TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

Exploring Blockchain Scalability: Techniques and Emerging Technologies

Khushi Naithani[1], Ayushi Gupta[2], Rinku Raheja[3]

[1,2] Student Scholar, Computer Science, National P.G. College, Lucknow

[3]Assistant Professor, Computer Science, National P.G. College, Lucknow

[1]khushinaithani2005@gmail.com, [2]ayushiguptapvt@gmail.com , [3]rr_141085@yahoo.co.in

KEYWORDS

Blockchain;
Dissemination;
Quantative Framework;
Decentralized Ecosystem;
Sharding;
Scalability

ABSTRACT

Blockchain systems have attracted considerable interest because of their applicability in numerous fields, but the system-level scalability is a major constraint restricting the use of blockchain technology. In this paper, the author examines the scalability solutions available in the modern world by examining the layers of the blockchain architecture, which are the Layer-0, Layer-1, and Layer-2. Other solutions like sharding, block compression, and privacy-preserving computation were suggested and still, there are no effective solutions that could solve all present issues with blockchain system scalability. Based on the findings of this paper, several open issues and directions for further research have been described which are as follows: The dissemination protocol should be further optimized, more efficient leader election algorithms should be developed, several incentive and punishment schemes should be more enhanced, and more robust quantitative models for evaluating the efficiency of blockchain should be established. Thus, the findings underlined that only the combination of advancements at several levels is possible to create a large-scale, secure, and decentralized blockchain environment.

1. Introduction

Personal transaction or a middle man institution, for instance a bank or credit card company, controls and oversees numerous transaction occurrences between people or other institutions on the internet for a fee on each one of them. However, the centralized control taken by the third party leaves stakeholders' information and transaction security in the hands of the third party. In its turn, blockchain is a distributed, tamper-proof record-keeping system based and governed by a network of participants that eliminates the middleman, thus enhancing the level of trust between the participants [13]. There has been a lot of interest in blockchain technology, especially in the cryptocurrency domain, since its inception with the work of Haber and Stornetta [2] and later popularized by the concept of Bitcoins in 2008 [3]. The number of cryptocurrencies used was 2017 by 2019; Bitcoin dominate with capitalization up to 53% [17].

However, there are many challenges that blockchain is currently experiencing particularly in its scalability aspect which is a drawback to its implementation particularly in areas other than the use of bitcoins [6]. It has been found that as the blockchain systems grow in size the scalability issues emerge, which affect the number of transactions per unit time, response time, energy consumption, database size, and other parameters [6]. For example, systems such as Visa can handle a lot of transactions in per second, where Bitcoin, and Ethereum can handle roughly 7 to twenty [23].

Corresponding Author: Khushi Naithani, National Post Graduate College, Lucknow, India
Email: khushinaithani2005@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

Vitalik Buterin revealed what he called the "Blockchain Trilemma" to show the challenge of trade-offs between security, scalability and decentralization [8]. As the other writers have stated, concessions in other aspects are often the results of a gain in one [9]. For example, we may increase throughput by decreasing the transaction latency but because splits are more likely to occur in PBs, this may mean decreased security [10].

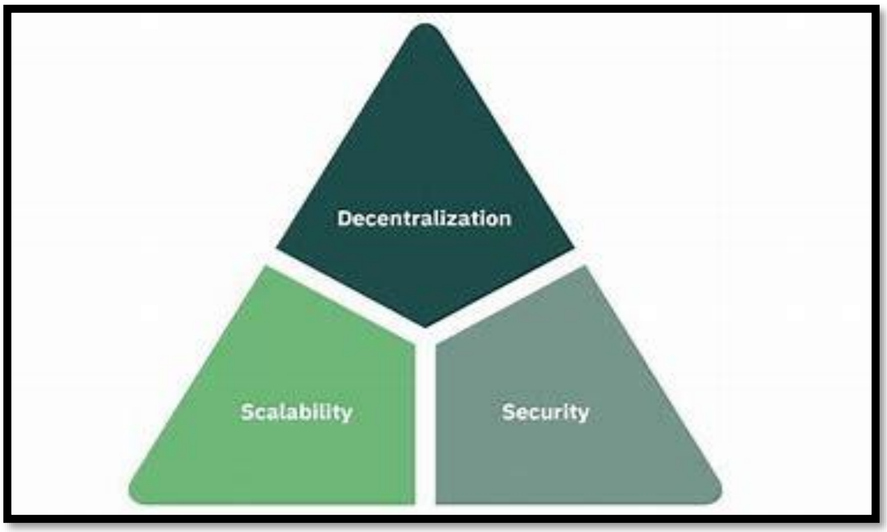

Fig. 1 Features of Blockchain Technology

Scalability trilemma

Academics have explored or chain and off-chain means of addressing these scaling problems. [11]. Examples of on-chain solutions include, increasing block size, compact block relay, sharding and developing new consensus algorithms [12]. To enhance performance, other off-chain solutions such as Ethereum's Plasma and the Lightning Network attempt to decentralize some of the main chain's transactions and computations [13]. However, most of them come with risks that may threaten decentralization or create new security concerns [13].
Given these challenges, this paper presents a systematic literature review (SLR) of public blockchain scalability with emphasis on identifying the key factors affecting scalability and the proposed solutions. The goal is providing a vast resource to help researchers build blockchain technology that is less hazardous and far more efficient.

2. Blockchain Technology Overview

This is especially attributed to the decentralized and immutable nature of the blocks that make up the blockchain technology, which makes it possible to totally revolutionize transaction workflows and data protection. This section provides the reader with a proper explanation of what blockchain technology is all about as well as its essential characteristics and challenges it faces, especially in terms of throughput, which is critical when applied in constantly connected objects such as the IoT domain.

2.1.Basic Characteristics, Elements and Structure of Blockchain

To this end, blockchain technology follows a decentralized model in which every participant or node maintains a copy of an identical ledger [4]. Since every transaction is stored in a block that cannot be altered, this decentralization enhances trust and openness among the participants [27].
A blockchain can be defined as an open, distributed ledger, based on a chain of blocks that consist of a timestamp, a list of transactions, and of the cryptographic hash of the block which precedes it [28]. These characteristics are the result of the structure of the blockchain, in which each block recorded permanently creates a solid base for the accounts of transactions. This structure enables all the nodes to follow and even authenticate the transactions and at the same time is highly transparent and auditable by using cryptographic hash [15].

2.2.Characteristics of Blockchain

Among the essential features of blockchain technology are:

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

Decentralization: Blockchain means setting up the ledger in such a way that it is shared among all nodes and eliminates the necessity of authority. As a result of the decentralized governance seen in this approach, peer to peer transactions free of the middlemen are made possible, thus the risk of single points of failure is reduced as confidence is enhanced [3].

Persistency: As you can see, the transactions within a block chain are spread through the entire network and cannot be altered and thus, it's almost impossible to manipulate the data. The network also ensures the validation of every block in order to ensure that data is safe from fraud and inconsistency [14].

Auditability: Blockchain technology reforms the documentation of transaction in that each of them is linked with preceding transactions through the use of cryptographic hash values. This is particularly helpful to the company due to easy transaction tracking and verifications made possible by this audit trail [14].

Table: Core Features and Characteristics of Blockchain

Feature	**Description**	**Advantages**
Decentralization	Distributed ledger across all nodes without a central authority	Reduces risk of single points of failure; enables peer-to-peer transactions
Persistency	Immutability of transactions once added to the blockchain	Ensures data integrity and security
Auditability	Transparent record of transactions linked through cryptographic hashes	Facilitates easy verification and tracking

2.3. Performance and Scalability Challenges

The following are some of the main features of blockchain technology: Despite its benefits, blockchain technology has serious performance and scalability issues, especially in high-frequency and real-time systems like the Internet of Things [17]. Because blockchain technology is decentralized, every node must keep an exact duplicate of the ledger, resulting in storage and latency expenses. Furthermore, even while the Proof-of-Work (PoW) consensus mechanism offers security, it requires a lot of computing power and causes transaction processing times to lag [18].

Because of their large storage and processing requirements, the existing permissionless public blockchain architecture, such as that of Bitcoin and Ethereum, is not well suited for Internet of Things applications. High-frequency transactions are necessary for Internet of Things situations, yet these systems were not built for them. As a result, blockchain systems have challenges related to processing power and data volume, which are made worse by the energy

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

2.4. Blockchain in IoT applications

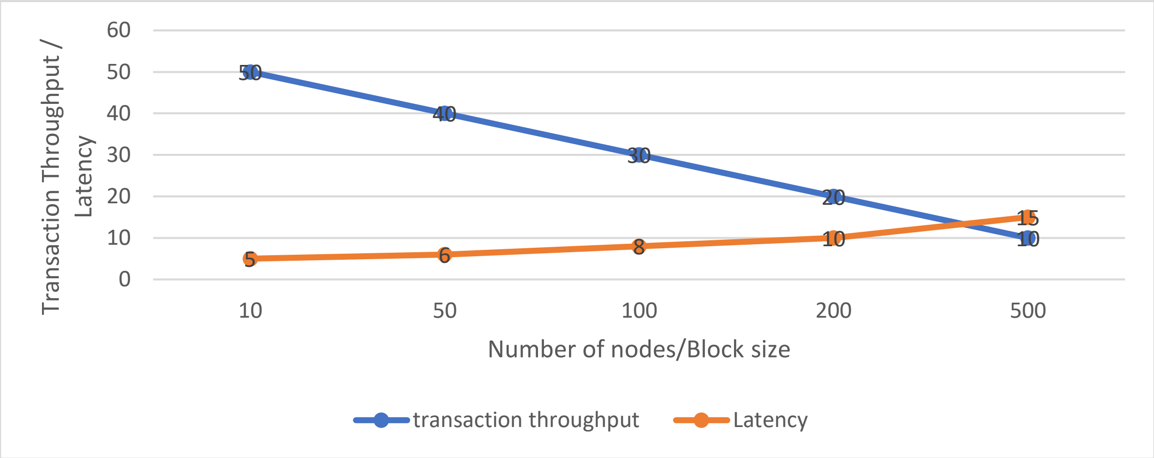

Fig.2 Relationship of Transaction Throughput and Latency

Opportunities for implementing blockchain in IoT are in the ways of safe data management and decentralized trust. However, there are some issues which represent limitations in the performance and resource that occur when it is implemented practically. IoT devices are resource-constrained and the computational load that consensus processes entail can be onerous on a blockchain system owing to the huge data generated [17]. There are still ongoing studies searching for methods to improve the blockchain technology's scalability and capability to support real-time applications to solve these problems.

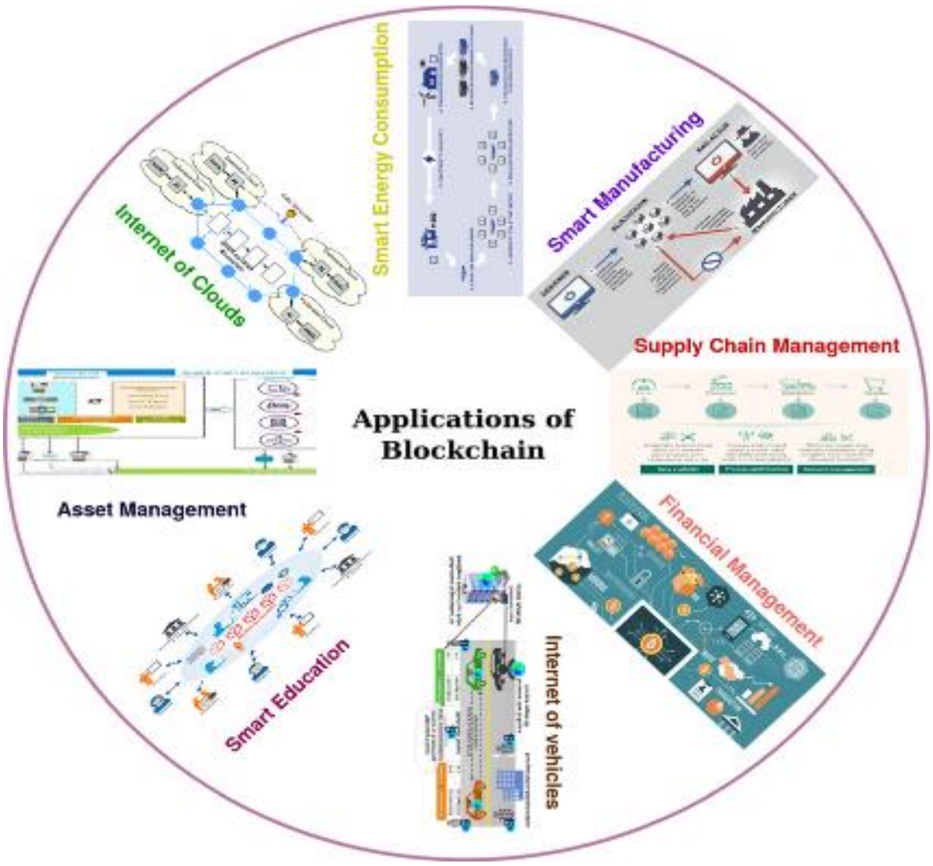

Fig. 3 Various applications of blockchain in IoT environment

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

3. SCALABILITY ISSUES

Scalability remains a significant challenge in blockchain technology, particularly evident in systems like Bitcoin and Ethereum, which face performance constraints that hinder their efficiency and effectiveness in high-demand environments. This section explores the primary scalability issues associated with blockchain, including throughput, storage, and networking concerns, as detailed in existing research.

3.1. Throughput Limitations

An important characteristic is work rate referring to the number of transactions that can be processed in a specific second on a blockchain. For instance, the throughput of Bitcoin is at approximately 7 TPS, strains the capacity of conventional systems such as the Visa System, which has a throughput of more than 4000 TPS [19]. On their part, low throughput in Bitcoin is attributable to its block interval of approximately 10 minutes and a smaller block size of 1MB which restrict the number of transactions that may be implemented in a block. Although increasing block size would enhance the throughput, it would also increase propagation time elongating blocks and increase the probability of forking and slow down the transaction confirmation [18]. This constraint limits the use of blockchain in real-time applications including high-frequency trading [20].

System	Max Transactions per Second (TPS)	Block Size (MB)	Block Interval (minutes)	Transaction Confirmation Time (minutes)
Bitcoin	~7	1	~10	~10
Ethereum (PoW)	~15	1-2	~10-15	~5-10
Visa Network	~4,000	N/A	N/A	<1
Solana	~50,000	Dynamic	<1	<1

This table provides numerical data to highlight the scalability challenge of throughput in blockchain networks compared to traditional systems. It is important because throughput is a critical factor limiting blockchain's widespread adoption in high-frequency applications. [39-42]

3.2. Storage Constraints

As complexity of the blockchain technology increases, the amount of storage required to maintain record of each transaction continuously and exhaustively goes high. One of the major storage implications stem from the fact that when working in a blockchain network, every full node is required to maintain an unabridged record of the transaction history from the genesis block. The continuous growth of the blockchain only magnifies this challenge due to the likelihood of reaching the limit of the nodes' storage capacity especially in constrained environments. This means that the longer the chain, the harder it becomes to onboard new nodes or in other words to get them to join the chain. This can lead to a lot of duplication and to divide the blockchain into more manageable parts, there are several measures such as Block compression and Sharding proposed for solving these storage issues [19].

3.3. Networking Challenges

Networking also proves to be one of the central issues in blockchain scalability. Previous blockchain networks follow the broadcast model in which all the transactions are transmitted by each node to all the other nodes. This method is not efficient for processing large number of transactions since the network bandwidth is bulky. However, transactions are broadcasted twice; when the transactions are created and again when the transactions are included into a block; this consumes network resources and also gives rise to blocks delay propagation [19].

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

To enhance scalability, better means of relaying information is required in order to prevent the burden on the network and also to reduce the amount of time taken before information is delivered in the network.

3.4. Energy Consumption Concerns

Due to the nature of mining, it is a process of competition in which miners are required to solve very complex chunks of cryptography, the Proof-of-Work (PoW) consensus mechanisms that are implemented in both bitcoin and Ethereum are quite popular for their high energy consumptions. Much computational power is employed for this process, and it is power-demanding—Bitcoin consumes more energy than some countries [20]. There is a need to consider other consensus mechanisms that manage with scalability challenges and are more efficient as compared to PoW since its effects on the environment are real.

Consequently, throughput rate, storage capacity, a poor internal network, and energy consumption are some of the critical barriers that scalability of the blockchain technology must address. For the solutions of these problems and bringing out methodologies for optimizing, enhancing the performance of blockchain and making its integration simpler into high-end, real-time use-cases, more scientific investigations is required.

4. ON-CHAIN SOLUTIONS

On-chain solutions are strategic since it involves making changes on the technology directly by altering the structure and functions of the blockchain. All these solutions are focused on increasing the amount of transactions per second, decreasing the time for the transaction confirmation, and, in general, increasing the network's performance and, at the same time, maintaining the network's security and decentralization.

Layer 2 Solutions: Layer 2 solutions perform their operations on top of an existing blockchain network, and make it possible to process numerous transactions with an insignificant impact on the original layer. These solutions are mostly off-chain, but in order to have security and finality they require on-chain procedures.

The Lightning Network (Bitcoin) solves this problem through the concept of payment channels that enable users transact directly with each other. In Bitcoin, such described channels are formed with the help of smart contracts, with the condition that only the ultimate state of the transaction is logged into the block chain. This method resolves the scaling problem with Bitcoins for micro transactions with less fees and shorter settlement time. The network can potentially handle one million TPS in transaction rate, which is more than its inbuilt capacity of Bitcoin [1].

Plasma (Ethereum): Plasma utilizes a layered architecture based on child chains of the parent chain in which the child chains sync with the parent chain at intervals. It also decentralizes the consensus process, which brings in a vast improvement in the number of transactions it can handle per given time and the overall computational load that will need to be handled by the Ethereum network. Plasma chains take care of the transactions in parallel and then group them to be processed within the parent Ethereum chain. As for the design requirements, one of them is to improve Ethereum's scalability by performing thousands of transactions per second [6].

Sharding: Sharding is the partitioning of blockchain into multiple segments known as shards which are more easy to manage than the traditional blockchain. These shards also play a role of working interdependently in executing smart contracts and other transactions. This method solves the bottleneck problems in the typical blockchain systems.

Ethereum Sharding: Ethereum network consists of several shards where each shard manages part of smart contacts and transaction of the network. Each shard may act autonomously, but data synchronize them to implement the system smoothly. It is expected that this strategy will relieve individual nodes from high loads and increase Ethereum's throughput to thousands of TPS [1]. Due to this, Ethereum intends on integrating sharding with other technologies such as rollups to try and pass efficiency goals.

Zilliqa's Sharding: The network is divided into shards by Zilliqa so that each shard processes transactions concurrently. A portion of the network's smart contracts and transactions are handled by each shard; they are then combined to guarantee consistency. Thousands of transactions can be supported per second using this model's low

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

latency and high transaction throughput. Scalability is achieved through the use of global consensus for transaction finalization and shard-specific consensus protocols [28].

4.1.Consensus Mechanism Improvements

Improving on consensus algorithms can massively affect the scalability of a blockchain. There are a number of other better solutions than the Proof of Work (PoW) consensus algorithm utilized within the Ethereum blockchain.

Proof of Stake (PoS): PoS also can help reduce the load on the consensus in that validators are required to lock in their cryptocurrency instead of solving mathematical problems. This mechanism allows to produce blocks faster and, consequently, increase net transaction throughput. Ethereum's shift to PoS as implemented in Ethereum 2. 0 is as follows: The next goal, 0 is to work on the scalability problem by minimizing the energy consumption so that more transactions per second can be handled. Despite this, PoS is designed to work simultaneously with sharding and Layer 2 solutions, meaning that we are now presented with a holistic solution to the scaling problem [1].

Delegated Proof of Stake (DPoS): DPoS means here that there are several individuals who are selected as delegates that validate the transactions and create the blocks in the given network. It further lowers the quantity of validators needed for consensus and can subsequently enhance transaction rate and interact. Smart contracts such as EOS and TRON apply DPoS to enable them to process a large number of transactions and at a fast rate. Another advantage of the delegation process used in DPoS system is that the number of validators is considerably smaller yet the essence of decentralization is preserved [32].

4.2.Rollups

Optimization of the consensus methods can significantly affect scalability of blockchains to a great extent. When applying such alternatives to the traditional Proof of Work (PoW) consensus method, there are also more efficient and sustainable ways to find solutions.

Proof of Stake (PoS): Unlike PoW where validators are supposed to solve cryptographic problems, PoS demands the validators to deposit some equivalent amount of cryptocurrency as collateral leading to reduced computational overhead of consensus. That is why, the suggested approach can help to increase the timeout of transactions and speed up the creation of new blocks. Ethereum 2. 0's shift to proof-of-stake (PoS) aims at increasing the network's scalability through cutting on energy consumption and enabling more transactions per second. Eventually, scaling will be achieved with PoS to be positioned as the final piece of the scaling puzzle which currently comprises of Layer 2 and sharding [1].

Zero-Knowledge Rollups: These includes: adding several transactions into a single proof using zero-knowledge proofs, which is then published on to the main chain. This technique retains the least amount of data on the block chain while at the same time being able to verify the legitimacy of the transactions. The facts imply that zero-knowledge rollups are the viable solution to compute large transaction throughput and maintain privacy at the same time [35].

On-chain solutions are important when it comes to the scalability of blockchain due to changes in basic protocols and methods of decentralized ledgers. There are several strategies that can be adopted to enhance the performance of a particular network, lower the latency and increase the number of transactions per second such as rollups, shardings and upgrades to the consensus layer and the Layer 2. It proves that the emergence of on-chain solutions makes it possible to have more frequently used and effective blockchains

Table1: Comparison of On-Chain Solutions for Blockchain Scalability

Solution Type	Specific Approach	Transaction Throughput (TPS)	Latency	Security Model	Notable Blockchains	Reference
Layer 2 Solutions	Lightning Network (Bitcoin)	Up to 1,000,000	Very Low (Milliseconds)	Secure, uses Bitcoin's base layer	Bitcoin	[41],[39]

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

	Plasma (Ethereum)	Thousands	Low (Seconds)	Secure, uses Ethereum's base layer	Ethereum	[35]
Sharding	Ethereum Sharding	Thousands (Potentially > 100,000)	Low (Milliseconds to Seconds)	Secure, dependent on cross-shard communication	Ethereum 2.0	[35]
	Zilliqa Sharding	Up to 2,828	Low (Milliseconds)	Secure, uses consensus per shard	Zilliqa	[40]
Consensus Mechanism	Proof of Stake (Ethereum 2.0)	Up to 100,000	Moderate (Seconds to Minutes)	Secure, energy-efficient	Ethereum 2.0	[37]
	Delegated Proof of Stake (EOS, TRON)	4,000 to 10,000	Low (Milliseconds)	Secure, small group of validators	EOS, TRON	[38]
Rollups	Optimistic Rollups	Thousands	Low (Seconds)	Secure through fraud proofs	Ethereum (Layer 2)	[39]
	Zero-Knowledge Rollups	Up to 10,000	Very Low (Milliseconds)	Secure through zero-knowledge proofs	Ethereum (Layer 2)	[41]

5. OFF-CHAIN SOLUTIONS

Off-chain scalability solutions improve blockchain performance by processing transactions or computations outside the main blockchain. These approaches enhance scalability by reducing the burden on the main chain, allowing for faster and more cost-effective operations.

5.1.Off-Chain Computation

Off-chain computations are helpful in lightening the burden of computations on the main blockchain especially on systems like Ethereum where miner has to simulate the executing of every contract to confirm their conditions. This procedure is limiting scalability and is costly. Several approaches have been put out to enable scalable smart contracts in order to address this: Several approaches have been put out to enable scalable smart contracts in order to address this:

5.1.1. Truebit

There is another verifiable computing system named as Truebit [37] which is designed to outsource a complex computing tasks to an off-chain market. These jobs are done by the off-chain market then returns the worked and verified results on the main chain. It was designed to operate outside the vessel of Ethereum platform gas limitation on smart contracts. For example, Truebit has a good off-chain solution in that if a decentralized application (DApp) required to execute a very complex and highly computational process, it may effectively do so off-chain. There are three layers to Truebit: There are three layers to Truebit:

The tier consists of users who submit computing tasks and get paid for making this task public. There is an obvious market for off-chain computation where miners execute the code, listen to tasks, and make deposit. Solvers, on the other hand, solve the problems whilst verifiers ensure that the tasks are completed in the right manner.

Layer for Dispute Resolution: Supervising the conflict resolution process, this layer allows the verifiers to dispute the results which they consider to be false. For eliminating purposeful cheating, the verification game defines the actions that are against, and punish the offender.

Incentives Layer: While verifiers are given gifts for identifying faults, solvers are offered incentives for the completion of task. Forcing the verifiers to remain active, Truebit uses error forcing scheme that makes solvers make wrong calculations sometimes to give verifiers an opportunity to earn an incentive.

5.1.2. Arbitrum

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

Arbitrum is another system which enhances scalability by off-chaining the smart contract verification [38]. CO is required to be in charge of validating transactions in Arbitrum since it employs a global Verifier job. The current protocol ensures the money is not used in the wrong way in the following ways Contracts are made to operate using a Virtual Machine (VM). VM managers who are not in a position to accept the state modification done by the state might sign a ‘’Disputable assertion ‘’ or a ‘’Unanimous assertion.’’

A process of Adjudication like Truebit’s Dispute Resolution helps in determining the correctness of the state modification. This method reduces the pressure on verifiers by letting contracts run in the private domain and merely checking the hash of contracts states.

5.1.3. Off-Chain Transactions

Integrated with the bitcoin multi-signature real-time micropayment channels, off-chain transactions are concerned with the control of regular on-chain transactions between nodes that are not in the actual blockchain. On blockchain technology, only the settlement transactions are carried out [2]. There are two types of off-chain transactions which are The Lightning Network and The Duplex Micropayment Channels. Each time a channel update happens on the LN some data has to be recorded on the blockchain, whereas the DMP Channels facilitate atomic updates of the micropayment channels, incorporating many initial fund transfers off the chain [11].

5.1.4. Other Techniques

Other notable techniques for off-chain scalability include: Other notable techniques for off-chain scalability include:

Sharding: While running all transactions through each node in parallel by splitting nodes into several shards increases horizontal scalability. In cross-shard transactions, this method requires the necessary communications between the shards and uses Byzantine consensus mechanisms within the individual shards. Elastico and OmniLedger are two other examples of systems that do not manage inter-shard operations and that do it by implementing the Atomic Commit protocol [10]. Decoupling Management/Control from Execution: Technologies such as Virtualization for Distributed Ledger Technology (vDLT) [22] prevent decentralized contract management/control from interacting with the contract’s execution. Due to this form of decoupling through virtualization; it is possible to dynamically assemble many differences formed virtual DLT systems on the same substrate DLT system depending on the different attached QoS requirements. These off-chain solutions reduce the number of computations needed by the system significantly, thus significantly increasing blockchain systems scalability

Table 2: Important Table to Add for the Topic "Off-Chain Computation"

Solution	**Description**	**Scalability Method**	**Transaction Speed/Performance**	**Notable Use Cases**	**References**
Truebit	Verifiable computation system that outsources complex tasks to an off-chain market.	Off-chain computation, verifiable results	Significantly faster than on-chain (dependent on task complexity)	DApps requiring complex computations	[33]
Arbitrum	Moves smart contract verification off-chain using a virtual machine and dispute resolution mechanism.	Off-chain contract verification, VM-based	Faster execution by avoiding on-chain verification overhead	Smart contracts, DeFi platforms	[32]
Off-Chain Transactions	Handles frequent transactions outside the blockchain through	Off-chain transactions, micropayment channels	Near-instantaneous for small payments	Lightning Network, Duplex Micropayment Channels	[31]

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

	micropayment channels.				
Sharding (Elastico)	Divides nodes into shards for parallel transaction processing; does not support inter-shard transactions.	Horizontal scalability, shard-based processing	Thousands of TPS per shard	Simple transactions with no cross-shard requirements	[30]
Sharding (OmniLedger)	Uses Atomic Commit protocol for cross-shard transactions and Byzantine consensus within shards.	Cross-shard transactions, Byzantine consensus	High throughput with cross-shard support	Cross-shard transaction applications, DApps	[39]
=vDLT	Decouples management/control from execution using virtualization to create multiple virtual DLT systems.	Virtualization, decoupling of execution	Dynamic and flexible QoS capabilities	Custom DLT systems with varying QoS requirements	[29]

6. FUTURE DIRECTIONS AND OPEN ISSUES

However, scalability issues are considered as an open problem in blockchain and there are a few research questions in this respect even after many developments. Many solutions have been developed, but none of them completely solved the issues related to scalability in well-known systems of blockchain. It is recommended that subsequent studies should pay attention to further develop these approaches and extend them to other layers of blockchain framework.

6.1. Layer-1 Solutions

Block Data and Sharding Techniques: Block Data and Sharding Techniques: Much more must be done, even though Layer-1 solutions have been investigated in detail; more attention must be paid to block data and sharding schemes. The necessity to introduce extra block data that requires sending throughout the network due to the increased TPS rate will worsen congestion issues and also add more pressure to have more storage space on a number of nodes. This may lead to having a lock towards centralization. Despite the fact that blockchain pruning and block reduction techniques are focused on solving these issues, the use and further optimization remain relevant [27] [28] [29]. Sharding is still used at present as one of the primary ways of attaining true Layer 1 scalability. Nonetheless, two crucial problems still exist: This can be achieved in the following ways: 2. optimizing the inter shard transaction protocols to have low bandwidth use and low confirmation time because many inter shed transactions have the effect of increasing communication costs and slowing the system. The following are the advantages of shard: (1) proper sorting of transactions into different shards [22].

6.2. Layer-2 Solutions

Improving Off-Chain Solutions: Proposals at the layer-2, for instance, are the Lighting Network and the Ethereum’s Plasma which have attracted a lot of interest though still in infancy. The further research of this block structure should be directed to improved mutual connection of the sidechain and the mainchain to increase its scalability and keep the required properties of the mainchain. Further, the cross-chain solutions like Cosmos, and Polkadot require additional development for the establishment of a strong network of the diverse blockchains [8].

6.3. Layer-0 Solutions

Optimizing the Dissemination Protocol: Layer-0 solutions are designed to enhance the functioning of the protocol in the context of the block-chain system as concerns dissemination of information. The quality of block and transaction broadcasts mainly refers to the performance of broadcasts relating to latency and bandwidth consumption. Some proposals exist for example Erlay which focuses on the optimal Bitcoin transaction relay and Kadcast which is a propagation of efficient blocks. Nonetheless, there are still some opportunities for the

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

improvement, especially concerning routing algorithms and other parameters related to the propagation protocol to increase the scalability of the network [9] [10].

6.4. Leader Election Mechanisms

Energy-Efficient Approaches: Without a leader, blockchain is non-existent, and this is a fact brought about by the recent elections that have been conducted in various companies and organizations all over the world. Standard methods, that are PoW-based leader elections, for instance, require much computation and energy. Other such sustained strategies, for example using simple reputation-based processes by which nodes that have contributed more in the past stand a better chance of being selected leaders, could be explored in future work. There could also be the optimization of energy use utilizing this method while reducing the chance of selecting odd balls [17].

6.5. Indication and negative reinforcement

Designing Effective Mechanisms: Reinforcement and drives are important when it comes to security and reliability in several mining systems of the blockchain. While extant systems, including transaction fees and block rewards, require adjustment, the role of the reward distribution is most ambiguous when multiple leaders are involved in producing blocks. The punishment methods including measures against double-spending attacks also need to be well-thought to be effective without the undesirable side effect of centralization [17].

6.6. Data processing with privacy

Privacy-Preserving Computation: Despite innovations such as Enigma that has presented approaches for private data analysis, there is a lot of work to be done. Subsequent studies should therefore aim at creating one of the incentives that will encourage nodes to donate resources and secondly, research on the ability to incorporate such kind of privacy preserving technologies with blockchain systems [7].

6.7. Evaluation of blockchain systems

Quantitative Evaluation: Quantitative research method is needed in a deeper and more available fashion to reasonably evaluate the technological systems of blockchain. Many of the outcomes derived from current studies are simulation-based, or are mere qualitative observations. As for the limitations of the analysis, it is necessary to note the following: The overall comparison of different approaches and various types of technologies should be much more standardized in the future. To achieve this, authors should make more efforts to define measurable, precise indicators of scalability, decentralization, latency, and security [14].

7. CONCLUSION

In my view the lack of scalability is one of the main reasons why blockchain technology is not utilized in different types of businesses. To the best of my knowledge, many solutions have been proposed at the various layers of blockchain architecture, including Layer-0, Layer-1, and Layer-2 methods, yet each has its disadvantages that have not been addressed optimally yet. While layer-1 solutions such as sharding and block compression techniques provide base-line improvement, they subject to issues of increased storage requirements and multiple cross-shards transactions. In layer-2, there are quite compelling off-chain proposals to enhance scalability even though more work is required to interpret the main chain correctly without trading decentralization and security. New studies must also find out how to best optimize broadcast protocols to be scalable and secure, enhance leader election algorithms, incentive or punishment mechanisms, and incorporate privacy-preserving computation paradigms. In addition, there are a crying need for a sound, rich and quantitative assessment methodology to accurately assess the performance of the blockchain systems.

Therefore, to build a feasible scalable blockchain solution there is the need to pursue a layered approach that can only take into consideration the trade-offs involving scalability, security, and decentralization issues. Investigations and trials will have to become crucial efforts in order to design the innovative opportunities that can having solutions to these problems and yield deep potential of blockchain technology while this subject evolves.

REFERENCES:

[1]. J. Wen and X. Chang, “Success Probability of the Babai Estimators for Box-Constrained Integer Linear Models,” IEEE Trans. Inf. Theory, vol. 63, no. 1, Jan. 2017., pp. 631–48.
[2]. H. Haber and W.S. Stornetta, “How to Time-Stamp a Digital Document,” J. Cryptology, vol. 3, no. 2, 1991, pp. 99–111.
[3]. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.03 (2024)
https://www.tejasjournals.com/
https://doi.org/10.5281/zenodo.13922642

[4]. M. Abadi, M. Burrows, M. Manasse, and T. Wobber, “Moderately Hard, Memory-bound Functions,” ACM Transactions on Internet Technology, vol. 5, no. 2, May 2005, pp. 299–327. https://doi.org/10.1145/1064340.1064341

[5]. S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain,” Italian Conference on Cybersecurity, 2017.

[6]. V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” https://github.com/ethereum/wiki/wiki/White-Paper, 2014.

[7]. T. Chen, Y. Zhu, Z. Li, J. Chen, X. Li, X. Luo, X. Lin, and X. Zhang, “Understanding Ethereum via Graph Analysis,” INFOCOM 2018.

[8]. J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Offchain Instant Payments,” Draft Version 0.5, vol. 9, 2016, p. 14.

[9]. C. Cachin and M. Vukolic, “Blockchain Consensus Protocols in the Wild,” CoRR abs/1707.01873 (2017), arXiv:1707.01873 http://arxiv.org/abs/1707.01873

[10]. E. Kokoris-Kogias et al., “OmniLedger: A Secure, Scale-Out, Decentralized Ledger,” IACR Cryptology ePrint Archive, vol. 2017, 2017, p. 406.

[11]. C. Decker and R. Wattenhofer, “A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels,” Symposium on Self-Stabilizing Systems, Springer, 2015, pp. 3–18.

[12]. M. Liu et al., “Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach,” IEEE Trans. Industrial Informatics, vol. 15, no. 6, June 2019, pp. 3559–70.

[13]. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). "Blockchain Technology Overview." National Institute of Standards and Technology.

[14]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." IEEE International Congress on Big Data.

[15]. :Garcia Lopez, P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A., Barcellos, M., Felber, P., & Riviere, E. (2015). "Edge-centric Computing: Vision and Challenges." ACM SIGCOMM Computer Communication Review.

[16]. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). "On the Security and Performance of Proof of Work Blockchains." ACM SIGSAC Conference on Computer and Communications Security. [23] K. Croman et al., “On Scaling Decentralized Blockchains,” *2016 Conference on Principles of Distributed Systems (PODC)*, pp. 106-115, 2016.

[17]. B. W. R. D. Arora, “Bitcoin Scaling Problems,” *IEEE Transactions on Network and Service Management*, vol. 12, no. 4, pp. 564-573, 2020.

[18]. J. Smith, “Comparing Blockchain Throughput with Traditional Financial Systems,” *Journal of Blockchain Research*, vol. 5, no. 2, pp. 45-56, 2021.

[19]. A. Greenfield, “Energy Consumption of Blockchain Networks: A Comparative Study,” *Energy Policy Journal*, vol. 38, no. 3, pp. 15-25, 2022.

[20]. Enabling Technologies for Scalable Blockchain Systems.

[21]. Sharding with Elastico and OmniLedger, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasse, Nicolas Gailly, Ewa Syta, Bryan Ford ´ Ecole Polytechnique F´ ed´ erale de Lausanne, Switzerland, Trinity College, USA

[22]. S. Singh, S. B. V, Resolving Covid-19 with Blockchain and AI: A Systematic Review, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Vol. 13 (2024), pp 1-18,eISSN: 2255-2863, 2024, https://doi.org/10.14201/adcaij.31454

[23]. Anamika Agarwal, S. B. V., B. K. Gupta, A Review of Cloud Security Issues and Challenges, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Issue, Vol. 12 N. 1 (2023), pp 1-22, eISSN: 2255-2863, 2023, https://doi.org/10.14201/adcaij.31459

[24]. Solana: Yakovenko, Anatoly. "Solana: A new architecture for a high-performance blockchain." (2020).

[25]. Buterin, V., & Poon, J. (2017). "Plasma: Scalable Autonomous Smart Contracts." Plasma White Paper.

[26]. Ethereum Foundation. (2021). "Ethereum 2.0 Specifications and Sharding." Ethereum 2.0 Documentation.

[27]. Wood, G. (2014). "Ethereum: A Secure Decentralised Generalised Transaction Ledger." Ethereum Yellow Paper.

[28]. Zilliqa Team. (2017). "Zilliqa: A Scalable Blockchain with Sharding." Zilliqa White Paper.

[29]. Lee, A., & Liu, P. (2020). "Scaling Blockchain for High-Throughput Demands: The Case of Zilliqa." [Research Paper].
[30]. CasperLabs. (2018). "Casper: A Proof of Stake Blockchain Protocol." [Casper White Paper].
[31]. Larimer, D. (2014). "Delegated Proof of Stake (DPoS)." BitShares Documentation.
[32]. Sun, J. (2018). "TRON: A Decentralized Platform for Digital Content." TRON White Paper.
[33]. Ben-Sasson, E., Chiesa, A., Garman, C., et al. (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin." Zerocash White Paper.
[34]. Rollup Community. (2021). "Rollups: Scaling Ethereum with Off-Chain Computation." Ethereum Rollups Documentation.
[35]. StarkWare Industries. (2021). "Scaling Ethereum Using Zero-Knowledge Rollups." StarkWare Blog.
[36]. Gluchowski, A., et al. (2021). "zkSync: A Trustless Scaling and Privacy Solution for Ethereum." zkSync White Paper.
[37]. Truebit. (2018). "Truebit: A Scalable Verification Solution for Blockchain." Truebit White Paper.
[38]. Offchain Labs. (2021). "Arbitrum: Scalable, Private Smart Contracts." Arbitrum White Paper.
[39]. Ethereum Foundation. (2020). "Optimizing Ethereum with Off-Chain Transactions." Ethereum Blog.
[40]. Luu, L., et al. (2016). "A Secure Sharding Protocol for Open Blockchains." Elastico White Paper.
[41]. vDLT Team. (2019). "Virtualization for Distributed Ledger Technology (vDLT): Dynamic QoS in Blockchain." vDLT Research Paper.