International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Navigating the Scalability Maze in Blockchain Technology – An Analysis of Scalability, Transaction Issues and Solutions

Ravi Prakash B[1*], Mohamadi Begum Y[2]

Submitted:10/03/2024 **Revised**: 25/04/2024 **Accepted**: 02/05/2024

Abstract: Recently, blockchain has garnered immense attention from both public and private sectors as the most sought-after technology. Despite its potential, scalability remains a critical challenge hindering its full realization. Blockchain provides a secure and transparent network through its features such as trust, data security, decentralization, immutability, and transparency. The potential of blockchain technology to revolutionise numerous industries has attracted a lot of attention in recent years. Scalability, however, is among the major issues preventing its mainstream use. Blockchain networks encounter capacity and speed constraints as they expand in size and complexity, which results in higher transaction fees and delays. The scalability problems with blockchain technology are examined in this paper, along with a thorough discussion of the numerous scaling solutions put out in the literature. The solutions for scalability and transaction speed can be categorized into two main groups - on-chain and off-chain. On-chain solutions include Segwit, block size increase, Sharding, Directed Acyclic Graph and Consensus mechanisms, while off-chain options encompass Interoperability technique includes payment channels, cross-chains, and side-chains and Finally, in this paper, we have covered well-known scalable consensus mechanisms and the future directions of block chain in terms of scalability and transaction throughput.

Keywords: *Blockchain, On-chain, off-chain, Interoperability, Scalability issues, Consensus, Transaction speed.*

1. Introduction

The attractions of blockchain technology in recent days include greater transparency, decentralization structure, individual control of data, Trust, and fraud tolerance. These advantages have prompted the widespread use of blockchains in practically every sector, such as Healthcare systems, cryptocurrencies, Supply chain finance, logistics monitoring, banking sectors, the Internet of things, and government agencies. Blockchain is a decentralised digital ledger mechanism that uses a computer network to store data and log transactions. In 2008, Satoshi Nakamoto, the person behind the crypto called Bitcoin, in that paper, they described how blockchain works and features like Proof-of-work (PoW), mining, incentives, transactions, and privacy [1]. Blockchain is a technology, and Bitcoin, Ethereum, and Ripple are protocols/coins that adopt blockchain technology. Blockchain, as the name implies, is a series of blocks. Having these features, the main drawback of blockchain is "scalability". So this limitation is intolerable for centralized systems such as finance and business sectors because they aim for faster transactions, at least 1,000 transactions per second, since blockchain considered an innovative technology that potentially provides tremendous benefits, academia, business, and government sectors are paying close attention to blockchain Technology. The public and private blockchain systems are the two types of blockchain systems. Public chains are permissionless where there is no need of central authority, while private chains are permissioned. Although various studies have shown that blockchains have developed for various uses, their real applicability is constrained due to slow transaction speeds, block size constraints, and chain size difficulties. These problems are known as scalability challenges and are one of the significant concerns in Blockchain Technology. Each node in a blockchain network must process and validate each transaction, which can slow the network's performance as the rate of transactions rises. This causes scalability problems. The most frequent blockchain scalability problem has to do with transaction processing time. Transactions take longer to authenticate and confirm when there are more users and transactions, which slows down transaction speeds and escalates fees. Blockchain scalability is the capacity of a blockchain network to cope with an increasing volume of transactions without experiencing performance degradation. On the other hand, transaction speed describes how quickly a transaction is processed and verified on the blockchain. Scalability issues with blockchain have been a key barrier to the development and use of this technology. The network's restricted ability to handle a huge volume of transactions at once is one of the issues with blockchain scalability. This may cause the network to become congested, cause lengthy confirmation periods for transactions, and increase transaction costs. In order for a blockchain to scale, transaction speed is also crucial. The blockchain network and transaction cost affect how long it takes for a transaction to be processed and confirmed, as well as how quickly it is processed. Transaction speeds are

[1] *Department of Computer Science and Engineering, Presidency University, Bengaluru, E-mail: ravi.pb@presidencyuniversity@gmail.com*
[2] *Department of Computer Science and Engineering, Presidency University, Bengaluru, E-mail: mohamadi.begum@presidencyuniversity.in*
** Corresponding Author Email:ravi.pb@presidencyuniversity@gmail.com*

comparatively slow on some blockchain networks, including Bitcoin which process 7 transaction per second(tps) and Ethereum process 25 transaction per second (tps) on an average [2] and the average block confirmation time is 5 and 10 minutes respectively [3] and sometimes a transaction takes between five minutes and three hours to get confirmed, and confirmation time depends mainly on current network traffic. Even though some blockchain's transaction speed exceeds 1500tps, they do not use Proof of work as a consensus mechanism. Proof of work is critical for the public blockchain because of its decentralized and peer-to-peer design, achieving public consensus and security [1]. Scalability of blockchain technology and transaction speed are thus two crucial factors for its development and use. These elements can be made more effective and appealing for a larger range of use cases by improving them in blockchain networks. A wide range of Scalability and transaction speed challenges are covered in this paper along with potential solutions in order to improve blockchain research and allow us to develop and use Blockchain applications similarly to how we presently design and use centralised system apps.

tps - Transaction per second

1.1. Working Of Proof-Of-Work Consensus Mechanism

TF - Transaction fees

SV – Value set by Miners

TV – Transaction value

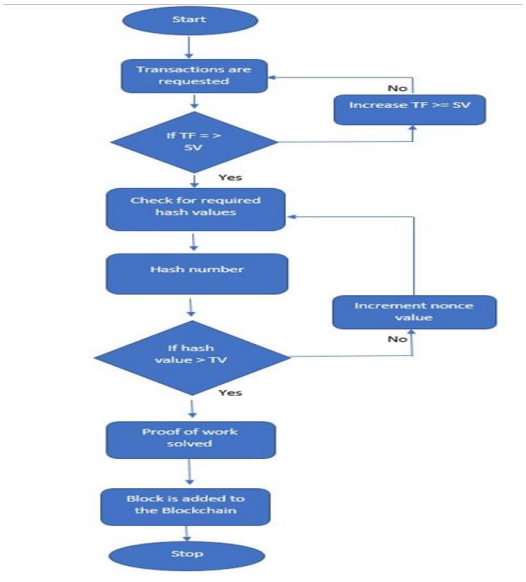


Fig 1. Working flow of consensus mechanism

The flowchart depicting how blockchain operates using the consensus mechanism is shown in Figure 1. When a user wants to start a transaction on the blockchain, they must first submit a request for the transaction, as well as the transaction fees. On the other hand, miners set some default values. If the transaction cost exceeds the miner's metric values, it is included in the block, and miners validate the block and transactions by checking the hash value. The block is validated and added to the blockchain if the miners discovered hash values that are bigger than the transaction value, i.e. the required zero bits.

1.2. Evaluation Metrics for Blockchain

The specific objectives and needs of the distributed ledger network can influence the evaluation parameters for scalability. To evaluate scalability in the frame of economic model, latency, security, and decentralisation, the following are some crucial indicators frequently employed:

1.2.1 **Economic Model**

1.2.1.1. Throughput

Throughput in a blockchain network refers to the number of transactions or activities it can process within a specific time frame, usually measured in transactions per second (TPS). A higher throughput signifies the network's ability to handle a greater volume of transactions efficiently, indicating improved scalability. This is crucial for the practical application of blockchain technology in various industries, as it ensures that the network can support a growing user base and an increasing number of transactions without compromising performance. Enhanced throughput helps maintain low latency and high reliability, making the network more robust and capable of widespread adoption.

1.2.1.2. Transaction Fees

To prevent high fees due to scalability issues, it's essential to assess transaction costs within the network. As user adoption increases, the network can become congested, driving up transaction fees. This impacts the overall user experience negatively, as higher costs can deter users from frequent or micro-transactions. Evaluating and optimizing transaction costs helps maintain affordability, thereby encouraging continued user engagement and satisfaction. Efficient scaling solutions, such as sharding or layer 2 protocols, can help manage these costs. Ultimately, a balance between scalability and cost-efficiency fosters higher user adoption and a better overall user experience.

1.2.1.3. Resource Efficiency

Measuring the resources needed for the maintenance and operation of a blockchain network involves quantifying several key factors. Processing power is essential, as it determines the network's ability to handle transactions and maintain security. This is typically gauged by the hash rate for Proof-of-Work blockchains or the number of validators in Proof-of-Stake systems. Energy consumption, another critical aspect, depends on the efficiency of the hardware used and the overall network load. Assessing these resources provides insight into the environmental impact, operational costs, and scalability potential of the blockchain, guiding optimizations and improvements for sustainable

and efficient network performance.

1.2.2 Latency

1.2.2.1. Block Confirmation Time

The time required to verify and include the newest block in the blockchain, known as the block confirmation time, is crucial for the efficiency of blockchain networks. Shorter confirmation intervals mean that new transactions are validated and added to the blockchain more quickly, reducing waiting periods for transaction completion. This accelerates the transaction processing time, allowing for a higher volume of transactions to be processed within a given timeframe. Consequently, the overall performance and responsiveness of the network are significantly enhanced, leading to better user experience and increased trust in the blockchain system's reliability and effectiveness.

1.2.2.2. Transaction Confirmation Time

Transaction confirmation time is the period it takes for a transaction to be fully processed and deemed final. This time frame is critical in both financial and digital transactions as it affects user satisfaction and operational efficiency. Faster confirmation times reduce waiting periods, making transactions more seamless and convenient for users. In financial systems, swift confirmations can minimize the risk of fraud and improve liquidity. In blockchain and cryptocurrency contexts, quicker transaction confirmations enhance the network's reliability and user trust. Overall, reducing confirmation times is essential for improving the speed, security, and efficiency of transaction-based systems.

1.2.3 Security

1.2.3.1. Consensus Algorithm

Understanding the blockchain network's consensus algorithm is essential for evaluating its security. various consensus mechanisms with various security properties include Proof-of-Work (PoW), Proof-of-Stake (PoS), and others.

1.2.3.2. Attack Tolerance

Evaluating a network's resistance to attacks like 51% attacks, double-spending, and Sybil attacks is crucial for assessing its security. A 51% attack occurs when a single entity controls the majority of the network's mining power, enabling them to manipulate transactions. Double-spending involves spending the same cryptocurrency multiple times, undermining transactional integrity. Sybil attacks involve creating multiple fake identities to gain disproportionate influence. By analyzing the network's defenses against these threats, one can gauge the robustness and reliability of the system's security measures.

1.2.4 Decentrilisation

1.2.4.1. Node Distribution

Analysing the diversity and geographic distribution of a network's active nodes involves examining how spread out and varied these nodes are globally. Better decentralization is achieved when nodes are widely dispersed and heterogeneous, meaning they are located in numerous, distinct geographical areas and operated by a diverse group of individuals or organizations. This reduces the risk of central points of failure, enhances security, and ensures the network's resilience and stability against localized disruptions or coordinated attacks.

1.2.4.2. Governance System

Examining a blockchain network's governance involves analyzing how decisions are made and who holds power. Effective governance ensures power is not concentrated in a few hands but distributed among participants, fostering decentralization. Decision-making by consensus, rather than by a single entity, enhances fairness and inclusivity. This process typically involves mechanisms like voting systems, community proposals, and stakeholder involvement, ensuring that all voices are heard and the network remains resilient, transparent, and democratic.

2. EXISTING SCALABILITY PROBLEMS

There are different factors affecting the scalability of Blockchain, and we have listed some of the prime issues in this paper:

2.1. Frequent growth of number of nodes

Since blockchain is a distrubuted technology all the nodes in the chain need to maintain full copy of whole blockchain. So It is highly challenging for every node to maintain a copy of the whole blockchain due to the increase in the number of nodes in the chain. The current bitcoin blockchain size is 398GB [4] and not all the nodes in the chain need to download the entire chain. Only full nodes keep a copy of the entire blockchain. Full nodes are the miners or nodes that will mine and validate the blocks for the chain. They need to download the entire blockchain. Another type of node is partial nodes, also called lightweight nodes, which depend on the full node for their functions. An increase in partial node servers puts much load on blockchain servers, which is one of the crucial pitfalls for scalability. In Figure 2 the graph shows how the difficulty of the network is rising as the number of nodes increases.

Fig 2. Network difficulty of a Bitcoin chain [5].

2.2. Transaction fees

The transaction fee plays a significant role for the users of the blockchain transaction fee. The users determine the fee for every transaction, prioritising transactions with higher fees. As a result, users with lower transaction fees must wait a long time for confirmation of their transactions. Sometimes there is a chance of rejecting those transactions because the fees associated with the transaction are awarded to the miners as rewards once the consensus mechanism and transaction are completed. Figure 3 shows the average transaction fees of bitcoin concerning Bitcoins.

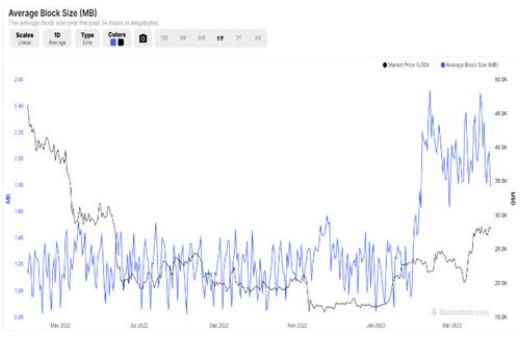


Fig 3. Transaction fees are paid to the miners by users [6].

2.3. Block size

Since the blockchain is a distributed database, Block size is the primary concern for the blockchain network performance because it needs to keep a copy of the entire blockchain along with its attributes. The average size of the bitcoin block is 1.72MB [7]. This is a diminutive figure when compared to the number of transactions happening nowadays, so it restricts the number of transactions. Additionally, most blockchain block sizes are regulated for security reasons. Figure 4 shows the average block size of Bitcoin with respect to Megabytes (MB).

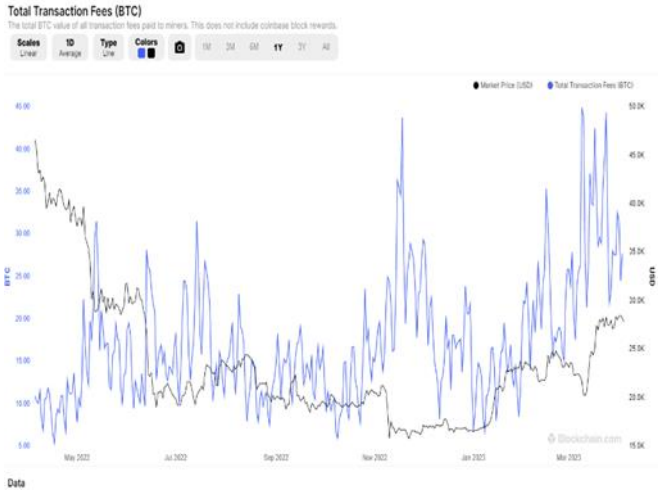


Fig 4. Average Bitcoin Block size [5].

2.4. High computational power and cost

Table 1. Shows Block time and Transaction Speed Comparison between different Blockchains.

Blockchain/protocols	*Average Confirmation Time*	*Average Transaction Speed*	*Consensus Mechanism*
Bitcoin	10 minutes	7 Tx/s	Proof of work
Ethereum	5 minutes	20 Tx/s	Proof of work
Ripple	3-5 Seconds	1500 Tx/s	Ripple(RPCA)
Visa	-----	1700 Tx/s	------
IOTA	1-5minutes	1500 Tx/s	Proof of Work
Stellar	3-5 seconds	1000 Tx/s	Stellar Consensus Protocol(FBA)
Binance smart chain	3 seconds	300 Tx/s	DPOS and Proof of Authority
Solana	5 minutes	50,000 Tx/s	Proof of History

Computing power and cost depend upon the entire block verification process (mining), i.e., the consensus mechanism. Ethereum [9] and Bitcoin [1] use proof of work as a consensus mechanism to find their block's hash and verify transactions. Recently Ethereum has shifted to proof of stake Consensus mechanism. One of the main obstacles to the broad use of blockchain technology is its scalability. As more users use the technology, the demands on the network expand, resulting in slow transaction speed and higher transaction fees. The computational power and high stake needed to conduct transactions on a blockchain network can be substantial.

The consensus mechanism utilised in the majority of blockchain networks is one of the key causes of the high processing power demand. To solve difficult mathematical puzzles, the proof-of-work (PoW) consensus method used by Bitcoin, for instance, needs a lot of computational power, which has a high energy cost and consumption. Furthermore, since blockchain technology is decentralised, all transactions must be verified by the network, which results in lengthier throughput as the network gets bigger. Because customers could have to shell out a fee to have their transaction prioritised, this might also result in greater transaction fees.

3. On-chain transactions and existing on-chain solutions

The term "on-chain transaction" describes a transaction that is handled and stored directly on blockchain. Blockchain's scalability and transaction speed are boosted in a number of ways by on-chain transactions. First, on-chain transactions eliminate the need for middlemen or external validators, which can slow down the transaction process. Faster transaction times are achieved via the decentralised network of nodes processing and verifying transactions. On-chain transactions are also more transparent and safe. It is very impossible to tamper with transaction data or influence the system because every transaction is confirmed by the network and recorded on the blockchain. Eventually, by enabling more effective resource use, on-chain transactions can aid in boosting scalability. On-chain transactions can be improved as more users conduct transactions on the blockchain to lessen network load and speed up transaction times. By doing this, the blockchain can handle growing usage in the future without compromising on speed or security. The system's trustworthiness may increase as a result of the increased security and transparency, encouraging wider adoption and use. On-chain transactions cannot be modified; these transactions need to be authenticated and validated. As a result, it takes longer to finish all of its operations because they must all be completed before transactions can be considered successful.

3.1. Sharding

Sharding is a scalability strategy for blockchain networks intended to increase blockchain processing power and lighten the strain on individual nodes [11]. Sharding is a strategy for increasing network speed by dividing the entire network horizontally into smaller slices called "shards" and spreading the load of the entire network over each shard. All shards will be placed on their own servers, and each shard will be responsible for sharing the network's workload. So the Divide and Conquer strategy is the basic purpose of Sharding as a result, this strategy aids in the escalation of transactions.

2.5 Block time

Block time is also called "block generation time" (TB). It is time a miner takes to finish the entire consensus of a block. In Bitcoins, the average block generation time is 10 minutes. Ethereum's average block time is 12 to 14 seconds [10]. Currently, there are 1500–2500 transactions per block. So if the block time is high, thousands of transactions must wait a long time. In (Table 1), we have presented the Average Block time and Transaction speed of a few blockchains across the globe.

3.1.1. Rapid Chain

Rapid chain, the first public blockchain based on sharding technique [12]. This is supposed to lead to a quicker transaction rate and lower latency in larger networks. The Intra-Committee Consensus Algorithm is used by the Rapid chain for rapid throughput with the help of block pipelining. To ensure robustness, it additionally makes use of a special large-block gossiping mechanism and a provably secure reconfiguration technique. The technology also incorporates smart contract capability, allowing programmers to design safe, decentralized, and user-friendly applications. Companies looking to automate operations, cut expenses, and streamline procedures, it is the perfect option. Rapid Chain Protocol prevents transactions from being broadcast to the entire network by using an effective cross-shard transaction verification mechanism. Rapid chain investigations reveal that it can process more than 7,300 transactions per second in a network of 4,000 nodes with an estimated confirmation delay of about 8.7 seconds. Additionally, Rapid Chain permits each committee to accept up to 33% of flawed or malicious nodes.

3.1.2. Elastico

In 2016 Elastico was proposed for public blockchains, a safe Sharding-based protocol whose goal is to construct byzantine enemies who control 25% of the computing power [13]. This protocol was created to increase transaction rates. Elastico employs PFT for intra-committee consensus and proof of work for committee establishment. As the number of shards grows, the network develops linearly. Elastico ensures that every node in the network has the same bandwidth. It is the first solution that can scale up the throughput/transaction per second (tps) as the network grows in size in a decentralized environment. The main advantage of Elastico is that there is no need for the entire blockchain to verify the blocks. Only the block can verify itself.

3.1.3. Monoxide

It is a scalable, decentralized consensus methodology based on the blockchain mechanism unless compromised

security and decentralization [14]. Monoxide introduces asynchronous consensus zones. It helps to scale the blockchain system linearly by shards in parallel. To maintain uniform mining power in each zone (shard), Chu-ko-nu mining has proposed this mining allows miners to create multiple blocks in various zones with only one POW puzzle. This saves much computational power. Monoxide Experimental Evaluates were tested with 48,000 nodes and achieved 1000x throughput and 2000x capacity when compared to Bitcoin and Ethereum.

3.1.4. Omni ledger

To address some of Elastico's issues, Kokoris-Kogias proposed Omni Ledger, a sharding-based system [15]. To ensure security, the protocol employs a bias-resistant randomness method. Omni Ledger, like Elastico, uses a Proof-of-work consensus mechanism to construct committees and PFT for intra-committee consensus. Omni Ledger can handle cross-shard transactions with a Byzantine shard atomic (Atomix) commit. To process and complete quicker transactions (up to 500 tx/s when the network reaches 1800 nodes), the OmniLedger consensus mechanism employs a variation of ByzCoin. OmniLedger will match Elastico's total resiliency and committee resiliency.

3.2. Directed Acyclic Graph (DAG)

After Ethereum was considered Blockchain 2.0, the Directed Acyclic graph emerged as Blockchain 3.0 with some revolutionary concepts. Vertices and edges are the backbones of DAG. Unlike blockchain, DAG does not consist of any blocks. All the transactions that will participate in the network are stored in the vertices, and those vertices are interconnected to each other with the help of edges. Many limitations of blockchain have been overcome with the help of DAG. There is no concept of mining in DAG, only using vertices; the transactions will work in the DAG network with no mining and transaction fees since there is no block creation, resulting in an increase in transaction speed. In DAG, a node must perform a proof of work task to submit a transaction. However, using a DAG also poses certain difficulties. As there may be several legitimate paths through the graph, it might be challenging to come to an agreement on the order of transactions in a DAG. Consensus algorithms made particularly for DAG-based blockchains, such as the Tangle consensus algorithm utilised by the IOTA coin, can be used to solve this issue. Ultimately, using a DAG in distributed ledger technology brings significant benefits in terms of scalability and transaction speed, and raises new issues that must be properly explored and resolved. And DAG is not entirely decentralized, which is the main drawback of DAG. IOTA [16], Spectre [17], DLattice [18], Nano [19], Phantom [20], XDAG [21], are some of the DAG-based systems. An overview of IOTA, Spectre, Nano, and DLattice is presented in this paper.

3.2.1. IOTA (Tangle)

IOTA is the DAG-based blockchain protocol that is most widely used [16]. IOTA is a public distributed ledger that is scalable and created primarily for the Internet of Things (Popov, S). The distributed ledger that IOTA's Tangle technology uses to transfer data and, value is public, cost-free, and scalable. Each message in the Tangle data structure is attached to two to eight preceding ones in a directed acyclic graph (DAG). Rather than being constrained to a single location for attaching new messages, you can do it across the front of the Tangle in several locations. These different attachments can be processed in parallel by the protocol. Tangle also has the characteristics needed to set up machine-to-machine micropayment protocols. Every node in an IOTA network maintains a copy of the Tangle and agrees to its contents.

3.2.2. Spectre

Spectre was introduced to overcome the scalability concern faced by the Nakamoto consensus [17]. Like bitcoin and Ethereum, the spectre protocol allows the miners to mine blocks. To achieve higher transaction rates, the spectre protocol is developed that is based on a directed acyclic graph (DAG) also, the consensus is based on proof of work to achieve high throughput and to withstand attacks up to 50%. IOTA is designed for IoT systems, whereas spectre is designed for payments.

3.2.3. DLattice

DLattice, a public blockchain protocol with an innovative double-DAG design, was proposed by Zhou [18]. To achieve user consensus, DLattice employs the DPoSBA-DAG approach (PANDA). Each account in DLattice has its own Account-DAG structure, which is combined by all accounts to form a larger Node-DAG structure. DLattice also parallelizes the creation of every account's AccountDAG, ensuring that transactions from other accounts have no effect on the current account. Data assembling, data anchoring, and data authorisation are all part of DLattice's data tokenization technique, which is based on its own structure.

3.2.4. Nano

Nano is a peer-peer, open-source, and distributed cryptocurrency network that takes zero fees and uses a block-lattice –Directed acyclic graph architecture [19]. A data structure called a "block lattice" allows for the control of individual accounts' blockchains. In Nano, every account consists of its own blockchain, and everyone in the network keeps a copy of the entire chain. Nano is a lightweight protocol designed especially for digital payment with high transaction speed. The critical point is that Nano uses a unique consensus protocol called Open

Representative Voting (ORV).

3.3. Some of the other On-chain Strategies to improve the Scalability of a Blockchain

3.3.1. Increasing Block Size

This is the primary concern that blockchain is dealing with, especially in public blockchains that use proof-of-work protocols. The larger the block size, the more transactions they can add to the block, which can help to enhance transaction throughput and reduce transaction fees. Currently, Bitcoin's average block size is 1.72 MB [23], while Ethereum is 92 KB [22].

3.3.2. Segwit (Segregated witness)

In particular, to increase the scalability of Bitcoin, Segwit is proposed. Segwit is not about expanding blocks [24]. Segwit is an update that can be done as a soft fork. The goal is to eliminate signatures and public keys because signatures are large hexadecimal values that take up nearly 60%–65% of the transaction data [25]. As a result, Segwit is proposed to remove that space, and with that free available space, more transactions can be added to a block. So, due to this, the throughput of the transactions (tps) will be boosted.

3.3.3. Bitcoin cash

Bitcoin cash was introduced in 2017 [26]. It is intended to address Bitcoin's scalability issue by increasing the chain's block size to 32MB. It is crucial to note that Bitcoin Cash is a hard fork. There is no going back once a coin has undergone a hard fork. There is no backward compatibility, so users must decide which fork they wish to use to continue transacting.

Bitcoin Cash mining: - Bitcoin Cash uses a scalable mining difficulty to ensure that transactions are always processed quickly. When the network has fewer miners, the mining difficulty algorithm adapts and gets more manageable, guaranteeing that transactions are processed promptly. Bitcoin Cash thinks it is following Satoshi Nakamoto's vision for Bitcoin's future. The bitcoin world has reacted with some scepticism to this conclusion.

3.3.4. Merkle Abstract Syntax Tree

MAST is implemented mainly to maintain data integrity and to scale cryptosystems by good code compression for the sake of permanent storage of a contract in the cryptosystems [27]. MAST is a combination of Merkel trees [23] [1] and Abstract syntax trees [28], Merkle trees which are used in Bitcoins to store the transactions efficiently. Blockchain technology uses the Merkle Abstract Syntax Tree (MAST) data structure to improve scalability and anonymity. In a MAST, the leaf nodes of the tree hold the actual data, while the other nodes have hashes of the children. As a result, only the necessary portions of the tree need to be downloaded and confirmed, resulting in less storage usage and more effective verification. A MAST can also be used to design smart contracts with hidden conditions, so only the participants of a transaction can fully understand the requirements. Compared to conventional smart contracts, where all terms are made public on the blockchain, this improves privacy.

4. Off-chain transactions and solutions

In the context of blockchain technology, off-chain transactions are those that take place away from the core network. They do not require verification by the network's consensus mechanism and are not added to the blockchain ledger, in other words. Off-chain transactions have the ability to significantly improve the efficiency and scalability of blockchain networks, especially for cryptocurrencies that are battling with excessive transaction fees and poor processing times.

Off-chain scalability solutions overcome most on-chain problems, such as computational power, transaction speed, and latency, because off-chain has been discovered to increase transaction speed outside the primary blockchain.

4.1. Interoperability

Blockchain interoperability is a crucial component that enables communication between various blockchain networks. As a result, a seamless ecosystem of decentralised networks is created, allowing for the flow of assets and data between blockchains. In the realm of blockchain, where several blockchain networks run independently, the idea of interoperability is essential. A better user experience is produced by interoperability, which encourages productivity and connectivity among different blockchain networks. Additionally, it facilitates the development of novel use cases that would not have been conceivable in a single blockchain network in the past. Cross-chain asset transfers, decentralised exchanges, and other cutting-edge blockchain-based applications are made possible through interoperability.

A fair comparison for interoperability is made with automated teller machines (ATMs), which have long been a vital part of consumer banking. When a bank customer uses a magnetic stripe card to make an ATM withdrawal, the ATM terminal contacts a host processor, which connects the machine to the ATM interbank networks. So in this analogy, two banks connect with each other to avoid consumer problems, In the same way in Interoperability two blockchain connects each other to avoid scalability problems.

There are various types of data and transactions stored on

each blockchain. Interoperability makes it possible for blockchain to communicate, access, and share information. Since the number of users and transactions is steadily expanding, the majority of permissionless or public blockchains are now experiencing scalability challenges. The two most well-known public blockchains are Bitcoin and Ethereum, both of which are experiencing performance concerns. Interoperability was thus suggested in order to lighten the load on such blockchains.

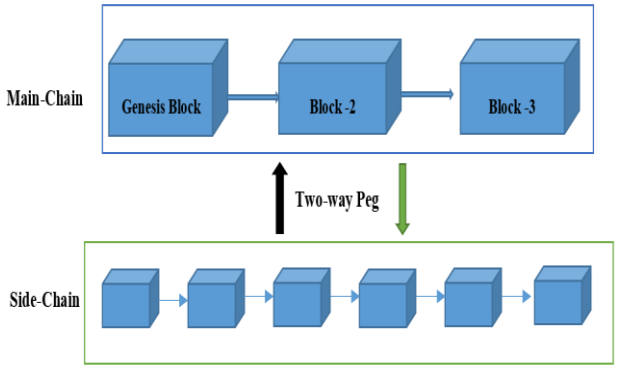
Interoperability in blockchain technology comes in the form of side chains and cross chains. A side chain is a distinct blockchain connected to its parent blockchain via two-way peg. With the help of the two-way peg, the parent blockchain and side chain can exchange data at a set rate. Typically, any subsequent blockchains are referred to as "sidechains," and the original blockchain is referred to as the "main chain". With the addition of interoperability between several blockchains, cross-chain technology, an emerging technology, hopes to address scalability issues. It implies that they can all interact with one another and exchange information.

4.1.1. Cross-Chain Technology

Cross-chain Technology is a revolutionary technology that simplifies the exchange of information between two or more blockchain networks [29]. Cross-chain technology emerged to address the scalability concerns of blockchain by enabling the Interoperability concept in the network by allowing users to connect and share data. This protocol permits data sharing between various blockchain networks and makes it possible for various blockchain networks to function together by eliminating the middleman, users can communicate among themselves through the cross-chain protocol. Therefore, blockchains that have comparable networks can exchange value and data [30].

4.1.1.1. Side chains

A sidechain is an independent blockchain that is linked to its parent blockchain via two-way peg [31]. The two-way peg technique allows the exchange of data between the main chain and sidechain by achieving Interoperability. With the use of side chains, a network can enhance its privacy and security while reducing the amount of additional trust needed to keep it running. Figure 5 shows the pictorial representation of the working of sidechains with the main chain with the 2-way peg technique. The 2-way peg technique uses the “lockbox” technique to transfer data between two blockchains. let us take a simple example of how these lockboxes are utilized to make it easier for data to be transferred from chain to chain. Consider transferring 1 BTC to a sidechain from the Bitcoin network. You start by sending a 1 BTC transaction to a specific lockbox address on the Bitcoin network. For the time being, every Bitcoin that is in the lockbox is effectively taken out of the available supply. You also specify the sidechain address where you want to transmit the BTC in that transaction. The sidechain lockbox unlocks 1 BTC and communicates it to the address specified in the Bitcoin network transaction as soon as the transaction is accepted by the Bitcoin network and added to the blockchain. To send BTC back to the main chain just carry out mentioned steps in a reverse manner.



- **Plasma**

[32] Plasma is a scalable approach to accelerate the execution of smart contracts, it is possible for plasma due to Ethereum’s account-based transaction model. Plasma is composed of two core components i.e. Map reduce functions and consensus mechanism. This design is made possible by creating smart contracts on the primary blockchain that use fraud proofs to enable state transitions to be imposed on a parent blockchain. Plasma organizes blockchains into a tree hierarchy and considers every branch as an independent blockchain with a required blockchain history and computation that is committed into Merkle proofs. Every child chain that branches off the root chain is typically run by a smart contract implemented on the parent chain.

- **RSK (Root stack Bitcoin)**

[33] Root stack is another type of 2-way pegged sidechain project which helps the Bitcoin blockchain to execute smart contracts which was not possible earlier, this communication takes place between the Bitcoin network (parent chain) and the RSK network (side chain), SBTC (Smart-Bitcoin) as their native token to transfer across the networks, in this project, Bitcoin tokens are converted to SBTC Tokens so users don’t have to convert their tokens to while utilizing the smart contracts. Every time a transfer of BTCs attempt for the RSK network occurs, those sent BTCs get blocked in the federation wallet and an equivalent quantity of SBTCs is moved to the RSK wallet and vice versa [34].

- **Polygon(Matic)**

In 2017, Matic was developed as a highly scalable sidechain solution based on the Ethereum virtual machine (EVM) architecture [35]. In 2021, Matic changed its name to Polygon, but they opted to keep Matic for their token. The layer-2 scaling architecture on the Ethereum blockchain known as Polygon is powered by the MATIC native token. With the help of the Plasma Network, which has been modified for Polygon, the Ethereum Main Net is used. Since it uses a proof of stake consensus mechanism, Polygon/Matic was initially built on the Ethereum kovan Testnet. Inadequate scalability, poor transaction rates, excessive transaction fees, and other issues with the Ethereum network are all addressed with Polygon/Matic. Chains can execute blocks relatively quickly with polygon/Matic thanks to a layer called the Block produce layer. Users may therefore create high-quality, scalable DApps using the Polygon network.

- **Lisk**

Another project focusing on side-chain technologies is Lisk [36]. Lisk allows users to develop their own applications on distinct side chains, linked to the Lisk main chain. In this technology, the main chain logs all the LSK transactions, which take place between the LSK accounts, any added features must be programmed in a side chain connected to the main chain. For a secure digital signing process, Lisk uses the "Edwards-curve Digital Signature Algorithm" (EdDSA) hashing algorithm. It also employs a delegated proof-of-stake consensus mechanism with 101 active delegates, who are chosen by the network's stakeholders based on the votes they have earned. The selected active delegates can only add blocks to the chain. A predetermined number of LSK tokens are awarded as a fee if a block is successfully added to the chain and contains up to 25 transactions per block. The block time of Lisk is 10 seconds and can process up to 25 tps.

- **Liquid**

Liquid is an open source sidechain-based platform that allows users of the liquid network to move tokens from bitcoin and Liquid network via a two-way peg [37]. The encapsulated form of the Bitcoin token is called L-BTC. In this case, the user must "Peg-in" to begin the transaction. Owners of L-BTC can use this tokenized Bitcoin on the Liquid Network. A peg-in transaction requires 102 Bitcoin network confirmations before the funds may be received on the Liquid Network. This high degree of protection is required in the event of a substantial block rearrangement of the Bitcoin chain in order to protect all participants' assets.

Table 2. Comparison of Different Side-chain Protocols/Projects.

Project/Protocol	*Main Chain*	*Native Token*	*Consensus Mechanism*	*Smart ontracts*
Plasma	Ethereum	Ether	Proof-of-Stake	Yes
Rootstack Bitcoin	Bitcoin	Smart Bitcoin (RBTC)	Proof-of-work	Yes
Polygon	Ethereum	Matic	Proof-of-stake	Yes
Lisk	Lisk	LSK	Delegated Proof-of-Stake	Yes
Liquidity Network	Bitcoin	BTC	------	Yes
Polygon	Ethereum	Matic	Proof-of-Stake	Yes

4.1.1.2. Hashed Time-lock Contract

Time-lock hashed A unique feature known as a contract is utilized to generate smart contracts and is a common component of decentralized smart contracts [38]. The lightning network initially used HTLC by integrating it into payment channels. Hash lock and the time contract are the two major parts of HTLC [39]. With HTLC, the sender generates a key before hashing it. The hash is stored in pre-image as a storage where it is exposed during the last transaction. After a predetermined amount of time has passed or a particular number of blocks have been generated, HTLC will expire. Where the timer CheckLockTimeVerify (CLTV) and CheckSequenceVerify (CSV) are the two time locks that make up the next crucial part of the HTLC time lock with the aid of CLTV, tokens can be locked and released so that they can be released only after a specified day and time or at a certain height of Block size. CSV, on the other hand, is not time-dependent, rather, it uses the quantity of blocks generated as a monitoring indicator to choose when to complete a transaction.

4.1.1.3. Atomic Swaps

Atomic swaps, also referred to as atomic cross-chain trading, is a technology that enables traders to exchange two cryptocurrencies directly between themselves without the need for a third party or trust [40]. This technology satisfies the concept of programmable, decentralised currencies by enabling digital asset exchanges over blockchain technology. Developer Sergio Demian Lerner wrote the initial version of a trustless exchange protocol in July 2012 [41]. However, Nolan is largely credited with creating atomic swaps since in May 2013, he published a detailed overview of the process.

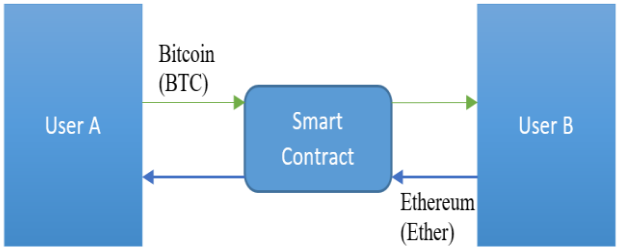


Fig 6. Representation of Atomic Swap.

In Figure 6 User A has Bitcoin BTC while User B has Ethereum Ether. While user A wants ether, user B wants BTC. With the aid of an atomic exchange, they both decide to trade. When User A deposits bitcoins into a contract, a hash is generated as a result. This hash operates similarly to a safe's lock. The value that User A creates in a data string serves as a key to unlock those monies from this fictitious safe. Then, in order for User B to complete his part of this contract's transaction, he transmits it to User B. The identical process is followed by user B, who uses the same hash as user A to deposit his Ethereum into the contract address. In this manner, the same key is used to lock both monies. The key needed to access User B's bitcoins from User A's address is made public when User A Sends User B Ethereum from his address.

4.1.1.4. Notary Mechanism

Notary Mechanism is a type of Interoperability mechanism, but this scheme is centralized, which implies two parties must go through an intermediary in order for it to work, which is against the core concept of Blockchain technology [42] [43]. This Scheme is encouraged only when both parties agree on a centralization to employ the notary scheme. One of the main protocols of the notary mechanism is inter-ledger, which enables the movement of funds between two different blockchain systems via an intermediary called "connectors." The third-party connectors can be considered a type of notary for cross-chain transactions, allowing users from various blockchains to move money to one another.

4.1.1.5. Blockchain Routers

Blockchain routers provide interoperability between various blockchain networks. According to the design of the blockchain router, the many blockchain networks, including Bitcoin, Ethereum, etc are seen as terminal components known as sub-chains in the routing network. Sub-chains cannot directly communicate with one another; instead, they can only interact through a blockchain router. For instance, the blockchain router facilitates communication across sub-chains via a cross-chain communication protocol. A blockchain stores all of the data registered on subchains. The blockchain router allows communication between subchains and builds a trust bridge across chains [44].

4.2. Payment Channels

A transaction system works off-chain. Because the blockchain's purpose is to work with a distributed ledger mechanism (i.e. without a central authority), transactions are routed through the micropayments network channels. Therefore, scalability is the only significant challenge. This method can be overcome by increasing the transaction rate and decreasing the confirmation time. The primary goal of the payment channel is to lower the primary chain's transaction weight without compromising the network's overall transaction efficiency.

There are two distinct categories of payment channels: unidirectional and bidirectional

- **Unidirectional payment channels**

One-way transactions involving two parties typically use unidirectional payment mechanisms. They are frequently utilised in scenarios where one party pays another party repeatedly, such as in the case of subscription services. The sender deposits a particular amount of digital assets into the channel, and the parties create a channel on the blockchain for this kind of payment channel. After that, until the channel is closed, the recipient can gradually withdraw these assets. The final balance is documented on the blockchain when the channel has been closed.

- **Bidirectional payment channels**

For two-way transactions between two parties, bidirectional payment channels are employed. They are frequently employed when parties have an ongoing relationship and need to do continuing business with one another. In this kind of payment channel, both parties contribute a fixed quantity of digital assets to the channel, after which they can transfer assets back and forth without needing to log each transaction on the blockchain. Until the channel is closed, every transaction alters the balance until the final balance is recorded on the Blockchain.

Scalability, high transaction speed and transaction fees problems with blockchain technology have a viable answer in the form of payment channels. They enable quick, safe, and private payments among participants without requiring that each transaction be recorded on the blockchain. Here we have listed out some of the Bi-directional payment channels and Trinity channel supports both Unidirectional and Bi-directional channels.

4.2.1. Some of the well-known Scalable Payments Channels

4.2.1.1. Lightning network

The Lightning Network is Bitcoin's scalable off-chain Instant Payment solution It is a decentralized system uses state channel technology to transfer transactions across the

network of micropayment channels and it it follows Bidirectional payment networks design. [45]. The network can handle a higher number of transactions per second and achieve scalability by enabling multiple, off-chain transactions between participating nodes. The Lightning Network, which is constantly being upgraded by the development community, can handle a certain amount of transactions depending on the number of nodes in the network and their capability.

4.2.1.2. Raiden Network

Off-chain scaling ideas for Ethereum include the Raiden network. It is similar to Bitcoin's Lightning Network in terms of implementation [46]. The Raiden Network enables Ethereum payments to be made quickly, cheaply, and scalable. On the Ethereum blockchain, the Raiden network enables all ERC-20 token transfers. The ERC token is a technical standard token that can only be used on the Ethereum network. The Raiden network is built on smart contracts. It uses digital signing and hash-locking to move tokens without relying on global consensus. It is known as "balance proof". Raiden networks are inexpensive because they do not use global consensus.

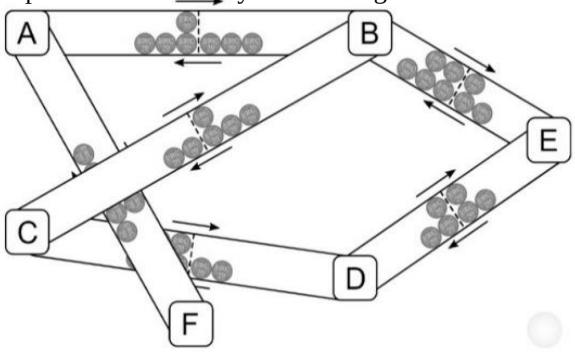


Fig 7. Working of Raiden Network. [47]

4.2.1.3. Trinity

Trinity is Neo's Off-Chain Scaling Solution that is designed to support unidirectional payments. Real-time payments with minimal transaction fees and excellent scalability are possible because of the state technology [48]. State channels enable many transactions to be performed off-chain exceptionally quickly and resolved on-chain to assure security. The Trinity network uses the Neo UTOX and NEP-5 as its standard tokens. A Channel Service Layer (CSL), a Channel Network Layer (CNL), and a State Channel Layer comprise the Trinity Framework (SCL). To serve DAPPs independently, both the Trinity logic layers and the blockchain are entirely divided from each other. Proof of Asset as Consensus achieves scaling and security. The Trinity State channel is a free channel that encourages more people to adopt the micropayment eco-habit.

4.3. Some of the well-known Scalable and high speed transaction Cross-chain chains

4.3.1. Polkadot

Polkadot is open-source blockchain technology and cryptocurrency built by Ethereum co-founder Gavin Wood [49]. It integrates blockchains by allowing separate chains to securely exchange messages and conduct transactions with one another without the need for an intermediary. This enables data or asset transfers between blockchains and the creation of cross-chain DApps using the Polkadot Network.

4.3.2. Blocknet

Blocknet is a blockchain protocol that allows for communication, interaction, and exchange across public and private blockchains and connecting to off-chain APIs and services via oracles [50]. This dramatically expands development capabilities and creates a new generation of robust blockchains and services. The Blocknet has its token called Block uses a proof of stake consensus mechanism.

4.3.3. Cosmos

Cosmos is a network of parallel blockchains that uses BFT consensus algorithms like Tendermint. Cosmos is a scalability and collaboration blockchain ecosystem [51]. Until Cosmos, blockchains were separated and unable to communicate. They were complex to build and faced transaction speed problems. Cosmos takes a new look at these concerns. Using Cosmos, we can connect Ethereum and Bitcoin networks, and also Cosmos additionally offers shared security. The Cosmos Hub has its token called ATOM. The Cosmos Hub receives transaction fees and staking rewards in exchange for securing the Hub's services by staking ATOM.

4.3.4. Rollups

Rollups are a layer 2 scalability option that tremendously speed up transactions and lower expenses. A rollup is an Ethereum mainnet smart contract that combines several transactions into one transaction and publishes it in the network. To do this, the transactions are storing on a sidechain, a different blockchain that is linked to the Ethereum blockchain [52]. This has the potential to significantly improve network effectiveness and reduce transaction costs The Ethereum mainnet can accept a single proof that was produced by the sidechain after it had verified the transactions. Following a successful verification by the mainnet, the main Ethereum blockchain is updated to incorporate the latest data. Rollups have the opportunity to revolutionize blockchain and increase its availability to a more number of users due to their capacity to handle high volumes of transactions.

ZK-Rollups (Zero-Knowledge Rollups) and Optimistic Rollups are the two main varieties of rollups. While both strategies seek to be scalable, they employ various

methods for transaction processing and validation.

4.3.4.1. ZK-Rollups

ZK-Rollups combine several transactions into a single proof using zero-knowledge proofs, which is subsequently published on the main blockchain [53]. This cryptographic proof demonstrates the validity of the bundled transactions without disclosing their specifics. ZK-Rollups assure transaction validity while preserving privacy and scalability by using zero-knowledge proofs. ZK-Rollups have the benefit of offering solid security guarantees because all transactions are verified on-chain using zero-knowledge proofs.

4.3.4.2. Optimistic Rollups

These rollups adopt a new strategy by processing transactions off-chain and publishing to the main blockchain only a compressed or summarised proof of the transactions. The summary contains details on the state changes brought on by the completed transactions. Transactions are assumed to be valid in Optimistic Rollups by default, and any potential invalid transactions are contested afterwards during a dispute period. The consolidated transactions are included on the main blockchain and are deemed final if no challenges are brought up.

When compared to ZK-Rollups, optimistic rollups offer quicker transaction processing and reduced costs. However, they add a challenge phase where users can contest transactions, which increases complexity and raises the possibility of transaction completion delays.

5. Scalable consensus mechanisms

Consensus mechanisms are crucial for enhancing scalability. Each consensus mechanism employs distinct algorithms and methods to ensure validations, thereby making the blockchain secure and scalable. Figure 8 illustrates several consensus mechanisms that contribute to addressing blockchain scalability.

5.1. Proof-of-Stake (PoS)

Sunny King and Scott Nadal created the Proof of Stake mechanism, which was first used in PeerCoin in 2012. In this system, coin holders govern the network, generate new blocks, and ensure the chain's security. Instead of miners, PeerCoin designates its block producers as "ministers." The PeerCoin protocol utilizes a concept called "coinage" to select which minister will create the next block. Coinage is calculated by multiplying the number of coins in a user's wallet by the duration (in days) those coins have been held [54] [55]. Therefore, a minister with a high coinage would have a substantial number of coins that have been in their wallet for a considerable period.

To be eligible to mine new blocks, ministers must hold coins in their wallets for at least 30 days. The blockchain faces a well-known risk of 51% attacks, where if one or more nodes gain control of 51% of the network's CPU power, they can potentially execute malicious activities.

5.2. Practical Byzantine Fault Tolerance

Barbara Lisker and Miguel Castro developed PBFT, which stands for Practical Byzantine Fault Tolerance [56]. PBFT is designed to optimize network capability in dealing with Byzantine faults, where a network must reach a clear consensus even if some nodes are trying to distribute false information. PBFT achieves this by employing a Byzantine State Machine approach, replicating servers and coordinating client actions with these server copies. This ensures fault tolerance and allows the network to manage thousands of transactions per second with minimal overhead. PBFT was among the first studies addressing Byzantine faults and achieving consensus. [57] A significant benefit of PBFT is its ability to improve transaction speed in blockchain networks by processing multiple transactions simultaneously across different nodes, enhancing scalability and accelerating transaction processing times. The PBFT algorithm can handle Byzantine faults in up to one-third of the nodes. [58] The concept of Byzantine fault tolerance originated from the Byzantine Generals Problem, which led to the development of PBFT.

5.3. Proof of Elapsed Time (PoET)

PoET tackles the scalability challenge by using trusted execution environments (TEEs), such as Intel's Software Guard Extensions (SGX) or similar technologies. These TEEs provide a secure and tamper-proof environment for code execution. In PoET, each participant requests a random wait time from a trusted authority within a TEE [59]. The participant with the shortest wait time gets to propose the next block. PoET stands out for its efficient resource use. Unlike PoW, it does not require participants to perform resource-intensive computations, allowing them to conserve energy by simply waiting for their assigned time. This makes PoET a more sustainable consensus algorithm. The PoET algorithm is secure and resistant to various attacks, relying on the assumption that TEEs are secure and that the trusted authority generates wait times fairly and impartially. The random wait time mechanism ensures a fair selection process, as participants cannot influence or predict the outcome. While PoET has notable scalability features, it also has drawbacks. Its dependence on TEEs introduces a significant point of trust in the system. If the TEEs or the trusted authority are compromised, the security of the consensus algorithm is at risk. Additionally, the algorithm might advantage users with faster hardware or easier access to TEEs, potentially leading to centralization.

5.4. Delegated Proof of Stake (DPoS)

Delegated proof of stake (DPoS) operates similarly to proof of stake (PoS) but adds a voting and delegation feature to encourage users to secure the network with their staked assets. To participate in both PoS and DPoS, users must stake their coins. In DPoS, successful block creation requires network users to elect witnesses or delegates, who are the only ones authorized to validate transactions. These elected individuals are known as "block producers" or "witnesses." [60] Voting in a DPoS system involves pooling your coins in a centralized staking pool and assigning them to a specific delegate.

5.5. Proof of Quality-of-Service (PQoS)

Another scalable consensus method is Proof-of-Quality (PoQ), where the network is split into smaller regions. Within each region, a node is chosen based on its service quality. Subsequently, the selected nodes undergo a deterministic Byzantine Fault Tolerance (BFT) consensus process . By minimizing the chance of double spending (forks) in the blockchain, PoQ aims to prevent double spending incidents. During each block proposal cycle, a node is appointed in each partitioned region based on its QoS score to propose transactions for inclusion in the network. These nodes then form a committee and use deterministic Byzantine agreement protocols, such as Practical Byzantine Fault Tolerance (PBFT), to reach consensus on the block. Despite this, some researchers contend that this system lacks adequate security, as an attacker could potentially create a fork [61]. For example, if a malicious node controls more than one-third of the voting power, it could broadcast two different blocks simultaneously, causing conflicting information and resulting in a chain fork and a loss of network trust. Therefore, more robust solutions are necessary to maintain blockchain integrity and protect against vulnerabilities exploited by malicious actors [62].

6. Future directions.

6.1. Hybrid Blockchain Technology

Incorporating the benefits of both public and private blockchains, hybrid blockchains are a subset of blockchain technology. Private blockchains are capable of handling many transactions more quickly than public blockchains, but they frequently lack the security and transparency that are built into public blockchains. Public blockchains, on the other hand, provide greater security and transparency, however they sometimes have scaling issues. By combining the scalability of private blockchains with the security and transparency of public blockchains, hybrid blockchains aim to obtain the advantages of both types of blockchains. By using a variety of technical tools, such as permissioned access to the blockchain network, selective data encryption, and consensus methods that facilitate quick transaction processing, this integration is made possible.

6.2. Hardware and Algorithm Innovations

Researchers are looking into new hardware options that can speed up the processing of blockchain networks. They include quantum computing developments as well as customized chips created exclusively for processing blockchain data. Blockchain operations can be made more efficient by using quantum computing methods like quantum annealing and quantum-inspired algorithms. These methods might make blockchain processes like transaction validation and consensus algorithms more effective.

6.3. Smart Contract Optimisation

Scalability optimisation of smart contracts is a vital part of blockchain development. Smart contracts are agreements that automatically carry out their obligations because they are encoded in code. They are carried out via decentralised, distributed blockchain networks. Smart contracts can automate intricate business procedures by self-executing. This is known as optimizing smart contracts. But they might be slow and resource-consuming. To minimize the influence of smart contracts on blockchain performance, research in this area tries to optimize them. In conclusion, optimising smart contracts in the blockchain's in the potential future entails enhancing gas efficiency, investigating scaling options, taking into account alternate consensus mechanisms, enabling interoperability, boosting security through formal verification, and enhancing usability and developer experience. Through these initiatives, smart contracts in the blockchain ecosystem will reach their full potential by addressing existing issues, improving performance, and overcoming present constraints.

6.4. Usage of Cutting-Edge Technology

Emerging technologies like quantum computing, machine learning, and artificial intelligence may be employed to increase the scalability and transaction speed of the blockchain. So more research should be focused on the mentioned areas by merging two technologies

Ultimately, there are many potential routes for future study in the areas of blockchain scalability and transaction speed, and it is essential to keep innovating in these areas if blockchain technology is to succeed over the long term and be widely used.

7. Conclusion

Blockchain was created as a distributed, decentralized, and peer-to-peer network that enables users to store and communicate data over the network. Despite having these features, blockchains are still lagging behind when it comes to being used in real-world applications like

education, banking, finance, healthcare, and other governmental and private sectors. Blockchain is currently exclusively limited to cryptocurrencies and similar types of use cases. Blockchain congestion can delay transaction processing times and escalate transaction fees due to the increasing number of participants and transactions. The security and decentralisation of the blockchain may also be compromised by various scaling options, including sharding. In conclusion, blockchain scalability and transaction speed concerns are critical and call for ongoing innovation and development. There have been several approaches put forth to deal with these difficulties, but much work needs to be done before blockchain technology can fully realise its potential. However, there are many applications that can be done utilizing blockchain, and only a few applications are available in the market with blockchain technology because scalability issues are a significant downside of public blockchains. In this study, a number of problems related to scalability are discussed, including transaction fees, the number of nodes, block delays, and the need for high levels of computational power. These constraints make blockchain less scalable than other technologies. Blockchain use in practical applications has been the subject of extensive research. In this Review, we have tried to cover the scalability problems that blockchains are now experiencing with respect to scalability, and the existing solutions to such problems. In summary, blockchain scalability and transaction speed are difficult problems that call for a diverse strategy to solve. Although there isn't a single, complete solution, researchers are looking into a number of interesting directions to boost blockchain performance and enable it to realise its full potential.

References

[1] Nakamoto, S., 2009. Bitcoin: A Peer-to-Peer Electronic Cash System

[2] median-confirmation-time.(n.d.). Blockchain.Com.

[3] Bhalla, A., n.d. TOP CRYPTOCURRENCIES WITH THEIR HIGH TRANSACTION SPEEDS. [online] Blockchain-council.org.

[4] blocks-size. (n.d.) (2022). Blockchain.Com. Available from: https://www.blockchain.com/charts/blocks-size

[5] Blockchain.com | Charts - Network Difficulty. (n.d.-d).

[6] Blockchain.com | Charts - Total Transaction Fees (BTC). (n.d.).

[7] avg-block-size. (n.d.). Blockchain.Com. Available from:

[8] Blockchain.com | Charts - Blockchain Size (MB). (n.d.).

[9] Ethereum Whitepaper | ethereum.org. (n.d.). In ethereum.org.

[10] Smith, C.(2022).Ethereum. (n.d.). Blocks. Ethereum.Org. Available

[11] Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019, June). Towards Scaling Blockchain Systems via Sharding. Proceedings of the 2019 International Conference on Management of Data, 123–140. https://arxiv.org/abs/1804.00399

[12] Zamani, M., Movahedi, M., & Raykova, M. (2018, January). RapidChain. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 931–948. https://doi.org/10.1145/3243734.3243853

[13] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. 2016. A Secure Sharding Protocol For Open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 17–30. https://doi.org/10.1145/2976749.2978389

[14] Wang, J. (2019). Monoxide: Scale out Blockchains with Asynchronous Consensus Zones. USENIX Symposium

[15] E. Kokoris, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, (2018) “Omniledger: A secure, scale-out, decentralized ledger via sharding,” in IEEE Symposium on Security and Privacy (SP), pp. 583–598. https://eprint.iacr.org/2017/406.pdf

[16] [IOTA Wiki. (2018). Iota.Org.

[17] Yonatan Sompolinsky, Y. L. (2016). SPECTRE: Serialization of Proof-of-work Events: Confirming Transactions via. eprint.iacr.org, 66

[18] Zhou, T., Li, X., & Zhao, H. (2019). DLattice: a permission-less blockchain based on DPoS-BA-DAG consensus for data tokenization. IEEE Access, 7, 39273-39287.

[19] LeMahieu, C. (2018). Nano: A feeless distributed cryptocurrency network. Nano [Online resource], 4.

[20] Zohar, Y. S. (2018). PHANTOM: A Scalable BlockDAG protocol.Iacr.org,26.Availablefrom:https://eprint.iacr.org/eprintbin/getfile.pl?entry=2018/104&version=20180330:121321&file=104.pdf

[21] XDagger. “Xdag/WhitePaper.md at Master • XDagger/Xdag.” GitHub, 3 Jan. 2022, https://github.com/XDagger/xdag/blob/master/WhitePaper.md

[22] Ethereum Average Block Size. (n.d.). YCharts. Available from: https://ycharts.com/indicators/ethereum_average_block_size

[23] Gupta, S. S. (2017). Blockchain. IBM Online (http://www. IBM. COM). Available from: https://www.isical.ac.in/~debrup/slides/Bitcoin.pdf

[24] Lombrozo E., L. J. (2015). Segregated witness (consensus layer). Retrieved from https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[25] Sanka, A. I., & Cheung, R. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. Journal of Network and Computer Applications, 195. https://doi.org/10.1016/j.jnca.2021.103232

[26] Bitcoin Cash - Peer-to-Peer Electronic Cash. (n.d.). Bitcoin Cash. Available from: https://bitcoincash.org/

[27] Rubin, J., and Naik, M. V. (2014). Merkelized Abstract Syntax Trees. Mit.Edu. Available from: https://ird.sut.ac.th/e-journal/Journal/pdf/180101317.pdf

[28] Wikipedia contributors. (n.d.). Abstract syntax tree.Wikipedia. Available from: https://en.wikipedia.org/wiki/Abstract_syntax_tree

[29] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Cross-chain interoperability among blockchain-based systems using transactions," The Knowledge Engineering Review, vol. 35, 2020, doi: 10.1017/s0269888920000314.

[30] "Blockchain Mohamadi Begum Y., R. P. B. (2024). An Efficient and Scalable Framework for Decentralized Finance Application Using Blockchain Interoperability. Journal of Electrical Systems, 20(1s), 712–727. https://doi.org/10.52783/jes.814

[31] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," Journal of Network and Computer Applications, vol. 149, p. 102471, Jan. 2020, doi: 10.1016/j.jnca.2019.102471.

[32] J. Poon and V. Buterin, ''Plasma: Scalable autonomous smart contracts,'' White Paper, 2017, pp. 1–47. [Online].

[33] M. Morgado, "RSK: Bitcoin smart contracts (EN)," Coinmonks, Jul. 27, 2018. https://medium.com/coinmonks/rsk-bitcoin-smart-contracts-en-5b474ce87cd6 (accessed Nov. 08, 2022).

[34] S. Demian Lerner, "RSK Bitcoin powered Smart Contracts," White paper, p. 24, [Online].

[35] "Polygon and Matic: What's the Difference – crypto.news," crypto.news, Sep. 07, 2022

[36] Z. Hintzman, "Comparing Blockchain Implementations," nctatechnicalpapers, p. 29, 2017, [Online]. Available: Comparing Blockchain Implementationshttps://www.nctatechnicalpapers.com

[37] "Technical Overview — documentation," docs.blockstream.com.

[38] Boyd, C., Gjøsteen, K., & Wu, S. (2020). A Blockchain Model in Tamarin and Formal Analysis of Hash Time Lock Contract. In 2nd Workshop on Formal Methods for Blockchains (FMBC 2020). Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

[39] J. Poon and T. Dryja. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. [Online]. Available: https://www. bitcoinlightning.com

[40] M. Herlihy, "Atomic Cross-Chain Swaps," Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Jul. 2018, doi: 10.1145/3212734.3212736.

[41] D. V. FRM CFA, "Atomic Swaps," WallStreetMojo, Mar. 03, 2020.

[42] A. Xiong, G. Liu, Q. Zhu, A. Jing, and S. W. Loke, "A notary group-based cross-chain mechanism," Digital Communications and Networks, Apr. 2022, doi: 10.1016/j.dcan.2022.04.012.

[43] "World Economic Forum | widgets.weforum.org.

[44] S. Jhonson, P. Robinson, and J. Brainard, "Sidechains and interoperability," arxiv, vol. 1, p. 8, 2019, doi: https://doi.org/10.48550/arXiv.1903.04077.

[45] Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

[46] The Raiden Network [Internet]. High-speed asset transfers for Ethereum: - (n.d.). Available from: https://raiden.network/

[47] Raiden Network. (n.d.). https://raiden.network/101.html

[48] David Yiling Li, G. Z. (n.d.). Trinity White Paper. 20. Available from: - https://www.trinity.tech/#/writepaper

[49] Gavin Wood.POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK Available from-https://polkadot.network/PolkaDotPaper.pdf

[50] blocknet. (n.d.). Retrieved from Blocknet Documentation, Available from: https://docs.blocknet.co/

[51] cosmos. (n.d.).RetrievedfromCosmos: Available from:https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

[52] Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2021). Recent developments in blockchain technology and their impact on energy consumption. arXiv preprint arXiv:2102.07886.

[53] Gluchowski, A. (2019). Zk rollup: scaling with zero-knowledge proofs. Matter Labs.

[54] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).

[55] Peercoin — The Pioneer of Proof-of-Stake. (n.d.). Peercoin. https://www.peercoin.net/

[56] Castro, M., and Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery (Vol. 20, Issue 4).Association for Computing Machinery (ACM). https://doi.org/10.1145/571637.571640

[57] D. H. R., M. ., Mohan, K. G. ., Augustine, J. ., & Patra, G. K. . (2023). An Approach to Improvise Blockchain Scalability Using Sharding and PBFT. International Journal of Intelligent Systems and Applications in Engineering, 12(2s), 362 –. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/3635

[58] Dang, H., Anh Dinh, T. T., Ee-Chien Chang, D. L., Lin, Q., & Chin Ooi, B. (2019). Towards Scaling Blockchain Systems via Sharding. National University of Singapore.Available from: https://www.comp.nus.edu.sg/~hungdang/papers/sharding.pdf

[59] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (poet). In Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19 (pp. 282-297). Springer International Publishing.

[60] Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. IEEE Access, 7, 118541–118555.

[61] T. Y. Song and Y. L. Zhao, (2018) "Comparison of blockchain consensus algorithm", Comput. Appl. Softw., vol. 25, no. 8, pp. 1-8.

[62] Yu, B., Liu, J., Nepal, S., Yu, J., & Rimba, P. (2019). Proof-of-QoS: QoS based blockchain consensus protocol. Computers & Security, 87, [101580].