Review of Different Consensus Algorithms and Blockchains

Rakhi Agrawal* Jacob Jose † Aditi Narendran‡

December 4, 2022

Abstract

Blockchains are becoming hugely popular these days and are being introduced in new sectors such as healthcare, music, and charitable organizations. The blockchain is made up of blocks of digital transactions that are solely controlled by the participants. The participants use consensus algorithms to reach a mutual agreement about the present state of the ledger. Consensus algorithms are the backbone of blockchain technology. In this paper, we are reviewing new blockchains and consensus algorithms that have higher throughput, faster confirmation, and are more secure than traditional blockchains. The novel consensus algorithms, such as Blockene, facilitated implementation on devices with low computation power, such as smart phones. This paper also reviews consensus algorithms which are specific to certain application such as quantum, healthcare.

1 Introduction

A blockchain is an immutable, transparent, secure, and decentralized digital ledger. It can be used to electronically track transactions or store digital assets. Bitcoin was the first cryptocurrency to gain popularity and success. Ethereum is another currency that even allows for the modification of transaction rules. Because these blockchains have no central authority, all transactions must be validated and secured by the participants. This is accomplished using several consensus protocols. A consensus protocol enables all blockchain nodes to agree on the global state of the ledger. In other words, it is the responsibility of these consensus algorithms to ensure that every new block added is the real version and is agreed upon by all blockchain participants. There are various consensus protocols such as Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), etc.

But the major concern for these blockchains is their performance in the real world. Bitcoin uses Nakamoto consensus along with PoW but is slow in generating blocks. Statistically, they can generate only 1 MB of data every 10 minutes and process just 7 transactions every second. For a new transaction, it takes about 1 hour to be added to the chain. In this paper, we are reviewing some new blockchains and their consensus algorithms, which overcome these limitations and achieve the desirable properties of blockchain. Ideally, the blockchains should be secure and immune to attacks such as the Liveness attack, Sybill attack. They should have higher transaction rates, and the consensus between the participants should be reached quickly.

2 Problem Setup and Threat Model

The properties of blockchains, such as decentralization, transparency, and tamper resistance, make them attractive for many applications. However, most blockchains require devices with high computational power because their consensus algorithm relies on massive computations to ensure the integrity of the blockchain. The widely used blockchains such as Proof of Work (PoW) require the participants to solve complex problems to get the solution; while this is feasible with powerful computers, devices with less resources are not able to do so. In today's world, with a large number of devices collecting and processing data, there would be a lot of possibilities if features offered by blockchains could be brought into such devices. This paper is evaluating new blockchains and consensus algorithms that claim to have better throughput, have faster confirmation, and at the same time use less computational resources and thus can run even on smartphones. These protocols can bring blockchain applications to smaller devices and thus open the world to new possibilities.

The consensus algorithms are based on the assumption that a certain number of participants are trustworthy, and thus the transactions can be done successfully without any malicious attack because of these honest participants. If all the participants are dishonest and they attack synchronously, the blockchain can fail to meet its expectations.

*CSE Master's 2nd year
†SE Master's 1st year
‡CSE Master's 1st year

3 Literature Review

3.1 Blockene: A High-throughput Blockchain Over Mobile Devices

The authors introduce Blockene [8], a new blockchain with fast throughput and the ability to scale to millions of nodes or participants. Because this blockchain requires few resources, participants can validate blocks on a smartphone as well. Even on smartphones, the blockchain consumes very little battery power (approximately 3 % daily), allowing users to mine without worry. This is made possible by a revolutionary architecture that divides trust between honest and dishonest actors. Blockene only transfers roughly 60 MB of data every day, whereas other blockchains move about 10 GB on average. Blockene participants only need roughly 100–200 MB of storage, but other blockchain participants must maintain a whole copy of the blockchain. Citizens and Politicians are the two categories of member nodes. Citizens are the primary participants in the blockchain. They use smartphones and have a voice in the consensus protocol. The authors assume that two-thirds of citizens are trustworthy. They support this assumption by assuming that there will be millions of nodes acting as Citizens. Politicians are untrustworthy nodes that run on servers. There are only a few hundred politicians, and the researchers believe that only 20% of them can be trusted. They keep the blockchain safe. However, the algorithm empowers citizens to identify and respond to any vengeful behavior. Blockene can function even if 80% of politicians and one-third of citizens are corrupt. Citizens employ a technique known as replicated verifiable reads to validate the same data from several politicians to obtain the proper transaction. The role of the citizens is to validate every transaction and finalize the global state to commit by using Byzantine consensus with a variation. As there are millions of citizens for consensus, Blockene selects a random group of citizens (about 2000) for performing consensus on each block and the selection is made known to the citizens just few minutes before their participation to ensure reduction in data and battery usage. Citizens are free from huge amounts of data as they only have to process a small subset from politicians and create a new block. Citizens cannot directly take the values given by the politicians as they are not trustworthy; rather, they use a technique of sampling-based Merkle tree read/write that is tolerant to dishonest politicians. The system is designed such that they are protected against Sybil attacks, where a huge number of imaginary nodes are created to bias the voting procedure. This attack is prevented by taking the advantage of trusted hardware (TEE) available in almost all smartphones to certify each participant and make sure that atmost one participant is present through one smartphone.

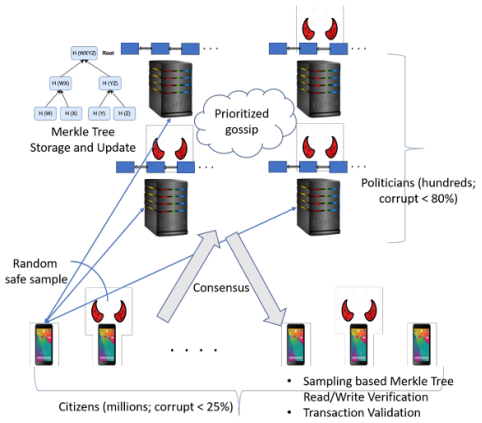
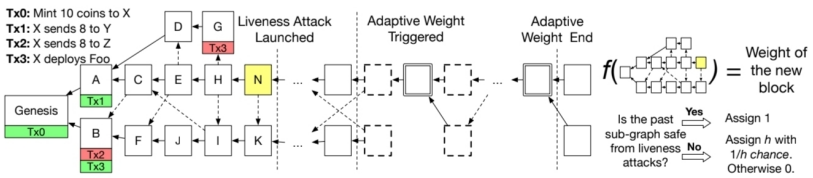


Figure 1: Architecture of Blockene

This protocol is one of a kind as it can work on mobile devices as the resource usage is very low and the battery consumption is quite negligible. It can work in the background without creating any issue for the user. The concept of dividing the nodes in two components and have different architecture for each type is making a difference. This protocol has the power to change the future if they are integrated with IoT devices.

3.2 Conflux: A Decentralized Blockchain with High Throughput and Fast Confirmation

The author introduces Conflux [6], a public blockchain with high throughput and fast confirmation. The author claims that it is the first blockchain to achieve all four blockchain features outlined in the previous section. It is stable and trustworthy, with excellent performance and scalability. It is as decentraized and secure as Bitcoin and Ethereum but has lesser latency and improved throughput of transactions. The blocks are arranged are Tree-Graph which means that the blocks share parent-child relationship. With respect to a parent node, the child nodes makes the edger appear as a tree but with respect to all the blocks, the ledger appears to be a Directed Acyclic Graph (DAG). The weights are assigned to each block depending upon their position in the Tree-Graph. This structure addresses many security challenges such as liveness attack. Conflux's consensus algorithm generates blocks using two separate strategies: conservative and optimistic. The conservative method (similar to the strawman algorithm) ensures consensus progress, whereas the optimistic strategy (similar to the GHOST algorithm) allows for fast confirmation. Using the adaptive weight mechanism, these two techniques are combined. The



(a) Tree-Graph Example. Solid blocks have weight one. Double-line blocks have weight 600. Dotted-line blocks have weight zero.

(b) Adaptive Weight

Figure 2: Examples of Conflux Consensus on Tree-Graph

conflux generally employs an optimistic strategy, but in the event of a liveness attack, the trustworthy members convert to a conservative strategy. Transactions are sometimes rolled back due to the rapid production of blocks, which wastes compute resources. Conflux overcame this obstacle by utilizing the deferred execution approach. It allows the stabilization of order rather than the immediate execution of transactions. To regulate the weights of the Tree-Graph, the consensus process employs a link-cut tree. This approach reduces the processing time per block from $O(n)$ to $O(\log n)$.

This protocol uses Tree Graph structure to connect their nodes and reduces the processing time substantially. They are performing better than Bitcoins and Ethereum on many factors. They are combining different strategies for their nodes to handle liveness attack.

3.3 ACCORD: A Scalable Multileader Consensus Protocol for Healthcare

ACCORD[2], as introduced by the authors, is a scalable permissioned quorum-based (multi-leader) consensus protocol that achieves fork resistance and robustness. The protocol follows a simple working that is performed in three distinct parts. After a transaction is transmitted to the network, the ACCORD protocol makes use of a quorum of leaders to equally allocate a single leader's duties across all the quorum members. The authors guarantee the accuracy of the block by requiring a certain percentage of the quorum members to vote in favor of the transactions prior to proposing their block. Before being added to the blockchain, this block must be asynchronously signed by the majority of the network's nodes in order for the network to accept it. The five main stakeholders in the consensus protocol, ACCORD, are the transaction makers, mining nodes, membership authorities, peer-to-peer nodes, and external observers, and the authors work on a set of assumptions based on these stakeholders.

In addition to robustness, fork resistance and scalability, the authors have also proposed liveness as a primary feature of the ACCORD protocol. This feature ensures that the protocol can guarantees that a successful transaction will show up in the ledgers of every trustworthy node within an acceptable amount of time. The protocol must guarantee that a new block will be generated by an honest quorum within a reasonable amount of time in order to maintain liveness. It is essential to take note that blocks generated by malicious quorums are allowed (assuming they are genuine), provided that honest quorums also generate blocks on a regular basis. Additionally, the authors claim that ACCORD enables fairness in miner selection as each miner is chosen with roughly the same frequency and a more uniform distribution than random selection.

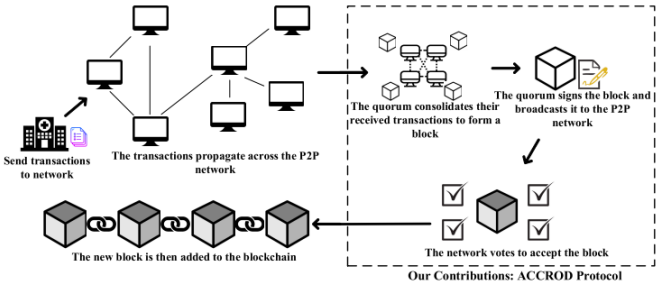


Figure 3: High level architectural diagram of the system

According to the threat-risk assessment and security analysis, this protocol renders forks extremely unlikely in a good environment and enables the network to effectively resolve forks in a bad environment by using the quorum selection protocol, the block creation protocol, the block acceptance method, and the impeachment procedure. While this protocol is vulnerable to long-range attacks, it relies on a well-established principle or a continuous checkpoint system for defense. It would not be possible to reverse a blockchain from the perspective of a node that has observed the blockchain between the blocks during the attack but it can be pretty easy to spot because there would likely be a purge, a widespread rekeying of mining nodes, or a sizable number of impeachments on the false branch. The experiment on selection manipulation looks at a method to keep control of the mining process in the event of no impeachment. Impeachment could be a valid strategy, even though it may be impossible to hold

control of the system repeatedly owing to the suspicious behaviour needed to do so. In the statistical analysis of the Impeachment and Malicious Block Takeover, using the recommended settings of $q = 16, \delta = 13, \delta = 2$, the probability of a malicious group being able to take control of any given block at 50% corruption was 23.2%. The probability of the malicious group taking control of 7 sequential blocks was 0.0074%.

This protocol, when compared with traditional single leader protocols seems to provide a better management of preventing the malicious manipulations of content. It could be a viable solution due to it's fork resistance and scalabilty but most of the assumptions made by this protocol revolve around the honesty and trust of the primary stakeholders and so if anyone of those are not trustworthy there can be chances of error.

3.4 Efficient Quantum Blockchain With a Consensus Mechanism QDPoS

The security of traditional blockchain is in risk due to the development of quantum computers so the authors propose to introduce an effective quantum blockchain system, their QDPoS [7] consensus mechanism combined with current quantum digital signature methods, where single qubits are utilized to form quantum blocks and are linked by entanglement. Additionally guaranteeing the efficacy and security of the suggested quantum blockchain system. For normal nodes to obtain a consensus and representative nodes to quickly produce corresponding blocks, a new quantum voting based consensus method is presented. This ensure that quantum computers won't really change the fairness of QDPoS, even if they become a reality in the future. The construction of quantum blocks with a single qubit, linking quantum blocks in states of weighted graphs or hypergraphs, and integrating quantum digital signature with the created consensus mechanism QDPoS are suggested as ways to create an effective quantum blockchain. Quantum voting is employed by QDPoS to elect a specific number of representative nodes, who then create new blocks, just like in traditional DPoS. The distribution center distributes quantum states, and each node has the option to vote favorably, negatively, or not at all. Following the selection of the representative nodes, they are arranged in a random order of appearance and the blocks are cycled through by them. Economic variables are integrated with QDPoS to offer nodes incentives in order to ensure that it performs better. The representative nodes' identities are not fixed in order to prevent monopolies. All nodes have the option of conducting fresh votes to choose new representative nodes once the final representative node completes the block production.

Combining the aforementioned quantum technologies, a quantum blockchain scheme was also developed by the authors in which quantum blocks are created by using classical information (set as phases of quantum states) and the entanglement features between them to link the blocks and form chains. The chain can have hyper graph or weighted graph states. To further assure the effectiveness and security of quantum blockchain, quantum consensus mechanisms and quantum digital signatures are employed. Each node has the ability to create verifiable data using the quantum digital signature method and communicate it to other nodes for verification. Verified messages are put to the quantum block via the QDPoS consensus technique, and all nodes are able to add this new quantum block to their own local quantum blockchain. Figure 4 depicts the workflow of the proposed quantum blockchain that uses the QDPoS consensus protocol.

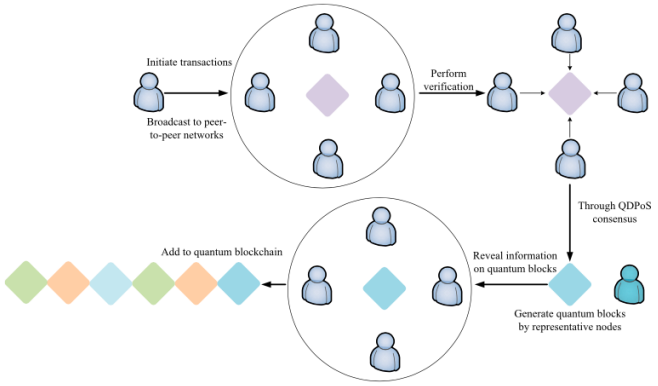


Figure 4: Quantum blockchain workflow

The structural design of the quantum blockchain follows the principle of quantum entanglement, and are usually a distributed and decentralized ledger. Since all quantum actions are reversible, any node may check to see if a quantum block has been altered by measuring it thereby ensuring immutability of data and preserving the security. As there is no third party to authenticate the transaction and force all nodes to agree on it, the unforgeability and consistency of connected transactions can shield against quantum assaults and ensure transaction integrity, non-repudiation, and authenticity. However, the keys for signing transaction information can only be used once, and future transactions should utilize alternative keys in order to be completely safe. This QDPoS blockchain scheme, which offers Byzantine fault tolerance and has the time complexity as O(n), appears to have the best outcome when compared to other quantum blockchain systems. But no matter how good any quantum consensus algorithm's security and protection are, it cannot be scalable and must instead be used with supercomputers or

extremely fast computers. Therefore, it is difficult to recreate this protocol and blockchain system for general usage.

3.5 PoTN: A Novel Blockchain Consensus Protocol with Proof-of-Trust Negotiation in Distributed IoT Networks

To reduce the massive computational resource usage on traditional blockchain systems the authors have proposed Proof-of-Trust Negotiation (PoTN) consensus algorithm[3]. In PoTN, a group of nodes in the blockchain are chosen to be miners. Each miner has a trust value associated with it and their position in the group depends on this. The miners' trust value increases when they perform the correct actions and decrease for malicious behavior. In the PoTN consensus algorithm, during the start of the blockchain, 51% of the nodes are randomly chosen to be in the miners group. The algorithm does not choose 100% of the nodes to be on the miners' group because doing so will lead to communication overhead in the blockchain network. The nodes selected as miners are evaluated consistently during each round of block creation, during this time blocks that misbehave are removed. During a block creation, a subset of nodes from the miners are chosen as proposers and another group is chosen as validators. Here, it is crucial that each of the nodes in these sub-groups have zero knowledge of other nodes that are in their group. Multiple proposers can ensure that a single block is proposed by multiple nodes, so even if a block is bad, the entire round of block creation is not rejected. A block that gets the majority of votes from the validators is chosen to be on the blockchain. In a blockchain with n nodes, ϕ nodes are chosen as miners. Each miner node M_i will be assigned two sets of tuples (f_i, r_i) and (w_i, c_i) where 'f_i', 'r_i' are the number of false and correct blocks proposed by node M_i. 'w_i' and 'c_i' are the wrong and correct votes proposed by node M_i. Based on these tuples, node M_i's trust values as proposer (PT_i), validator (VT_i), and miners (T_i) are calculated. θ, n_1, and n_2 are the threshold values for trust, proposal, and validation.
$PT_i = \frac{\theta * n_1}{f_i+1} - \frac{f_i}{r_i+1}$, $VT_i = \frac{\theta * n_2}{w_i+1} - \frac{w_i}{c_1+1}$ and $T_i = \frac{\theta * (n_1+n_2)}{f_i+w_i+1} + \frac{f_1+w_i}{r_i+c_i+1}$

According to the PoTN algorithm, a miner M_i cannot be chosen as a proposer if its proposal trust PT_i falls below θ. Also, the node cannot be a validator if its validation trust VT_i falls below θ. n_1 and n_2 are toleration values for wrong behaviors, their values should be according to the context of the blockchain. If the blockchain is to be implemented in an environment sensitive to the wrong behaviors of nodes, then their value should zero. Furthermore, honest nodes in the group will be having f_i and c_i values to be 0 and PT_i, VT_i, and T_i to be greater than θ Another feature proposed by PoTN is ensuring that a proposer or validator does not know which are the other proposers or validators in the network. After the selection of proposers and validators, the chosen nodes receive information that is encrypted by their public key. A node chosen as a proposer will receive the IDs of all miners chosen as validators, and one chosen as a validator will receive only information about those selected as proposers. Sharing only information can prevent the chosen nodes from getting or validating data sent by fake nodes in the blockchain. It also prevents any time of collusion between the nodes in the blockchain.

Compared to PoW consensus algorithm in which each node performs complex computation to get a block validated, the PoTN ensures that only a few selections of the nodes perform computation. This helps in a considerable reduction in resource consumption compared to PoW. Moreover, PoTN can be said to be more useful than Proof of Stake (PoS) consensus algorithm wherein the node with most assets is chosen as the miner. A drawback of PoS is that it is prone to the "rich get richer" problem. PoTN prevents this problem by randomly choosing nodes to propose blocks.

3.6 Consensus Algorithm of Proof-of-Stake Based on Credit Model

The Proof of Stake (PoS) consensus algorithm does not have the resource wastage of Proof of Work (PoW) since only a selection of node(s) is chosen to be the miner(s). In PoS, a node is chosen based on the number of assets it holds. When a miner successfully creates a valid block, it is rewarded with assets. PoS, however, is prone to concentration of power - the richest node has the highest chance to be selected as a miner and its assets are going to increase. This causes the phenomenon, "rich gets richer and poor gets poorer". Furthermore, by attacking the node with most assets an adversary can disrupt the blockchain. The Credit-PoS (Credit Model PoS) consensus algorithm proposed by the authors aims to reduce this centralization of power in blockchains that use PoS consensus.

In the Credit-PoS consensus algorithm [9], nodes have credit values that depend on their behaviour in the network. In this protocol, one is chosen to be main node using the following formula: $m = (s + h) mod\ num$ where 'm' is index of node chosen as main node, 's' is number of repetitions, 'h' length of current blockchain, and 'num' is number of nodes participating in consensus. The main node will broadcast a credit ranking request to participating nodes to send their credit ranking of other nodes. Each node calculates the credit degree of other

nodes using the Credit Evaluation Index in table1 and must reply to main node within specified time. Once the main node receives credit ranking from other nodes, it processes the credit model and then broadcasts the credit ranking of nodes taking part in consensus. To tolerate nodes that send faulty data, it is assumed that there will be 's' byzantine nodes the network. The credit evaluation processes is repeated 's + 1' times. The blockchain system must also satisfy the condition of $num > 3 * s$. Once the main node receives credit ratings from the participants, the main node using the credit model, creates credit ranking of other nodes. This credit ranking is then broadcast to all nodes participating in consensus. The nodes upon receiving this crediting, adjust their hashing difficulty according to their ranking and then start mining. PoS consensus algorithm has fewer resource consumption than

First-level indicators	Second-level indicators	Indicator description	Weights
Transaction	The total number of transactions	The total number of transactions generated after joining the network	0.1
	Currency liquidity	Amount of spending on account/ The amount of income in the account	0.15
Node performance	Network latency	Network latency	0.1
	Offline times of nodes	Node offline times	0.1
	Node liveness	(Total time of access to the network- Total offline time)/ Total time of access to the network	0.15
Node credit	Effective block ratio	Number of valid blocks submitted/ The total number of blocks committed	0.2
	Credit degree of the last round of nodes	Credit degree of the last round of nodes	0.2

Table 1: Node Credit Evaluation Metrics

the widely used PoW consensus. The most advantage of Credit-PoS system is the dynamic hashing difficulty of the participants. This can greatly motivate new nodes to participate in the mining process. Moreover, since only few number of nodes are chosen to the proposers, the high resource waste that comes in PoW can also be avoided.

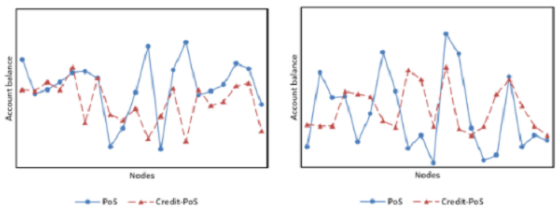
4 New Construction

Blockchains function better and use fewer resources when miners are divided into proposers and validators. Participants in a blockchain, however, must keep a copy of the blockchain. The need for more storage increases with blockchain length. It might be possible to install blockchain on devices with limited processing power if blockchain data can be archived to a small number of nodes while other nodes keep up the blockchain's signature. Negotiating on trust could be used to accomplish this.

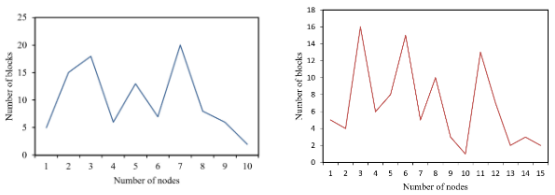
5 Evaluation

5.1 Consensus Algorithm of Proof-of-Stake Based on Credit Model

To evaluate the improvements of Credit-PoS over PoS, the authors have analyzed two aspects: concentration of property (asset worth held of nodes) and centralization of power (concentration of accounting rights) [9]. The



(a) Accounting Balance of 20 nodes before and after transactions



(b) Number of blocks generated

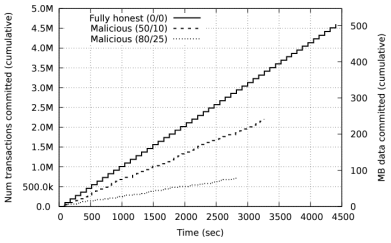
Figure 5: Performance Evaluation of Credit Proof of Stake

wealth (accounting balance) of 20 nodes that implemented PoS and Credit-PoS for the same time was measured figure 5a. From the results, it was evident that in Credit-PoS, the wealth gap of the nodes was lower than PoS before and after the transactions. The authors also used Gini coefficient to scale down the value to range [0, 1], wherein a value closer to '0' indicates uniform distribution. The Gini coefficient of PoS were higher than that of Credit-PoS,

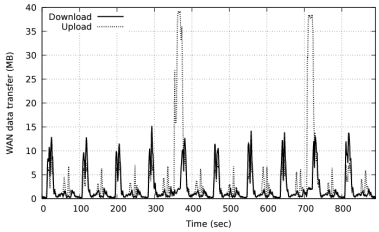
indicating the Credit-PoS to have a more uniform distribution of assets. To determine the centralization of power the authors simulated 100 times of mining using blockchain systems having 10 and 15 nodes using the Credit-PoS algorithm. From the results it was seen that number of blocks generated by nodes were non-linear - power was not concentrated. This can be attributed to the dynamic hashing difficulty of the nodes.

5.2 Blockene: High throughput and low resource usage

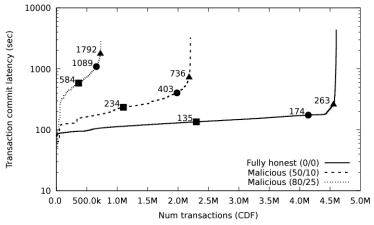
The authors built a Blockene prototype in which the citizen nodes are implemented as an Android app and the politician node is written in C++. They are designed in such a way that smartphone battery usage is extremely low. The implementation is tested for speed, latency, and load on Citizen nodes (battery/data usage). The protocol has 2000 citizen nodes and 200 Politician nodes. For 50 consecutive blocks, the throughput is assessed under three



(a) Throughput under various configs



(b) Network usage at a Politician Node



(c) Transaction Latency under various configs

Figure 6: Evaluation of Blockene based on Latency, Throughput and Network usage

conditions: 100% honesty, dishonest citizens, and untrustworthy politicians. In the scenario of perfect honesty, 4.6 million transactions are handled in 4403 seconds, for a throughput of 1045 transactions per second. If we consider the worst-case scenario for blockene, which is 25% honest citizens and 20% honest politicians, we get 257 transactions per second. Figure 6a clearly demonstrates how Blockene handles dangerous behavior smoothly. Figure 6c displays the Cumulative Distribution Function of the transaction's latency's in various configurations. They have a lag of roughly 135 seconds for complete honesty. The latency grows as the number of malicious individuals increases, yet it remains under control. The network load at a general Politician node over the course of 10 blocks is shown in Figure 6b. The Blockene program consumes just 3% of the overall battery and 61 MB of data every day, so users won't even notice it is running. The blockene performs better than most of the public blockchains and have similar transaction rate to Consortium and Algorand but at a very low cost and resource usage as shown in Figure 7.

Blockchain	*Scale of members*	*Trans.* rate	*Cost*	*Incentive needed?*
Public (*e.g.*, Bitcoin)	**Millions**	4-10 /sec.	Huge (PoW)	Yes
Consortium	Tens	**1000s /sec.**	High	Yes
Algorand	**Millions**	**1000-2000/sec.**	High	Yes
Blockene	**Millions**	**1045 /sec.**	**Tiny**	**No**

Figure 7: Comparison of blockchain architecture

6 Conclusions

As part of this paper, we reviewed many different research papers on new consensus algorithms and blockchain. These new techniques are trying to have faster transaction rates to tackle the transactions done in real world applications. Blockene can process more than 1000 transactions per second even on mobile devices. Poster Dean [1] is another consensus algorithm for EDGE computing. Conflux has a better technique to handle liveness attack and double spending attacks. Accord is another scalable blockchain used in healthcare.

But these new blockchains look better than the established blockchains on a higher level but the real test for them would be handling millions of participants simultaneously. Although their protocols are performing well in limited environment, they look hopeful to perform well as full scale applications and open new possibilities for everyone. Each of these consensus algorithms have their own assumptions and limitations, but they show promise to improve these over the years.

References

[1] A. Al-Mamun, J. Dai, X. Xu, M. Sadoghi, H. Shen, and D. Zhao. Poster: Dean: A blockchain-inspired consensus protocol enabling trustworthy edge computing. 2020.

[2] G. D. Bashar, J. Holmes, and G. G. Dagher. Accord: A scalable multileader consensus protocol for healthcare blockchain. *IEEE Transactions on Information Forensics and Security*, 17:2990–3005, 2022.

[3] J. Feng, X. Zhao, G. Lu, and F. Zhao. Potn: a novel blockchain consensus protocol with proof-of-trust negotiation in distributed iot networks. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, pages 32–37, 2019.

[4] M. Fitzi, X. Wang, S. Kannan, A. Kiayias, N. Leonardos, P. Viswanath, and G. Wang. Minotaur: Multi-resource blockchain consensus. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 1095–1108, New York, NY, USA, 2022. Association for Computing Machinery.

[5] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 3–16, New York, NY, USA, 2016. Association for Computing Machinery.

[6] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, and A. C.-C. Yao. A decentralized blockchain with high throughput and fast confirmation. In *2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20)*, pages 515–528, 2020.

[7] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang. Efficient quantum blockchain with a consensus mechanism qdpos. *IEEE Transactions on Information Forensics and Security*, 17:3264–3276, 2022.

[8] S. Satija, A. Mehra, S. Singanamalla, K. Grover, M. Sivathanu, N. Chandran, D. Gupta, and S. Lokam. Blockene: A high-throughput blockchain over mobile devices. *CoRR*, abs/2010.07277, 2020.

[9] J. Wang and L. Ge. Consensus algorithm of proof-of-stake based on credit model. In *The 2022 4th International Conference on Blockchain Technology*, pages 88–94, 2022.