ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20210205103310

Subject review

Performance-Based Analysis of Blockchain Scalability Metric

Jyoti Yadav*, Ranjana Shevkar

Abstract: Cryptocurrencies like Bitcoin and Ethereum, are widely known applications of blockchain technology, have drawn much attention and are largely recognized in recent years. Initially Bitcoin and Ethereum processed 7 and 15 Transactions Per Second (TPS) respectively, whereas VISA and Paypal process 1700 and 193 TPS respectively. The biggest challenge to blockchain adoption is scalability, defined as the capacity to change the block size to handle the growing amount of load. This paper attempts to present the existing scalability solutions which are broadly classified into three layers: Layer 0 solutions focus on optimization of propagation protocol for transactions and blocks, Layer 1 solutions are based on the consensus algorithms and data structure, and Layer 2 solutions aims to decrease the load of the primary chain by implementing solutions outside the chain. We present a classification and comparison of existing blockchain scalability solutions based on performance along with their pros and cons.

Keywords: consensus; decentralization; latency; scalability; security; throughput

1 INTRODUCTION

Blockchain is a decentralized, distributed, immutable ledger with a sequence of blocks interlinked and secured using cryptography. Block is a basic unit of blockchain that bundles a set of transactions initiated by participating nodes in the blockchain network. Block is a combination of the block header and block data. Block header generally holds information like current block hash, Merkle root hash: a cryptographic hash of all transactions of the block, timestamp: the time when the block is created, nonce(number used once): 32-bit random number that can be manipulated to get the current block hash within difficulty limit and previous block hash: reference to parent block. Block data portion contains the total number of transactions, transaction details (sender address, the value being transfer, receiver address, transaction fee, etc.). Block header is metadata that is used to verify and validate the block. The first block of the blockchain is called as a *"genesis"* block that does not have any previous block address. The main purpose of blockchain is to develop a network without a central repository and authority. The conceptual framework behind blockchain was first introduced by Haber and Stornetta [1] in 1991, for time-stamping of digital documents to avoid backdating it. An efficient optimization of the hash chain using Merkle tree was first described in the paper. This technology became widely known at the beginning of 2008 when Satoshi Nakamoto introduced Bitcoin: an electronic currency that involves the digital transfer of money [2]. Ethereum [3] was introduced by Vitalik Buterin in 2012 with the addition of Smart Contract as a primary feature. Smart contract was developed in 1997 by Nick Szabo [4] and used for the first time in the Ethereum cryptocurrency (ether) in 2015. Ethereum is not just a platform for the exchange of digital currency, but also a programming language used to build and publish Distributed Applications (DApps) without any downtime and fraud. Various digital cryptocurrencies such as Bitcoin, Ethereum, Ripple, Litecoin and Dagcoin are some examples of this technology. But apart from cryptocurrency, the technology is also instrumental in a variety of domains namely financial sectors such as money transfer, global trade financing, insurance, antimony laundering, KYC and other sectors such as health care, media, logistics, supply chain management, power and utilities, Government, property, E-voting etc. Apart from attractive features and interesting applications, the most challenging task of blockchain is its ***scalability***.

This paper attempts to classify and compare existing scalability solutions of blockchain. These solutions are broadly divided into three layers. Fig. 1 shows the mind map which depicts the taxonomy that classifies the blockchain scalability solutions at a glance. Layer 0 focuses on solutions for data propagation. Layer 2 presents on-chain solutions and Layer 3 focuses on off-chain solutions.

The remainder of the paper is organized as follows: Section 2 defines study methodology with the term Scalability and the related concepts. Section 3 presents scalability solutions in all the three layers. Section 4 compares all the solutions discussed in section 3, based on their performance. Section 5 concludes the paper and section 6 discusses about the future work.

2 STUDY METHODOLOGY

2.1 Scalability

Scalability is defined as the ability to process transactions regardless of volume and the number of participants in the blockchain network. The network is said to be scalable if it is capable to grow along with the demand of user-base [5]. It is also stated as the independence between the speed and number of participants in the network. Scalability is one of cryptocurrencies' primary and urgent concern, especially when it comes to the public blockchain.

The public blockchain should be able to handle millions of users on the network, to become mainstream. It is not a singular property of a system, but it relates several key metrics to teach other. The two most important performance metrics are throughput and latency.

2.2 Throughput

It is the number of transactions confirmed/processed per second (TPS). The most popular and widely used public

blockchains Bitcoin and Ethereum are especially slower than centralized payment processing networks such as VISA and Paypal. Both Bitcoin and Ethereum have extremely low throughput in terms of transaction processing rate as Bitcoin blockchain processes 7 TPS. Ethereum blockchain being faster can process 20 TPS approximately. As opposed to this, PayPal can process 193 TPS and VISA can process 1700 TPS.

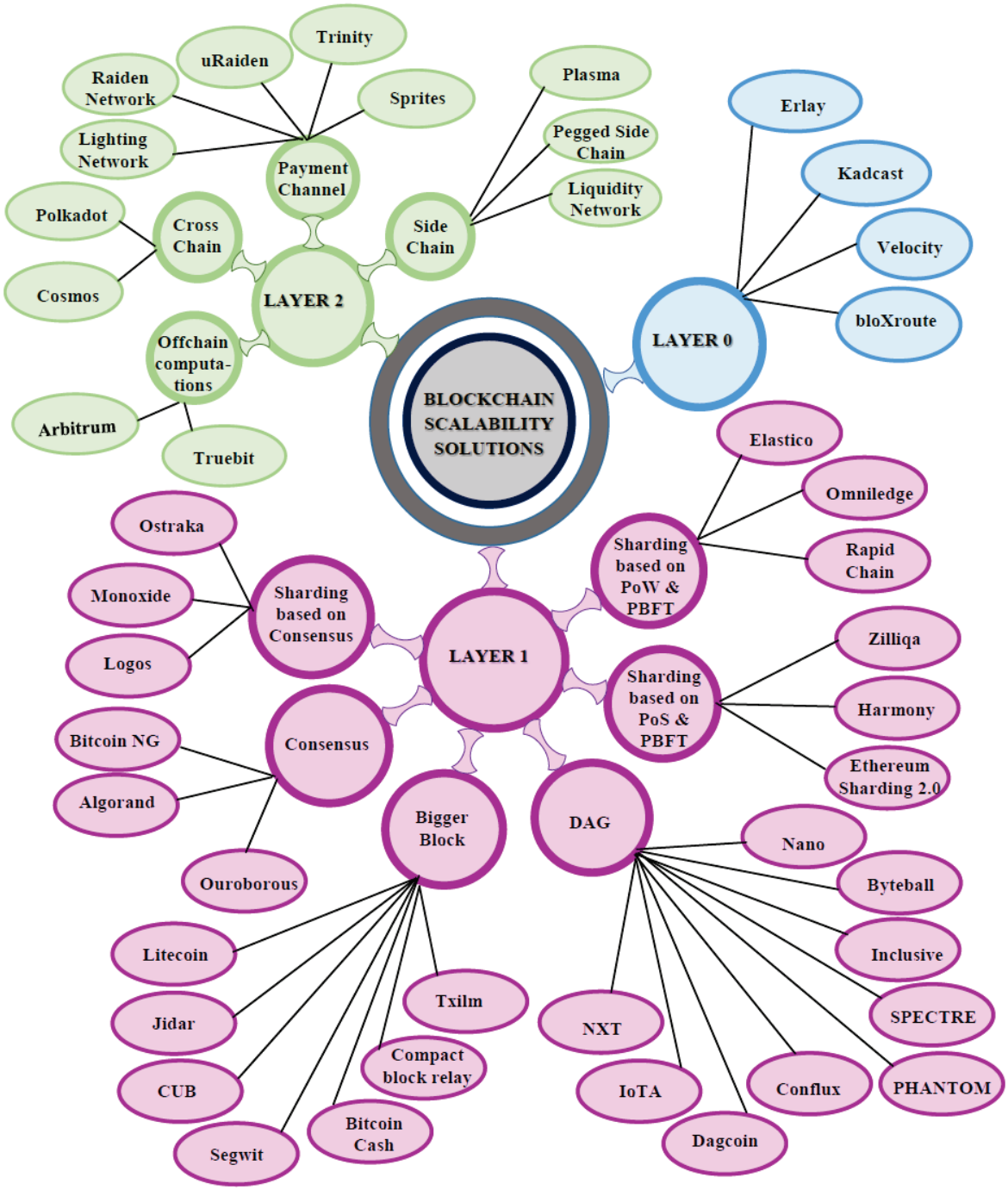

Figure 1 Taxonomy of Existing Blockchain Scalability Solutions

2.3 Latency or Block Time

It is defined as the time between submission and first confirmation of transaction in the blockchain. It is also termed as confirmation time or block time. An increase in number of nodes causes an increase in the number of transactions. Essentially, every single node verifies every transaction, and hence the verification time increases. The confirmation time for Bitcoin is 10 minutes, whereas for Ethereum it is 15 seconds. Thus to cope up with the centralized tech giants of financial sectors such as VISA, MasterCard, and PayPal, some upgradation is needed to scaleup the blockchain technology to increase the user-base like the internet.

2.4 Scalability Trilemma

The corner stones of the scalability trilemma are ***scalability, decentralization,*** and ***security.*** Effectively scaling up the blockchain without compromising on its other two important characteristics namely decentralization and security create alarming challenges to the researchers. Fig. 2 shows the scalability trilemma. The trilemma indicates that decentralization, security, and scalability, cannot co-exist. Blockchain can only possess two of these three properties at a time.

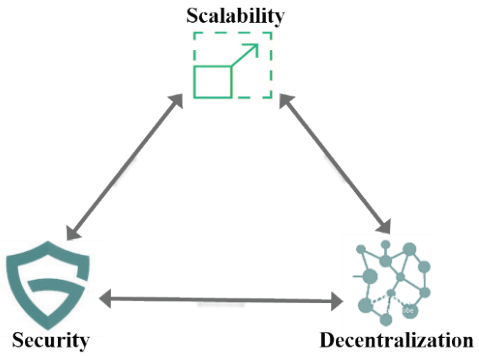

Figure 2 Scalability Trilemma

For instance, to improve scalability, decentralization is compromised by adding a centralized coordinator into the system that reduces the computational power consumed by the proof-of-work algorithm to reach a consensus on a set of transactions. Sacrificing decentralization by creating authority and trust using Hyperledger Fabric greatly improves the scalability and performance of the Blockchain [6]. In case of Bitcoin, reducing the block time improves the transaction throughput by increasing the probability of fork (the new protocols are implemented by splitting the original blockchain into two separate blockchains), which affects the security of the system. Hence, it is essential to balance these three characteristics, particularly for the future development of public blockchain systems. Building a secured system to meet the optimal transaction rate of Bitcoin users remain a formidable challenge.

3 SCALABILITY SOLUTIONS

The following section describes the scalability solutions currently being used in different applications at all three layers.

3.1 Layer 0 Solutions

Layer 0 solutions mainly focus on the propagation protocol for optimizing propagation of information, in the form of transactions and blocks in the blockchain network. The blocks and transactions are transmitted by nodes of the blockchain, but this transmission is not efficient due to high latency and bandwidth. When the block propagation is faster, the larger is the number of blocks added in a shorter block-interval, leading to an increase in transaction throughput. Following are the solutions available in the literature to enhance the propagation protocol:

1) **bloXroute** [7] is the first Blockchain Distribution Network (BDN) that allows faster propagation of blocks and transactions. It allows to increase the block size, reduce the block interval and risk of forks.

2) **Velocity** [8] is an improved block propagation protocol using erasure code (fountain code). This protocol tries to increase the transaction throughput by mining larger blocks.

3) **Kadcast** [9] is a fast, secure and efficient protocol for block propagation. The Kademlia architecture, a well-known structured overlay topology, used for efficient broadcast operation with adjustable redundancy and overhead.

4) **Erlay** [10] is a transaction dissemination protocol that saves 40% bandwidth consumed by a node. Improves the security of the network by allowing more connections to be established at a smaller cost as well as privacy by hardening the network against attack. Effectively, it increases the network connectivity at a very less cost in terms of bandwidth and latency.

Thus using distribution network, erasure code and overlay topology, the block propagation is enhanced along with increasing the throughput and reducing the latency.

3.2 Layer 1 Solutions

Layer 1 solutions concentrate on the consensus algorithms, network and data structure of the blockchain. The execution of these concepts is on-chain, hence these solutions are also referred to as on-chain solutions. There is no need to add anything on top of the existing architecture. The increasing block size of the original blockchain protocol resulted in its modification like bitcoin-cash, bitcoin gold using hard fork. Hard fork is a radical change to a blockchain network's protocol that makes previously invalid blocks/transactions valid (or vice-versa) and all nodes or users need to upgrade to the latest version of the protocol. Data structure like directed acyclic graph has also been studied as a layer 1 scalability solution.

Following are the Layer 1 scalability solutions based on the parameters like block size, sharding using PoS (Proof of Stake) and PoW (Proof of Work) with PBFT (Practical Byzantine Fault Tolerance) and consensus algorithms:

3.2.1 Block Size

The list of transactions are stored in a block and are created periodically. The block size limits the number of transactions stored in a block. Large block size means more number of transactions processed per second. Block interval is the time to generate the next block in the chain. The throughput of the blockchain is directly proportional to the block size and inversely proportional to the block time. As such, the increase in block size leads to slow propagation of blocks in the network and decrease in block time leads to forking of new chains. It is the amount of time between generation of the transaction and adding it to the blockchain. Apart from increasing block size, other solutions are

proposed to compress a number of transactions added to the block [47]. Compact Block Relay and Txilm are some such solutions proposed in BIP152 (Bitcoin Improvement Proposal). The usage of blockchain on mobile phones and low-end PC's is prevented due to the requirement of high storage space. CUB and Jidar are the solutions for it.

Following are the protocols used in the scalability solutions based on block size:

1) **Litecoin** is a peer-to-peer decentralized and open source protocol. Litecoin can handle large volume of transactions than bitcoin. As compared to bitcoins' block interval of 10 minutes, Litecoins' block interval is 2.5 minutes, which is four times faster. Consequently faster block generation supports more number of transactions. The throughput of Litecoin is 56 TPS. It is more resistant to a double spending attack [43]. But it leads to drawbacks such as increased blockchain size and more orphaned blocks (the stale block which is valid and verified, but rejected by the blockchain network due to a time lag in the acceptance of the block). Litecoin uses a new cryptographic algorithm named Scrypt, over a longstanding SHA256 algorithm used by Bitcoin. [44]

2) **SegWit** (Segregated Witness) [11] is the process of separating/segregating the digital signature (witness) of the transaction and is used to increase the block size limit. When certain parts of a transaction are removed, this frees up space/capacity to add more transactions to the chain. The digital signature accounts for 65% of the space in a given transaction. It is defined in BIP141 [45] and designed to solve Bitcoin's malleability and scalability issues. In SegWit block size has been increased from 1 MB to 4 MB and the block is divided into two parts: base transaction block of size 1MB and extended block of size 3MB. Base transaction block contains information about sender and receiver. The digital signature and other data of transactions known as a witness are stored in an extended block. The maximum block size in SegWit is measured in weight, computed as follows:

$$B_{\mathrm{w}} = 3B_{\mathrm{s}} + T_{\mathrm{s}} \tag{1}$$

Where B_{w} is the block weight, B_{s} is the base size: the number of bytes needed to serialize the transaction without witness (3 MB) and T_{s} is the total size: the block size in bytes with transactions serialized including base data and witness data (1 MB).

3) **Bitcoin Cash** (BCC) is a cryptocurrency created from a fork of Bitcoin, in August 2017 [46]. BCC initially increased the block size from 1 MB to 8 MB and later to 32 MB, maintaining the same block interval of 10 minutes. But the large block size leads to centralization, as individual users will not be able to propagate blocks efficiently. Also, it is difficult to verify all transactions within a given time interval.

4) **Compact Block Relay** is a method of reducing the amount of bandwidth used to propagate new blocks to full nodes. Full nodes share almost same mempool contents. Sender sends compact block called sketches to the receiving peer. This compact block includes 80-bytes header of the new block, shortened transaction IDs that are designed to prevent Denial-of-Service (DoS) attacks and some full transactions which the sender predicts the receiver doesn't have yet. Using this information and the transactions already present in mempool, the receiver tries to reconstruct the entire block. The missing transactions are requested from the sender. Once all the transactions are available, the block is generated.

5) **Txilm** on the other hand compresses transactions of each block and saves the bandwidth of the network. Txilm uses a short hash value of TXID to represent a transaction. To avoid hash collisions due to short hash value, the transactions are sorted based on TXID. Thus 80 times data reduction causes an increase in the throughput of the blockchain.

6) **CUB** (Consensus Unit-based Solutions) [12] proposed a new concept called Consensus Unit (CU) that divides different nodes into units. The units of nodes are formed and total blocks of the blockchain are assigned to nodes, to maximize the storage space utilization and reduce the query cost.

7) **Jidar** (Jigsaw-like Data Reduction) [13] in which, each node stores only transactions needed and branches of the Merkle tree from the whole block. This is like selecting pieces from the jigsaw puzzle hence named Jidar. To get complete block data, the fragments are collected from other users and combined into a whole block. But this functionality needs incentive.

The above protocols increases the actual block size, implements enhanced cryptographic algorithm or compresses the transactions to improve the scalability.

Sharding is a widely used solution for scaling distributed databases such as MySQL and MongoDB. It splits the entire blockchain network into multiple smaller groups of nodes called shards or committees. In a blockchain, the shared ledger can be divided into various tasks such as account balances, smart contract code, transaction broadcasting, processing and storage etc. The shards process disjoint transactions in parallel and maintain a disjoint ledger. This results in improved throughput, reduced latency and storage requirements [14]. The sharding solutions are broadly categorized based on consensus as follows:

3.2.2 Sharding Based on PoW and PBFT

PoW consensus is used for committee formation, PBFT consensus for intra-committee communication.

1) **Elastico** [15] provides the first sharding protocol for permissionless blockchains tolerating one-fourth fraction of byzantine faults. It divides the network into multiple committees called shards. Each shard contains a distinct set of transactions. The shard number grows linearly with network size. Throughput is 40 TPS but is only 25% network resilient and 33% committee resilient.

2) **Omniledger** [16] is a distributed ledger based on sharding protocol. It is only 25% resilient to Byzantine faults. To overcome the security issue of Elastico, a bias resistant randomness protocol is used in Omniledger. Apart from PFT for intra shard communication, Byzantine shard atomic

committee is used for cross shard communication. The total and committee resiliency of Omniledger is the same as Elastico.

3) **Rapid Chain** [17] is the first one-third resilient sharding-based blockchain protocol that is highly scalable to large networks. Kademlia routing algorithm is used for inter committee routing. The throughput is greatly increased to 4220 TPS as compared to Elastico. Total resiliency is increased to 33% and committee resiliency to 50%.

4) **Ostraka** [40] architecture scales linearly with the available resources. Ostraka shards are the nodes themselves that runs parallely without affecting the security of the underlying consensus mechanism. The throughput of Ostraka is very high upto 400000 TPS.

Different inter and intra shard communication techniques along with routing algorithms are used to increase the throughput.

3.2.3 Sharding Based on PoS and PBFT

PoS consensus is used for committee formation and PBFT consensus for intra-committee communication.

1) **Zilliqa** [18] allows to process the transaction in parallel and achieve high throughput about thousand times of Ethereum. Zilliqa is susceptible to single shard takeover attacks as it does not support state sharding. Zilliqa's local and global resiliency is the same as Elastico and Omniledger. The throughput of Zilliqa is 2828 TPS.

2) **Harmony** [48] claims to be highly scalable. Along with network communication and transaction sharding, harmony supports state sharding. The distributed randomness process ensures high security. The local and global resiliency of Harmony is the same as Zilliqa, Elastico and Omniledger. In Harmony, one shard contributes to 500 TPS.

3) **Ethereum Sharding 2.0** [49] is the popular sharding based protocol with three phases: Beacon Chain, Shard Chain and State Execution. Beacon chain manages all shards in the network. The consensus rules, rewards and penalties are applied to the validators. Shard chain enables parallel transactions. The operations of the entire system are executed in the State execution phase.

It is observed that there is a sudden growth in the throughput of above solutions due to parallel execution of transactions and state sharding.

3.2.4 Sharding Based on Consensus

Apart from using PoW, PoS or PBFT, other consensus algorithms are used to enhance the performance.

1) **Monoxide** offers linear scaling using asynchronous consensus zones. The blockchain system runs multiple independent and parallel instances called as consensus zones. Each zone is responsible for its own data. It partitions the workload of all key components, without compromising on the decentralization and security of the system [19]. The core and zone-specific data structures, like blocks and transactions are replicated and stored only within their own zones. Mining competition, chain growth, and transaction confirmation are carried out separately and asynchronously in each zone.

2) **Logos** [50] uses Axios, a delegated PBFT consensus algorithm to increase the throughput and minimize latency. Each user on the Logos network has a separate chain to keep track of its transactions and can process in parallel. Sharding adds parallel processing of transactions. The elected delegates validate the transactions.

The asynchronous and delegated PBFT consensus are used to scale-up the performance of the blockchain.

3.2.5 Consensus

Different consensus strategies are used to improve the scalability. Mainly these solutions elects the leader block for the processing of transactions.

1) **Bitcoin NG** (Next Generation) [20] is a protocol that uses Nakamoto consensus, which divides time into epochs. One leader is responsible for transaction serialization in each epoch. Bitcoin-NG introduces key block and micro block. The key block is used only for electing the leader. The PoW mechanism is used by the miners to create the key block. The micro block contains packaged transaction data and is generated by leader. Transactions are processed continuously until new leader is selected. This enhances scalability and reduces transaction confirmation time.

2) **Algorand** [21] is a cryptocurrency built upon a Byzantine Agreement (BA) protocol. Users are selected as committee members using Verifiable Random Function. To reach the next set of transactions, the committee members participate in BA. The participants are replaced by sending a message in BA to avoid targeted attacks. Algorand is highly scalable up to 500,000 users, hence achieves high throughput.

3) **Ouroborous** [22] uses a coin flipping protocol to elect the leader. To determine whether a participant can be elected as a leader, a random number is generated by participants using Verifiable Random Function [19]. In the above listed solutions, Nakamoto consensus, BA protocol and verifiable random functions are used to scale-up the blockchain in terms of the throughput and the users.

3.2.6 DAG (Directed Acyclic Graph)

DAG is a network of nodes that uses topological ordering, where the nodes are connected in order – from earlier to later. The new transaction performed necessitates the validation of two earlier transactions before getting added to the blockchain network. More transactions are validated when new transactions enter the network. This distributed network of double-checked transactions does not need miners and fee for transaction authentication [23]. The scalability is improved by coupling network usage and transaction verification, meaning that a user must handle his/her own transactions in order to use the network [39]. Some DAG based blockchain technologies are as follows:

1) **NXT** [57] is the first crypto-currency to adopt DAG based on blocks instead of using linear linked list structure of blockchain. It is a 100% PoS cryptocurrency, developed in open-source Java. The unique PoS algorithm used in NXT, is independent of implementation of the coin age concept used

by other PoS cryptocurrencies. NXT is also resilient to nothing at stake attacks. The block generation time is 60 seconds and confirmation time is 10 minutes.

2) **Nano** [24] is a trustless, low-latency cryptocurrency that uses novel block-lattice architecture. Each participant has its own blockchain and achieves consensus using delegated PoS voting. Nano offers unlimited scalability, fee-free and instantaneous transaction and runs on low power hardware.

3) **Byteball** [25] is a cryptocurrency platform for smart payments. The transaction itself acts as a unit called ball that connect to each other using DAG. Bytes is the currency for the reward. A DAG is formed by referring one or more parent units. Consensus is achieved by building a main chain which contains most units published by witnesses. Witnesses are trusted and verified addresses which regularly publish sequential units.

4) **Inclusive** [26] protocol proposes to restructure the block chain into a DAG structure that allows transactions from all blocks to be included in the log. The "inclusive" rule is used to select the main chain from within the DAG and to incorporate contents of off-chain blocks into the log. It is verified that there is no conflict with previously included content. An important aspect of the Inclusive protocol is that it rewards fees of accepted transactions to the creator of the block that contains them—even if the block is not part of the main chain. Such payments are granted only if the transaction has not been previously included in the chain, and are decreased for blocks that were published too slowly.

5) **SPECTRE** [27] is specially designed for payments. It is a fast and scalable DAG-based public blockchain. The PoW consensus makes it more secure and resilient to attackers, with only 50% computational power.

6) **PHANTOM** [28] is a protocol for secured transaction confirmation for any throughput that the network supports. It uses a blockDAG that supports faster block generation and higher transaction throughput. PHANTOM uses a greedy algorithm to distinguish between blocks mined properly by honest nodes (a node that behaves as expected) and those that are created by non-cooperating (a node that misbehaves and tries to distribute invalid information) nodes.

7) **Conflux** [29] is a fast, scalable and decentralized system that can process about thousands of TPS and confirms each transaction in minutes. It uses a blockDAG and achieves consensus on the total order of the blocks. The consensus protocol used in Conflux, allows multiple participants to contribute concurrently to the blockchain, preserving the safety. Hence results in faster block generation and higher throughput. The throughput is equivalent to 6400 TPS with latency of about 4.5 to 7.4 minutes, tested on Amazon EC2 clusters.

8) **Dagcoin** [30] was initially built on the top of Byteball. The transactions are stored and ordered using DAG rather than blockchain. Each transaction is treated as a block and accentuates faster and secured confirmations as well as greater throughput. It claims to be faster and securer with the growth of usage.

9) **IoTA** (Internet of Things Application) [51] is the first open-source distributed ledger protocol for the emerging economy of the Internet of Things with feeless micro transactions and data integrity. The key feature of IoTA is Tangle which is the transaction storing and processing mechanism. IoTA is highly scalable, as Tangle can process transactions simultaneously. As more systems are attached to it, the Tangle becomes more secure and efficient at processing transactions.

The DAG solutions generally used for Payments with micro transactions and improves throughput with faster block generation.

3.3 Layer 2 Scalability Solutions

Layer 2 Solutions aims to decrease the load of the main-chain, accomplished by executing some transactions off-chain and shifting computationally intensive tasks on an off-chain platform. The layer 2 solutions are constructed on the top of main blockchain infrastructure. The base level protocols are not altered, instead a smart contract interacts with the blockchain software.

3.3.1 Off-chain Computations

The state of the smart contracts is verified by the validators by imitating the execution of all contracts. But the process of verification is costly, hence decline the scalability of Ethereum. These costly and complex calculations are performed off-chain to enhance the scalability.

1) **Truebit** is an Ethereum smart contract introduced in 2017 by founder and mathematician Jason Teutsch along with the creator of Solidity language Christian Reitwiessner, to facilitate trusted, computationally intensive applications [31]. Computations performed on the main Ethereum blockchain are costly as the transactions are processed by all full nodes on the network simultaneously. The compensation of the computation is given in the form of gas cost. Each block has a maximum gas limit that sets the cap on the total amount of computation performed by all transactions in a block. Hence complex computations are not included in the block. Truebit outsources the complex computations to a verified third party. The third party is trusted as it deposits token into the smart contract and is called as solver. Another third party called challenger, verifies the work done by solver and receives monetary incentives. The challenger identifies exact operation that causes disagreement. Thus the computationally intensive work of Ethereum main blockchain is narrowed down, at the same time true and correct results are recognized.

2) **Arbitrum** [32] protocol performs the verification of smart contract off-chain and improves the scalability. The role of the Verifier is to validate transactions. The fund owned by contract is not consumed for execution of contract. Such contracts are implemented on Virtual Machine (VM). Arbitrum uses mechanism designed to incentivize parties to agree off-chain on what a VM would do, so that the Arbitrum miners verify digital signatures to confirm that parties have agreed on a VM's behavior. A set of VM managers are created by every party, to force to work as per the code. The anonymous assertion is signed by all the managers, only after

agreed upon the new state of VM, otherwise, a disputable assertion is signed to challenge the VM's state change and be engaged in the bisection protocol. The bisection protocol resolves the dispute, identifies and penalizes the dishonest party. Thus, only hashes of contract states are verified and the load of the verifier is minimized allowing contracts to execute privately.

Thus smart contracts and virtual machines are used to reduce the load on the main chain in Truebit and Arbitrum.

3.3.2 Cross Chain

It is an interoperability between independent, heterogeneous blockchains to create a big network of blockchains. Thus the inter communication of independent blockchains can improve the scalability.

1) **Cosmos** [52] is a network of many independent blockchains called zones. The zones are powered by Tendermint BFT. The Tendermint BFT consensus algorithm provides high-performance, consistent, secured and strict fork accountability that controls the behavior of malicious actors. The first zone called as hub uses a governance mechanism enabling the network to adapt and upgrade. The hub and zones can communicate with each other via Inter Blockchain Communication (IBC) protocol to exchange tokens and data.

2) **Polkadot** [33] is a multi-chain protocol that connects heterogeneous blockchains with a relay-chain. Relay-chain enables an independent blockchain called parachain to exchange information and trustless inter-chain translation. Polkadot is a bridge that connects already running blockchains like Ethereum.

Hence secured and trustless intercommunication among the heterogeneous blockchains is achieved using Tendermint and Relay-chain.

3.3.3 Payment Channel

The payment channel is a temporary channel created, on which some transactions are transferred to reduce the load on main chain and to improve the throughput of the entire system.

1) **Lightning Network** [34] is Bitcoin's decentralized scalable solution for faster and high-volume micropayments. It uses a smart contract for instant payments across the network. The key features of Lightning network includes instant payments in milliseconds, high throughput and low cost. But Lightning network has certain drawbacks: (a) scales only transactions but not users, (b) the transactions are less secure than Bitcoin, (c) it works only for Bitcoin's micropayments.

2) **Raiden Network** [53] is an off-chain scaling solution. It is the same as Bitcoin's Lightning Network that facilitates fast, low-fee, scalable, and privacy-preserving payments. The tokens are securely transferred between participants without prerequisite global consensus using balance proofs. The balance proof is digitally signed and hash-locked transfer. The Raiden Network leverages on "off-chain" payment channels to transfer the value. It is not necessary to record each transaction on Ethereum blockchain for completion. Instead of verifying individual transactions, Raiden Network verifies net claims resulted from off-chain transactions. It is interoperable and works with any token that follows Ethereum's standardized token API (Application Programming Interface) (ERC (Ethereum Request for Comment) 20).

3) **µRaiden** [54] is a fast and free off-chain ERC20 token transfer framework, more specialized to a smaller range of applications. Along with all the features of Raiden network, µRaiden allows free off-chain token transfer, fee is incurred for opening and closing of the channel. As it does not support multihop fee transfer, the payments are unidirectional to the predefined receivers.

4) **Trinity** [55] is a universal off-chain scaling solution, with features like real-time payments, low transaction fees, scalability, and privacy protection for main chain assets. The transaction throughput is suddenly increased with the use of a state channel. To enhance privacy Trinity adopts multiple technologies like zero-knowledge proof to protect data security. Trinity works only for payment channels.

5) **Sprites** [35] is a novel payment channel that reduces the collateral cost, which each hob incur along the route. The constant lock times are developed to improve transaction throughput in payment channel networks. The partial deposits and withdrawals are supported without interrupting the payment channel.

The different techniques like state channel, multi hop and constant lock time are used in payment channel solutions.

3.3.4 Side Chain

It is a separate blockchain attached to its parent blockchain using a two-way peg. The two-way peg allows interchanging of assets between the parent blockchain and the sidechain at a predetermined rate. The reverse happens when moving back from a sidechain to the main chain.

1) **Plasma** [36] was proposed by Ethereum co-founder Vitalik Buterin and Joseph Poon in August 2017 as a second-most deployed scalability solution for Ethereum blockchain that aims to increase transaction throughput. Plasma refers to a framework that allows creating unlimited numbers of child chains which are smaller copies of parent blockchain. A tree-like structure is generated by creating more chains on the top of each child chain. The child chain is a customized smart contract designed as per the demand of specific use case. The overall work of main chain will be elevated by each child chain, hence there will be no congestion in the main chain. Plasma is a better solution for decentralized applications for which high transaction fee is obtained from users.

2) **Pegged Side Chain** [37] is a technology that enables transfer of bitcoins and other ledger assets between multiple blockchains. It also prevents the assets from malicious attackers and ensures the atomicity of the transfers. Pegged Side Chains proposed a protocol named Two-way peg, transferring the assets from parent chain to side chain. The coins are sent from parent chain to a special output and are locked until a Simplified Payment Verification (SPV) proof is received on the pegged side chain. After sending the coin,

confirmation period protects the transfer from denial of service attack and deals latency for security. After unlocking, the newly transferred assets cannot be spent on the sidechain to avoid double spending. Same process is used to send coins from the sidechain to the parent chain.

3) **Liquidity Network** [56] proposed Nocust (Non-Custodial) [38], a secured and scalable commit-chain. A new data structure Merkleized Interval Tree: a multi-layered tree is used in Nocust. Every users' balance is stored in exclusive non-crossing interval space. The total balances are verified with the amount recorded in the smart contract, available on the parent chain. There is no limit on funds while transferring, receiving and interacting with parent chain. The real-time transactions are guaranteed by Nocust. The transaction delays are reduced without extra fees and mortgages. With a very low transaction fee, high throughput is achieved while scaling to one billion users.

Two-way peg, child chains and Merkleized Interval tree are implemented in side chain solutions that results in very low transaction fee while increasing the throughput.

Table 1 Comparison of Various Scalability Solutions

Sr. No.	Solutions	Strategy used	Through-put (TPS)	Latency (Seconds)	Block Size (MB)
1	SegWit	Segregate digital sign	7	--	4
2	Byteball	DAG	20-30	60	NA
3	Elastico	Sharding	40	800	1
4	Litecoin	Scrypt	56	150	4
5	Bitcoin-Cash	Increased Block size	61	--	32
6	Bitcoin-NG	Nakamoto consensus	100	NA	NA
7	Ouroboros	Coin-flipping protocol	257.6	120	NA
8	IoTA	DAG and Tangle	500	60	NA
9	Algorand	Byzantine Agreement	875	22	NA
10	LOGOS (Social n/w on blockchain)	Axios	2500	<3	1
11	Zilliqa	Sharding, parallel processing of transactions	2828	--	--
12	Omniledger	Sharding	3500	800	1
13	Conflux	block DAG	6400	270 - 444	NA
14	Nano	block-lattice architecture	7000	1 to 10	NA
15	Rapid Chain	Sharding	7380	8.7	1
16	Monoxide	Asynchron-ous consensus	11694	13-21	1
17	Ostraka	Node sharding	400000	--	1

NA - Not Applicable, "-" - indicates Not available

4 COMPARISON OF SCALABILITY SOLUTIONS

4.1 Comparison of Various Scalability Solutions

As per the literature survey, following scalability solutions are arranged in ascending order based on their performance in terms of throughput. Hafid [41] has categorized scalability solutions only at layer 1 and layer 2. Reference [42] though listed all three layer solutions but has not compared on the basis of pros and cons. From Tab. 1, Ostraka, layer 1 solution of sharding based on consensus, has the highest throughput of 400000 TPS which is invented recently. Among the solutions like Dash, Litecoin, Bitcoin cash and Bitcoin SV, it is observed that increase in throughput is proportional to block size. Block size is not applicable for the DAG scalability solutions, as the transactions are connected to each other. Among all DAG solutions such as Bitcoin NG IoTA, Nano, Ouroborous, Algorand and Conflux, the throughput of Nano is maximum i.e. 7000 TPS. Along with good throughput, solutions like Nano, Logos and Rapid chain have lowest latency.

4.2 Benefits and Limitations of Scalability Solutions

Not only the performance but the other features of existing solutions are compared in terms of their advantages and disadvantages in Tab. 2.

Table 2 Benefits and Limitations of Scalability Solutions

Solutions	Benefits	Limitations
SegWit	• Block size/ capacity increased. • Fixes transaction malleability issue. • Linearly scales the signature-hashing • Reduces UTXO growth	• Causes hard fork on Bitcoin • Needs to be more scalability
Bitcoin Cash	• Increase the throughput	• Lead to Centralization • Difficult to verify large number of transactions within short interval
Txilm	• Saves bandwidth	
Elastico	• Increase in throughput - 40 TPS	• Division of epoch can be influenced by malicious nodes • Total resiliency 25% and committee resiliency 33%
OmniLedger	• Bias resistant randomness protocol used for security • Throughput 500 TPS	• Total resiliency 25% and committee resiliency 33%
Rapid chain	• High throughput 4220 TPS • Total resiliency 33% and Committee resiliency 50%	• Partitioning attack • Responsiveness
Zilliqa	• Throughput 1000 times that of Ethereum	• Susceptible to single shard takeover attack 2) total resiliency 25% and committee resiliency 33%
Harmony	• Highly scalable • Sharding of blockchain state • High security	• Total resiliency 25% and committee resiliency 33%
Spectre	• Specially designed for payments	• Not suitable for smart contracts
Lightning Network	• Low cost • Faster payment • High throughput	• Does not scale users • Less secured • Works only for Bitcoin's micro payment
μRaiden	• Token transfer is free, only fee incurred is for opening and closing of channels.	• Does not support multi hop fee transfer, hence the transfer is unidirectional

Table 2 Benefits and Limitations of Scalability Solutions (continuation)

Solutions	Benefits	Limitations
Trinity	• Real-time payments • Low transaction fees • Scalable • Privacy protection	• Works only for payment channels
Plasma	• Lower transaction cost and faster operations • Secured • Does not need all participants to be online	• Long waiting period to withdraw funds • Complex implementation
Pegged Sidechains	• Communicates among Heterogeneous blockchains	• Transaction fund is saved as a deposit in the trading channel. • The transaction channel depends on complex routing topologies

5 CONCLUSION

Different scalability solutions proposed in the literature are classified and compared based on their performance measures (throughput, latency and strategies used). The solutions are classified into three layers. Layer 0 proposes solutions that uses erasure code and overlay topology, to enhance data propagation and reduce bandwidth usage. Layer 1 describes on-line solutions based on block size, compression of transactions, state and node sharding based on various consensus algorithms, directed acyclic graph etc. Layer 2 focuses on off-line solutions like payment channels, side chain, cross chain and off-chain computations using smart contracts, virtual machines, Tendermint, relay-chain, state channel, two-way peg, child chains and Merkleized interval tree.

This comprehensive study and classification of solutions at different layers can inspire researchers for further enhancement in the scalability of blockchain.

6 FUTURE WORK

The limitations listed in Tab. 2 indicates the areas as recommendations for further work. To enhance the total and committee resilience in sharding solutions. Along with scaling transaction throughput, users also should be scaled-up. There is a scope to improve scalability which is limited to only the payment channels.

Notice

This paper was presented at IC2ST-2021 – International Conference on Convergence of Smart Technologies. This conference was organized in Pune, India by Aspire Research Foundation, January 9-10, 2021. The paper will not be published anywhere else.

7 REFERENCES

[1] Haber, S. & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-38424-3_32

[2] Nakamoto, S. & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.* https://bitcoin.org/bitcoin.pdf, 4.

[3] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

[4] Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*. https://doi.org/10.5210/fm.v2i9.548

[5] Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34. https://doi.org/10.1145/3316481

[6] Scherer, M. (2017). Performance and scalability of blockchain networks and smart contracts.

[7] Klarman, U., Basu, S., Kuzmanovic, A., & Sirer, E. G. (2018). bloxroute: A scalable trustless blockchain distribution network whitepaper. *IEEE Internet Things J.*

[8] Chawla, N., Behrens, H. W., Tapp, D., Boscovic, D., & Candan, K. S. (2019, May). Velocity: Scalability improvements in block propagation through rateless erasure coding. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 447-454). IEEE. https://doi.org/10.1109/BLOC.2019.8751427

[9] Rohrer, E. & Tschorsch, F. (2019, October). Kadcast: A structured approach to broadcast in blockchain networks. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (pp. 199-213). https://doi.org/10.1145/3318041.3355469

[10] Naumenko, G., Maxwell, G., Wuille, P., Fedorova, A., & Beschastnikh, I. (2019, November). Erlay: Efficient Transaction Relay for Bitcoin. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 817-831). https://doi.org/10.1145/3319535.3354237

[11] Lombrozo, E., Lau, J., & Wuille, P. (2015). Segregated witness (consensus layer). *Bitcoin Core Develop. Team, Tech. Rep. BIP*, *141*.

[12] Xu, Z., Han, S., & Chen, L. (2018, April). Cub, a consensus unit-based storage scheme for blockchain system. In *2018 IEEE 34th International Conference on Data Engineering (ICDE)* (pp. 173-184). IEEE. https://doi.org/10.1109/ICDE.2018.00025

[13] Dai, X., Xiao, J., Yang, W., Wang, C., & Jin, H. (2019, July). Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1317-1326). IEEE. https://doi.org/10.1109/ICDCS.2019.00132

[14] Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019, June). Towards scaling blockchain systems via sharding. In *Proceedings of the 2019 International Conference on Management of Data* (pp. 123-140). https://doi.org/10.1145/3299869.3319889

[15] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17-30). https://doi.org/10.1145/2976749.2978389

[16] Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018, May). Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 583-598). IEEE. https://doi.org/10.1109/SP.2018.000-5

[17] Zamani, M., Movahedi, M., & Raykova, M. (2018, January). Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 931-948).

https://doi.org/10.1145/3243734.3243853
[18] Team, Z. (2017). The ZILLIQA technical whitepaper. https://doi.org/10.2139/ssrn.3442330
[19] Wang, J. & Wang, H. (2019). Monoxide: Scale out blockchains with asynchronous consensus zones. In *16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19)* (pp. 95-112). https://doi.org/10.1016/j.automatica.2019.108620
[20] Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)* (pp. 45-59).
[21] Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017, October). Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles* (pp. 51-68). https://doi.org/10.1145/3132747.3132757
[22] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference* (pp. 357-388). Springer, Cham. https://doi.org/10.1007/978-3-319-63688-7_12
[23] Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018, December). A comparative analysis of DAG-based blockchain architectures. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 27-34). IEEE. https://doi.org/10.1109/ICOSST.2018.8632193
[24] LeMahieu, C. (2018). Nano: A feeless distributed cryptocurrency network. https://nano.org/en/whitepaper (date of access: 24.03. 2018).
[25] Churyumov, A. (2016). Byteball: A decentralized system for storage and transfer of value. https://byteball.org/ Byteball.pdf
[26] Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015, January). Inclusive block chain protocols. In *International Conference on Financial Cryptography and Data Security* (pp. 528-547). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-47854-7_33
[27] Sompolinsky, Y., Lewenberg, Y., & Zohar, A. (2016). SPECTRE: A Fast and Scalable Cryptocurrency Protocol. *IACR Cryptol. ePrint Arch.*, *2016*, 1159.
[28] Sompolinsky, Y., & Zohar, A. (2018). PHANTOM: A Scalable BlockDAG Protocol. *IACR Cryptol. ePrint Arch.*, *2018*, 104.
[29] Li, C., Li, P., Zhou, D., Xu, W., Long, F., & Yao, A. (2018). Scaling nakamoto consensus to thousands of transactions per second. *arXiv preprint arXiv:1805.03870*.
[30] Lerner, S. D. (2015). DagCoin: a cryptocurrency without blocks. *White paper*.
[31] Teutsch, J. & Reitwießner, C. (2019). A scalable verification solution for blockchains. *arXiv preprint arXiv:1908.04756*.
[32] Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S. M., & Felten, E. W. (2018). Arbitrum: Scalable, private smart contracts. In *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 1353-1370).
[33] Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper*.
[34] Poon, J. & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.
[35] Miller, A., Bentov, I., Bakshi, S., Kumaresan, R., & McCorry, P. (2019, February). Sprites and state channels: Payment networks that go faster than lightning. In *International Conference on Financial Cryptography and Data Security* (pp. 508-526). Springer, Cham. https://doi.org/10.1007/978-3-030-32101-7_30
[36] Poon, J., & Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. *White paper*, 1-47.
[37] Back, A., Corallo, M., Dashjr, L., et al. (2014). Enabling blockchain innovations with pegged sidechains. http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 72.
[38] Khalil, R., Gervais, A., & Felley, G. (2018). NOCUST-A Non-Custodial 2nd-Layer Financial Intermediary. *IACR Cryptol. ePrint Arch.*, *2018*, 642.
[39] Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018, December). A comparative analysis of DAG-based blockchain architectures. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 27-34). IEEE. https://doi.org/10.1109/ICOSST.2018.8632193
[40] Manuskin, A., Mirkin, M., & Eyal, I. (2020, September). Ostraka: Secure blockchain scaling by node sharding. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)* (pp. 397-406). IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00060
[41] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling blockchains: A comprehensive survey. *IEEE Access*, *8*, 125244-125262. https://doi.org/10.1109/ACCESS.2020.3007251
[42] Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access*, *8*, 16440-16455. https://doi.org/10.1109/ACCESS.2020.2967218
[43] "Litecoin" https://litecoin.org/
[44] https://www.scmspune.ac.in/journal/pdf/current/Paper%2010%20-%20Jaysing%20Bhosale.pdf
[45] "BIP 141" https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki#Block_size
[46] "Bitcoin cash" https://news.bitcoin.com/fork-watch-first-bitcoin-cash-block-mined
[47] https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki#Abstract
[48] "Harmony" https://harmony.one
[49] "Ethereum Sharding 2.0" Buterin. Ethereum Sharding FAQ. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ
[50] "Logos" https://logos. network/whitepaper.pdf
[51] "IoTA" https://www. iota.org/get-started/what-is-iot
[52] "Cosmos" https://cosmos.network/resources/whitepaper
[53] "Raiden Network" https://raiden.network/
[54] "μRaiden" https://raiden.network/micro.html
[55] Trinity, Universal off-chain scaling solution, Trinity White Paper. Available: https://trinity.tech/#/whitepaper
[56] "Liquidity Network" https://liquidity.network
[57] "NXT" https://nxtwiki.org/wiki/Whitepaper:Nxt

Authors' contacts:

Jyoti Yadav
(Corresponding author)
Department of Computer Science,
University of Savitribai Phule Pune University,
Ganeshkhind, Pune, Maharashtra 411007, India
yadav.jyo@gmail.com

Ranjana Shevkar
PES's Modern College of Arts, Science and Commerce,
Ganeshkhind, Pune, Maharashtra 411016, India
rsshevkar@gmail.com