Blockchain. The node that generates the uncle block in the Blockchain is reduced to encourage the continuation of the newest chunk in the Ethereum blockchain. EthHash uses the idea of searching for the right nonce contribution that can produce a hash rate beneath a convinced level of difficulty. For PoW, this is a time-wasting process, and the node should simply go through the nonce value and execute the set of rules each time to get the results. The static reserve is a Directed Acyclic Graph (DAG) of gigabyte size. Without pre-generation, the client may not be able to start mining without the DAG in that epoch, so there may be a large delay in all epoch transitions. The DAG is desirable only for extraction and not for validation purposes. Validation is an easy progression that can be calculated over an extended period with low Power, low memory, and CPU. Ethereum networks generate blocks every 15 seconds by adjusting the failure rate. Ethereum [48] divides the same concerns with Bitcoin for a 51 % attack. If an attacker can control 51 % of the mining power, divergence can be produced in the Ethereum blockchain. Though, ASIC's PoW has considerable resistance to the 51 % attack on Ethereum networks.

Proof of Stake Model (PoS):

The PoS [51] algorithm is developed to address the disadvantages of the PoW algorithm concerning the high power intake involved in mining processes. The PoS entirely exchanges the mining operation with another approach that involves the ownership of the user or the ownership of the virtual currency on the Blockchain system. In PoS, instead of purchasing a mining device, users can purchase cryptocurrency and use it as a strength to equalize block-building opportunities in the Blockchain system. The PoS algorithm selects the validator for block creation randomly so that it cannot be predicted earlier. This is a 'nothing' in the Stake problem, which needs to be addressed for the accuracy and effectiveness of the PoS. The Ethereum [52] PoS is known as Casper, which is probably the best-advanced PoS algorithm. Casper uses the concept of reservation of credits and stakes for the accomplishment of a contract. The nodes can be combined with Ethereum systems that are fixed by the process. These users are the joined validators, and by stacking security deposits, the initial list of joined validators shows commitment and interest in facilitating Ethereum Blockchains that is tracked by a special contract called Casper contract. From here, the joined validator list can go forward by joining the node away from the system to the old node. Each validator is haphazardly selected to generate a chunk from the active validator set and is generated with the highest prospect of selecting the deposit of each validator. If the validator is offline, another validator will be nominated, and this procedure will be repeated until the online validator that produces the block is detected. If the validator creates a block that is contained in the chain, you receive a block incentive that is equivalent to the entire Ether in the active validator set. This system suggests the "undetermined" problem, which stops the node from ending blocks that are not in the main chain, is resolved.

Proof of Elapsed Time:

Intel Ledger or Intel Ledger Lake is an Intel Blockchain [53] platform developed by the United States and is now officially proposed by the community as a proposal for further development under the Linux Foundation's Hyper ledger project. Intel Ledger uses an Intel-designed agreement algorithm called Proof of Elapsed Time (PoET), which is scheduled to run on a Trusted Execution Environment (TEE), such as Software Guard Extensions (SGX). The PoET is an arbitrary leader selection model and uses a voting technique that uses random reader models or lottery grounded on SGX, and the decorum arbitrarily chooses the next leader to make the final decision of the block. To function properly, you need to distribute a random reader choice among all available participating nodes. In addition, there is no space for the operation because it requires a safe way to verify that other nodes are correctly selected by a particular leader. This is done using TEE to ensure the maintenance and uncertainty of electing a leader. Individually validators request a time interval from the script that is running in the TEE. A component that validates with less interval of time can win the draw and turn out to be a leader. The roles in the TEE are intended to ensure that the execution is not tampered with by external software. If the validation node requests a claim as a reader and is mining a block, you can also create a record to generate the TEE that the other nodes can effortlessly authenticate. This must prove that the minimum delay period has occurred and that the protocol has waited for the specified amount of time before the protocol can start to mine the next block.

Byzantine-Fault-Tolerance-and-variants (BFT) (Hyper ledger Fabric):

Hyper ledger Fabric [54] is the maximum widespread Blockchain platform industrialized through the Linux groundwork, providing a flexible manner with a pluggable agreement model. The fabric is planned for the sake of being validated by a centralized registry in the system. It also provides well-designed agreements on Blockchains, and as well identify the chain code. Hyper ledger now supports two agreed models, which are the common Practical Byzantine Fault Tolerance (PBFT) and the SIEVE. The current proposal is based on a Cross Fault tolerance "(XFT)" model.

PBFT:

The PBFT algorithms projected by Miguel and Barbara were the foremost applied solutions to meet the agreement faced by Byzantine's failure [55]. The concept of a cloned state machine and duplication of the vote is used to change the state of the system. It also reduces the encryption of communications exchanged between customers due to replications. This algorithm allows the "3f + 1" replica to allow "f" failure nodes. This method invites a low performance of the computer-generated copies services. The author reports 3 % upraise for the imitation Network-Free System (NFS) package and reports that these services have been tested, but the PBFT has been scaled down and researched to 20 replicas. As the number of replicas increases, the messaging overhead is significantly increased.

SIEVE:

The SIEVE Consensus Protocol is planned to address non-determinism in Chain code performance. If non-determinism exists in a chain code, a different output is produced when it is performed by a different copy in the circulated network. SIEVE normally handles deterministic transactions, but in some cases, it might produce a different output; the SIEVE protocol treats the chain code itself as a black box. Initially, all the operations are inferred, and the output is compared between replicas.

Cross Fault Tolerance (XFT):

XFT is a novel protocol that streamlines the spasm model, enables integrated fault tolerance, and makes it more efficient to run real scenarios. The Byzantine Fault Tolerance (BFT) protocol assumes a Powerful attacker who can control the node at risk, as well as deliver messages over the network. The ability to cope with such a strong attack reduces the effectiveness of the BFT protocol and dramatically improves its complexity. XFT solves state machine replication issues by easing attackers' strong assumptions, simplifying the state machine replication problem, and providing efficient solutions that can tolerate Byzantine failure.

Federated-Byzantine-Agreement (Ripple & Stellar):

Ripple and Stellar are the payment protocols based on two Blockchain-based platforms and the Byzantine Fault Tolerance Consensus model variation with respect to joining the nodes. These Blockchain platforms, in particular, provide payment protocols for financial use cases and settlement domains and can pay for a few seconds for cross-border transactions between today's infrastructure. The participants in this system are users, economic institutions acting as associates, and market operators who may be users or economic organizations. End-users can use client software to generate payment transactions and keep payments with a number of gateways, just like the banks they use in the real world. The gateway holds the user funds that are issued to the gateway with a heavy currency and creates equivalent publications in the Ripple/Stellar network. This is reflected in the account balance in the Blockchain. Payment transactions can be validated by each node by denoting the account balance in the public Blockchain. Supreme transactions support payments in other cryptographic currencies so that the protocol has the greatest importance in placing a consistent order of transactions and preventing double overheads. Ripple and Stellar custom their individual agreement mockups to include unrestricted participation from users, gateways, and market manufacturers and are derived from the Byzantine fault tolerance.

For the Ripple protocol[56], every single node must state a unique Node List (UNL). UNL consists of extra Ripple nodes that are confidential by the specified node and does not collate against the node. The Consensus in the Ripple system is attained by every node by referring to other nodes in the UNL. Each UNL must have a 40 % overlap in the Ripple network. In this case, an individual node gathers a transaction in a Blockchain called a "candidate set", and then broadcasts the candidate set to additional lumps in the UNL. The nodes certify the transactions, vote for them, and transmit the vote. Considering the number of votes counted, each node will pass the next round of transactions to receive the candidate's number of votes and receive the most votes. If the candidate set receives the top 80 % of the votes get from every node in the UNL, the candidate develops an effective block, and Ripple terms that as a "ledger". When an individual subnetwork reaches an agreement, Consensus is reached across the network.

The Stellar Consensus Protocol (SCP) customs the idea of quorum and quorum slicing. A quorum is a group of nodes that are sufficient to achieve an agreement. A quorum slice is a subgroup of the quorum that can persuade a specific node of an agreement to be satisfied. Individual nodes may be displayed in multiple quorum slices. In Stellar, a quorum slice is introduced, allowing an individual node to select a group of nodes of its slice, permitting open contribution.

To reach a worldwide Consensus on all systems, a quorum must be crossed. The Consensus has been achieved globally by individual node decisions. The agreement protocol works as follows: Individual node initially accomplishes the first vote on the transaction. The second step is the acceptance step. The node does not accept that the statement is inconsistent with the current statement and accepts the statement if an individual node in the v-blocking set accepts the declaration. Approval is the final stage of the elective procedure. A brief description of the methodology of different consensus algorithms is discussed here. The strengths and limitations of the algorithms are summarized in Table 2.

In PoW, for a transaction, miners in the Blockchain use their supercomputers to solve a cryptographic puzzle. The answer to the puzzle tells them which next block will be added to the Blockchain. The first to solve the puzzle has been rewarded with quality bitcoins.

In PoS, instead of a user spending money to buy miniature computers, a minor would spend here to purchase an encryption token, then use these tokens as a stake to purchase proportional creation opportunities in a chain of blocks.

DPoS is similar to PoS with slight variations. PoS can be considered a direct democracy, whereas DPoS is like a representative democracy. In DPoS, coin holders use their coins to elect network delegates called "validators". Elected validators can impose blocks and add them to the Blockchain network.

Table 2. Summary of the Consensus algorithms

Algorithm	Strengths	Limitations
PoW	• First Consensus protocol and quite popular. • Highly scalable and Suitable for a variety of applications.	• Energy-intensive • 51% vulnerable to attack.
PoS	• Increased transaction processing speed compared to POW. • Less energy consumption because it does not need equipment (supercomputer) Fewer resource needs.	• Always vulnerable because a person with enough money to invest can buy a crazy number of encrypted tokens. • The rich get richer (the rich can control the network)
DPoS	• The speed of processing is greater than that of the PoW. • Less power consumption because no equipment is required (supercomputer). Fewer resource needs.	• Cartel formation (witnesses can form a cartel and rule the network). • Vulnerable to attacks • Quite centralized because Power is in the hand of a few delegated nodes.
PoET	• Low participation cost (more people can participate easily, which makes it decentralized) • All participants can simply verify that the delegate has been legitimately selected	• Even though it is cheap, it still needs specialized software. • Not suitable for public Blockchain

In the PoET algorithm, each participant network node must wait a randomly selected period, and the first to complete the designated waiting time wins the new block. Each block in a Blockchain network generates a random wait time and remains inactive for the specified duration. The first contender to wake up is the one whose waiting time is the shortest: he wakes up and sends a new block to the chain of blocks.

Challenges and Opportunities

Blockchain is currently under extensive research and development from both academia and the industry; however, there are still some major challenges to be overcome. As no special techniques are applied for the verification of the transaction, every transaction will be verified by the nodes in the network. This puts a constraint on what number of smart contacts would be processed in each block and, as a 77result, how large a smart contract application is likely to be before it could affect the whole performance of the Blockchain network immensely.

With the evolution of Blockchain and its being in trend due to new paradigm shift in business and networking, its application is also found in wireless networks. In Blockchain wireless networks, computation off-loading and content caching in Mobile Edge Computing [57] is also a significant issue. Another issue that Blockchain faces are designing Blockchain algorithm to promise a good quality of service to Blockchain-based application[58]. This problem becomes important to consider that the performance of Blockchain is mainly dependent on the selected Consensus schemes or algorithms in terms of robustness to randomly behaving nodes and speed of Consensus decision taken. It is predicted to beat the current trends and technologies to handle the business, consumer/customer services, distributing systems, and record-keeping systems. But it is still an evolving process. But surely, it can be foreseen clearly, that the future belongs to Blockchain.

Conclusion.

Blockchain-based frameworks alter the centralized storage systems, for example, relational databases, by making them secure and performing fewer transactions per unit time. Then again, these frameworks have the upside of giving progressively vigorous and fault-tolerant methods for storing critical data. To pick up the advantages of this innovation, it is significant that health associations directly investigate platforms, systems, and ways to deal with the implementation of this technology. This survey article gives an outline of Blockchain technology, including Blockchain framework and various Blockchain Consensus protocols. We, at this point, examine the distinctive Consensus protocols utilized in the Blockchain and contrast these algorithms in various regards. Moreover, we exhibit a few difficulties and issues that would upset Blockchain innovation. We analyzed and compared various consensus algorithms.

References

[1] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective," *SSRN Electron. J.*, 2015, doi: 10.2139/ssrn.2646618.

[2] G. Foroglou and A. L. Tsilidou, "Further applications of the blockchain," *Conf. 12th Student Conf. Manag. Sci. Technol. Athens*, no. MAY, pp. 0–8, 2015.

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *Proc. - 2016 IEEE Symp. Secur. Privacy, SP 2016*, pp. 839–858, Aug. 2016, doi: 10.1109/SP.2016.55.

[4] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A Whole New World: Income Tax Considerations of the Bitcoin Economy," *Pittsburgh Tax Rev.*, vol. 12, no. 1, pp. 24–56, 2015, doi: 10.5195/taxreview.2014.32.

[5] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin,"

2015 18th Int. Conf. Intell. Next Gener. Networks, ICIN 2015, pp. 184–191, Mar. 2015, doi: 10.1109/ICIN.2015.7073830.

[6] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9891 LNCS, pp. 490–496, 2016, doi: 10.1007/978-3-319-45153-4_48.

[7] C. Noyes, "BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning," Jan. 2016, doi: 10.48550/arxiv.1601.01405.

[8] M. Iansiti and K. R. Lakhani, "The truth about blockchain: It will take years to transform business, but the journey begins now," *Harv. Bus. Rev.*, no. January 2017, pp. 117–128, 2017.

[9] H. Jang and J. Lee, "An Empirical Study on Modeling and Prediction of Bitcoin Prices with Bayesian Neural Networks Based on Blockchain Information," *IEEE Access*, vol. 6, pp. 5427–5437, Nov. 2017, doi: 10.1109/ACCESS.2017.2779181.

[10] A. Stanciu, "Blockchain Based Distributed Control System for Edge Computing," *Proc. - 2017 21st Int. Conf. Control Syst. Comput. CSCS 2017*, pp. 667–671, Jul. 2017, doi: 10.1109/CSCS.2017.102.

[11] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 07, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.

[12] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016, doi: 10.1109/COMST.2016.2535718.

[13] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2015-July, pp. 104–121, Jul. 2015, doi: 10.1109/SP.2015.14.

[14] M. Schäffer, M. di Angelo, and G. Salzer, "Performance and Scalability of Private Ethereum Blockchains," *Lect. Notes Bus. Inf. Process.*, vol. 361, no. August, pp. 103–118, 2019, doi: 10.1007/978-3-030-30429-4_8.

[15] R. A. U. Ullah. A, Qayyum. H, Hassan. F, Khan. M. k, "Comparison of Machine Learning Algorithms for Sepsis Detection," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 1, pp. 175–188, 2022, [Online]. Available: https://journal.50sea.com/index.php/IJIST/article/view/190

[16] M. Anjum.S. M, Riaz.O,Latif, S, "Diastolic Dysfunction Prediction with Symptoms Using Machine Learning Approach," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 3, pp. 714–727, 2022, [Online]. Available: https://journal.50sea.com/index.php/IJIST/article/view/280/

[17] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017, doi: 10.6633/IJNS.201709.19(5).01.

[18] K. M. I. Baig. M. S, Imran. A, Yasin. A. U, Butt. A. H, "Natural Language to SQL Queries: A Review," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 1, pp. 147–162, 2022.

[19] "On Public and Private Blockchains | Ethereum Foundation Blog." https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed Jul. 27, 2022).

[20] D. H. Zaka. S, Majeed. M. N, "Blind Image Deblurring Using Laplacian of Gaussian (LoG) Based Image Prior," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 2, pp. 365–374, 2022.

[21] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," *13th IEEE Int. Conf. Peer-to-Peer Comput. IEEE P2P 2013 - Proc.*, 2013, doi: 10.1109/P2P.2013.6688704.

[22] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, "A review on consensus algorithm of blockchain," *2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017*, vol. 2017-January, pp. 2567–2572, Nov. 2017, doi: 10.1109/SMC.2017.8123011.

[23] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6693731.

[24] M. Kaur, M. Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty, and S. K. Pani, "MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols," *IEEE*

Access, vol. 9, pp. 80931–80944, 2021, doi: 10.1109/ACCESS.2021.3085187.

[25] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Syst. Appl.*, vol. 168, p. 114384, Apr. 2021, doi: 10.1016/J.ESWA.2020.114384.

[26] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, and R. Thomas, "A survey and taxonomy of consensus protocols for blockchains," *J. Syst. Archit.*, vol. 127, p. 102503, Jun. 2022, doi: 10.1016/J.SYSARC.2022.102503.

[27] A. Altarawneh, F. Sun, R. R. Brooks, O. Hambolu, L. Yu, and A. Skjellum, "Availability analysis of a permissioned blockchain with a lightweight consensus protocol," *Comput. Secur.*, vol. 102, p. 102098, Mar. 2021, doi: 10.1016/J.COSE.2020.102098.

[28] D. P. Oyinloye, J. Sen Teh, N. Jamil, and M. Alawida, "Blockchain Consensus: An Overview of Alternative Protocols," *Symmetry 2021, Vol. 13, Page 1363*, vol. 13, no. 8, p. 1363, Jul. 2021, doi: 10.3390/SYM13081363.

[29] B. Sriman, S. Ganesh Kumar, and P. Shamili, "Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake," *Adv. Intell. Syst. Comput.*, vol. 1172, no. March 2022, pp. 395–406, 2021, doi: 10.1007/978-981-15-5566-4_34.

[30] H. Afzaal, M. Imran, M. U. Janjua, and S. P. Gochhayat, "Formal Modeling and Verification of a Blockchain-Based Crowdsourcing Consensus Protocol," *IEEE Access*, vol. 10, pp. 8163–8183, 2022, doi: 10.1109/ACCESS.2022.3141982.

[31] M. Sun, Y. Lu, Y. Feng, Q. Zhang, and S. Liu, "Modeling and verifying the CKB blockchain consensus protocol," *Mathematics*, vol. 9, no. 22, pp. 1–15, 2021, doi: 10.3390/math9222954.

[32] G. A. F. Rebello, G. F. Camilo, L. C. B. Guimarães, L. A. C. de Souza, G. A. Thomaz, and O. C. M. B. Duarte, "A security and performance analysis of proof-based consensus protocols," *Ann. Telecommun. 2021*, pp. 1–21, Nov. 2021, doi: 10.1007/S12243-021-00896-2.

[33] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, pp. 1–16, 2019, doi: 10.3390/cryptography3010003.

[34] E. Filatovas, M. Marcozzi, L. Mostarda, and R. Paulavičius, "A MCDM-based framework for blockchain consensus protocol selection," *Expert Syst. Appl.*, vol. 204, p. 117609, Oct. 2022, doi: 10.1016/J.ESWA.2022.117609.

[35] Y. Zhan, B. Wang, R. Lu, and Y. Yu, "DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains," *Inf. Sci. (Ny).*, vol. 559, pp. 8–21, Jun. 2021, doi: 10.1016/J.INS.2020.12.077.

[36] Z. Ren, H. Xiang, Z. Zhou, N. Wang, and H. Jin, "AlphaBlock: An evaluation framework for blockchain consensus algorithms," *SBC 2021 - Proc. 9th Int. Work. Secur. Blockchain Cloud Comput. co-located with ASIA CCS 2021*, pp. 17–22, May 2021, doi: 10.1145/3457977.3460297.

[37] S. Y. Jin and Y. Xia, "CEV Framework: A Central Bank Digital Currency Evaluation and Verification Framework With a Focus on Consensus Algorithms and Operating Architectures," *IEEE Access*, vol. 10, pp. 63698–63714, Jun. 2022, doi: 10.1109/ACCESS.2022.3183092.

[38] F. Xiang, W. Huaimin, S. Peichang, O. Xue, and Z. Xunhui, "Jointgraph: A DAG-based efficient consensus algorithm for consortium blockchains," *Softw. Pract. Exp.*, vol. 51, no. 10, pp. 1987–1999, Oct. 2021, doi: 10.1002/SPE.2748.

[39] H. Samy, A. Tammam, A. Fahmy, and B. Hasan, "Enhancing the performance of the blockchain consensus algorithm using multithreading technology," *Ain Shams Eng. J.*, vol. 12, no. 3, pp. 2709–2716, Sep. 2021, doi: 10.1016/J.ASEJ.2021.01.019.

[40] H. Moradian and S. S. Kia, "a Study on Accelerating Average Consensus Algorithms Using Delayed Feedback," *IEEE Trans. Control Netw. Syst.*, pp. 1–11, 2022, doi: 10.1109/TCNS.2022.3188481.

[41] P. Wang, W. Chen, and Z. Sun, "Consensus algorithm based on verifiable randomness," *Inf. Sci. (Ny).*, vol. 608, pp. 844–857, Aug. 2022, doi: 10.1016/J.INS.2022.07.024.

[42] M. Kara *et al.*, "A Compute and Wait in PoW (CW-PoW) Consensus Algorithm for Preserving Energy Consumption," *Appl. Sci. 2021, Vol. 11, Page 6750*, vol. 11, no. 15, p. 6750, Jul. 2021, doi: 10.3390/APP11156750.

[43] P. Prabha and K. Chatterjee, "Design and implementation of hybrid consensus mechanism for IoT based healthcare system security," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1381–1396, May 2022, doi: 10.1007/S41870-022-00880-6/FIGURES/9.

[44] A. S. Sajjad. S, Abdullah. A, Arif. M, Faisal. M. U, Ashraf. M. D, "A Comparative Analysis of Camera, LiDAR and Fusion Based Deep Neural Networks for Vehicle Detection," *Int. J. Innov. Sci. Technol.*, vol. 3, no. special issue, pp. 177–186, 2021.

[45] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, pp. 1545–1550, Jun. 2018, doi: 10.23919/MIPRO.2018.8400278.

[46] H. F. Ouattara, D. Ahmat, F. T. Ouédraogo, T. F. Bissyandé, and O. Sié, "Blockchain consensus protocols: Towards a review of practical constraints for implementation in developing countries," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 250, pp. 304–314, 2018, doi: 10.1007/978-3-319-98827-6_29/COVER.

[47] C. Natoli and V. Gramoli, "The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium," *Proc. - 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks, DSN 2017*, no. December, pp. 579–590, 2017, doi: 10.1109/DSN.2017.44.

[48] C. Dannen, *Cryptoeconomics Survey*. 2017. doi: 10.1007/978-1-4842-2535-6_7.

[49] R. O. and S. W. Anjum. M. S, Mumtaz. S, "Heart Attack Risk Prediction with Duke Treadmill Score with Symptoms using Data Mining," *Int. J. Innov. Sci. Technol.*, vol. 3, no. 4, pp. 174–185, 2021.

[50] R. A. Manzoor. S, Qayyum. H, Hassan. F, Ullah. A, Nawaz. A, "Melanoma Detection Using a Deep Learning Approach," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 1, pp. 222–232, 2022.

[51] L. Fan and H.-S. Zhou, "A Scalable Proof-of-Stake Blockchain in the Open Setting * (or, How to Mimic Nakamoto's Design via Proof-of-Stake)," *Cryptol. ePrint Arch.*, 2018, [Online]. Available: https://eprint.iacr.org/2017/656.pdf

[52] "Comparison of Ethereum, Hyperledger Fabric and Corda | by Philipp Sandner | Medium." https://philippsandner.medium.com/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6 (accessed Jul. 27, 2022).

[53] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10616 LNCS, pp. 282–297, 2017, doi: 10.1007/978-3-319-69084-1_19/COVER.

[54] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proc. 13th EuroSys Conf. EuroSys 2018*, vol. 2018-January, Apr. 2018, doi: 10.1145/3190508.3190538.

[55] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform," *Proc. - 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks, DSN 2018*, no. June, pp. 51–58, 2018, doi: 10.1109/DSN.2018.00018.

[56] D. Mazi`eres and M. Mazi`eres, "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus".

[57] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Joint computation offloading and content caching for wireless blockchain networks," *INFOCOM 2018 - IEEE Conf. Comput. Commun. Work.*, pp. 517–522, Jul. 2018, doi: 10.1109/INFCOMW.2018.8406929.

[58] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.