A Comparative Analysis of Scalability Issues within Blockchain-based Solutions in the Internet of Things

Ahmed Alrehaili[1], Abdallah Namoun[2]
Faculty of Computer and Information Systems
Islamic University of Madinah
Madinah 42351, Saudi Arabia

Ali Tufail[3]
School of Digital Science, Faculty of Science
Universiti Brunei Darussalam
Brunei Darussalam

***Abstract*—Recently, enormous interest has been shown by both academia and industry around concepts and techniques related to connecting heterogeneous IoT devices. It is now considered a rapidly evolving technology with billions of IoT devices expected to be deployed in the upcoming years around the globe. These devices must be maintained, managed, traced, and secured in a timely and flexible manner. Previously, the centralized approaches constituted mainstream solutions to handle the ever-increasing number of connected IoT devices. However, these approaches may be inadequate to handle devices at a massive scale. Blockchain as a distributed approach that presents a promising solution to tackle the concerns of IoT devices connectivity. However, current Blockchain platforms face several scalability issues to accommodate diverse IoT devices without losing efficiency. This paper performs a comprehensive analysis of the recent blockchain-based scalability solutions applied to the Internet of Things domain. We propose an evaluation framework of scalability in IoT environments, encompassing critical criteria like throughput, latency, and block size. Moreover, we conduct an assessment of the notable scalability solutions and conclude the results by highlighting six overarching scalability issues of blockchain-based solutions in IoT that ought to be resolved by the industry and research community.**

Keywords—Blockchain; IoT; scalability; issues; distributed ledger; throughput; latency

I. Introduction

The Internet of things (IoT) based solutions have evolved to cover every aspect of our daily lives. IoT technology has been deployed in various environments, including smart homes, healthcare, industrial etc. [1][2]. It is a collection of smart devices that are connected like a swarm of heterogeneous nodes. For decades, the centralized approach has been recognized as a widespread solution for such environments. However, the rapid increase in these nodes made it impractical to manage and maintain with the traditional centralized approach due to various scalability and speed challenges.

A decentralized approach seems to be a preferable candidate to address challenges within such complexed environments. It will assist in solving many challenges attached to IoT environments while reducing the significant costs related to the previously adopted centralized approach [80]. Blockchain technology is one of the most known decentralized approaches deployed to resolve concerns related to IoT devices [3]. It has demonstrated its efficiency and performance in the financial domain with applications, such as Bitcoin and Ethereum [4][5]. Blockchain is capable of keeping immutable records of every data generated and exchanged by IoT devices. Therefore, it can present a perfect solution in the following aspects:

- IoT environments need a layer to facilitate the interoperability of heterogeneous IoT devices. Blockchain can provide a composite layer above the peer-to-peer network with standard access for every IoT device.
- IoT environments require a tier to support the traceability of data among these IoT devices. Blockchain works as an immutable distributed ledger with a historic timestamp to ensure this feature for IoT devices.
- IoT environments are expected to provide security measures and improve trust aspects by deploying smart contacts and digital signatures.

While the deployment of blockchain technology in IoT-based environments offers various advantages, they still pose overarching scalability concerns due to the vast amount of data generated and the enormous number of IoT devices.

Traditional Blockchain platforms have inherited by design a challenge in their limited throughput. Throughput is determined by the number of transactions that can be appended and mined in the blockchain platform [77]. Various known blockchain platforms have different scalability rates, which is insufficient to handle the IoT environments [76][78]. For instance, Bitcoin has a limited number of transactions in a short period. The bitcoin network blocks are fixed in terms of size and frequency, which causes a scalability issue. The Bitcoin platform has even a lower throughput than Ethereum and other confidentiality issues [8]. However, the Ethereum platform is regarded to have a low throughput when deployed in IoT environments [6][7].

Researchers have carefully identified the so called scalability trilemma within the Blockchain environment [17], as depicted in Fig. 1. The concept, which Vitalik Buterin first coined, identifies the difficulty of finding a balance between three blockchain properties: decentralization, security, and scalability simultaneously [18]. Scalability trilemma means we can only achieve two out of the three properties at the same time. Furthermore, the scalability issue has some implications related to the cost of the blockchain database. Practically, all transactions must be stored within a chain, so the chain size will increase as we append more transactions to the chain. This can increase the size of the chain, and maintaining and managing the chain becomes more difficult with time.

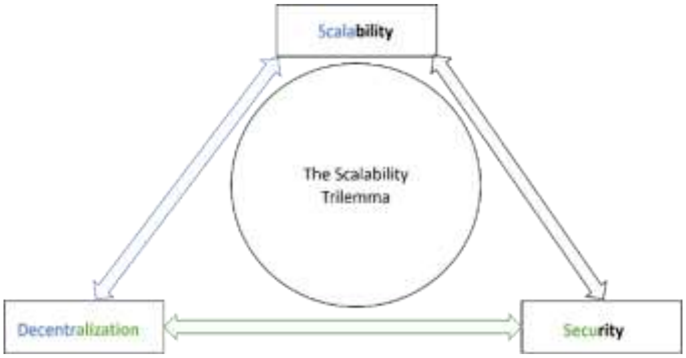

Fig. 1. The Blockchain Scalability Trilemma.

Currently, the blockchain size of Bitcoin and Ethereum are 354.419 GB and 870.37 GB, respectively [16][17]. Other blockchain platforms have been designed with high throughputs, such as IOTA, a commercial platform designed to be deployed in the IoT environment. However, it is regarded to have a long delay when addressing a massive amount of data [9]. Hyperledger Fabric and Ripple are two blockchain platforms that got high throughput [10][11]. Nevertheless, they suffer from the same issue of limited scalability, especially in terms of validating the nodes [12]. The following section will explain many solutions to tackle blockchain scalability issues.

In summary, we can summarize the contributions of our research as follows:

- Contribution one (theoretical): establish a fundamental understanding of the major scalability solutions using Blockchain in the IoT domain.
- Contribution two (theoretical): devise an evaluation framework for assessing the effectiveness of the current scalability solutions.
- Contribution three (empirical): evaluate existing scalability solutions with a focus on their strengths.

The remainder of this paper is divided into five sections. Section two reviews the Blockchain and IoT technologies. Section three compares various research scalability solutions that operate in different IoT layers. Section four proposes an evaluation framework and compares the Blockchain-based scalability solutions. Section five summarizes the key findings of our research.

II. Background Overview

A. Blockchain Technology

Blockchain, which is a distributed public ledger technology, was initially developed for cryptocurrencies such as Bitcoin. The concept of Blockchain was initially introduced by Nakamato [4] in 2008 but did not receive much attention initially. With the emergence of IoT in the past few years, Blockchain has started gaining the attention of researchers as a P2P technology for distributed and decentralized computation and data sharing. Blockchain can avert the possibility of intrusions by adopting cryptographic techniques in the absence of a centralized control environment. Interestingly, its unique security features, like transactional privacy, data immutability, authorization and integrity, fault tolerance, and transparency, allow Blockchain to be utilized in areas beyond cryptocurrency.

Blockchain technology has evolved around the idea that a single block, the fundamental component of Blockchain, stores certain types of information. The block is linked to similar blocks to form a chain where each block is associated with the previous block through a hash, as depicted in Fig. 2. The integrity of each block is assured by a hash function which is deployed to create a hash value of each block. The hash value is a digital fingerprint, which can be transformed to a different digital fingerprint by making minimal changes to the block, such as switching a bit value [52]. The hash value is the entity responsible for connecting every block with the previous block since each block possesses the block hash value behind it. Validation of the integrity by the system can easily be performed by running the hash function on every single block and then comparing the result with its prospective digital fingerprint.

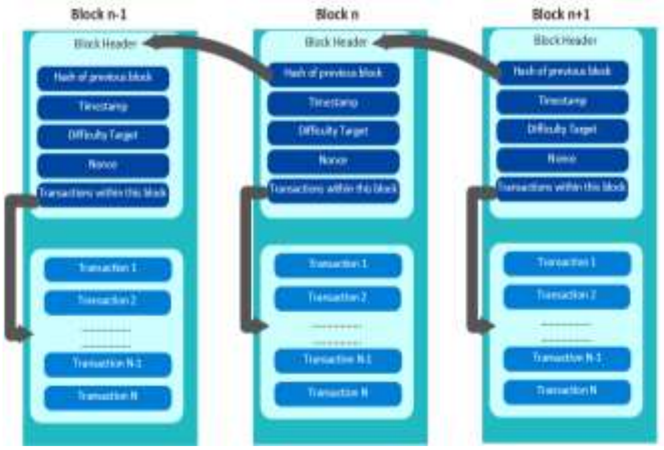

Fig. 2. The Blockchain Structure.

Blockchain technology is a decentralized ledger where each block is created and broadcasted to the connected peers. Therefore, each peer is guaranteed to have the identical most recent copy of the ledger. Thus, the forgery of a blockchain practically becomes very difficult. A blockchain environment has various characteristics, including decentralization, Tamper-proof, trustless, and anonymity.

- Decentralization: Blockchain is built around the idea of a distributed ledger with no central entity that controls the network. It means that the system is robust against a single point of failure. Therefore, if one node goes down, the system still functions properly.
- Tamper-Proof: The only way to take over the network is by launching a theoretical 51% attack [51]. In order to change the block content and make the validation process faster in comparison to all other peers within the network, the attacker roughly requires more than half of the computational power on Blockchain.
- Trustless: The blockchain environment depends on complete transparency. Thus, parties on the chain can trust each other.
- Anonymity: As mentioned above, there is no need for trust in the blockchain environment. Thus, parties on the chain remain anonymous with no need to reveal any party identity.

Furthermore, Blockchain can be arranged into three categories based on the participants' respective environment [27]. The categories can be summarized as follows:

1) Public blockchains: It is a permissionless blockchain that runs on a public network in a decentralized and distributed fashion. The environment is open, and any node can participate without any authorization [50].

2) Private blockchains: It is a permissioned blockchain that runs within a private network within an organization that governs and regulates all transactions.

3) Consortium blockchains: It is also a permissioned blockchain. However, it is initiated and controlled by related entities. A node must register ahead of their participation; then, they must adhere to rules and regulations.

Table I summarizes the key differences between the three blockchain categories.

B. *Internet of Things (IoTs) Technology*

Recently, the Internet of Things unleashed its power to deliver services across various domains from small businesses and social media to smart houses, smart cities, and industries. IoT connects resource-constrained heterogeneous devices with a broad range of functionalities in human and machine-centric communication networks. IoT has positively met the ever-evolving requirements of the above-mentioned sectors. However, the significant escalate in the number of such resource-constrained IoT devices and the massive information generated from them becomes a hurdle towards meeting the efficiency and security requirements.

TABLE I. COMPARISON OF MAJOR TYPES OF BLOCKCHAIN CATEGORIES

Characteristic	Public	Private	Consortium
Decentralization	Distributed Ledger	Centralized Ledger	Relatively Centralized Ledger
Immutability	Immutable	Not Immutable	Relatively Immutable
Transparency	Transpare nt	Not Transparent	Relatively Transparent
Scalability	Bad	Excellent	Good
Accessibility	Permissionless	Permissioned	Permissioned
Consensus Protocols	Proof of Work (PoW) & Proof of Stake (PoW)	Ripple	Practical Byzantine Fault Tolerance & Proof of Authority (PoA)
Example	Bitcoin & Ethereum	Ripple (XRP) & Multichain	Quorum & Hyperledger

The Internet of Things (IoT) is a network that attaches different devices to receive and transmit data over the Internet. The data is generated using various smart applications running on smart devices and sensors known as IoT devices. An estimated 50 billion IoT devices will be attached to the Internet worldwide in 2023 [49]. In Information Technology, IoT is undoubtedly a significant development connecting almost everything to the world wide web. Over the last few years, the increasing data rates and advancement in IoT paved the way for various concerns, with scalability being at the top of the list.

The IoT network consists of three layers, namely perception, communication, and industrial layer, as shown in Fig. 3. These sections can be briefly described as follows:

1) Perception layer: There are various IoT devices within this layer. These devices differ in function, which can include sensors, controllers, smart meters, etc. The primary function of these devices is sensing and collecting data from the physical environment. However, it might also react to actions in the physical environment.

2) Communication layer: There are several wireless/wired devices within this layer. These devices can be IoT gateway, Wi-Fi Access points, or small base stations. These devices deploy various communication protocols include Bluetooth, Near Field communication, etc. The primary function of these devices is to transfer data from the perception section to the industrial section.

3) Industrial layer: The industrial layer incorporates manufacturing, Airports, banks, supply chain etc. The decisions in these industrial organizations are build on the data gathered from the perception layer.

Previously, the centralized approach was the mainstream solution for handling complex structures of connected heterogeneous IoT devices. It was based on a traditional client server approach over the Internet. However, it suffered various challenges and is judged inadequate to handle data at this massive scale [80].

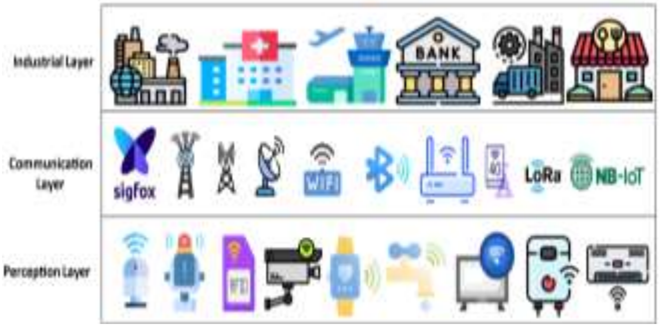

Fig. 3. Typical Three-Layer Internet of Things.

III. Analytical Comparison of Scalability Solutions

Due to the unraveled interest in deploying blockchain platforms in IoT systems, different approaches have been adopted to upgrade blockchain scalability. As mentioned, the challenge of enhancing blockchain scalability intensifies when more IoT devices/nodes are connected to each other and produce transactions at a higher rate. We identify and analyze the approaches published in recent literature to tackle the scalability issues. These approaches have been deployed in different layers of Blockchain and thereby can be classified as follows:

- Layer Zero "Approaches with the dissemination of Information": These proposed solutions focus on customizing the propagation protocol of information.
- Layer One "Approaches within the Blockchain": These proposed solutions focus on tackling the problem by changing the structure of blocks and consensus algorithms.
- Layer Two "Approaches off the Blockchain": These proposed solutions tackle the problem by executing some complex computational tasks off the Blockchain platform.

A. *Layer Zero: Approaches with Propagation Protocol*

Approaches dealing with the propagation protocol were classified recently by some researchers as a possible solution for scalability issues within Blockchain. Parties exchange and broadcast blocks of data/transactions inefficiently within the blockchain network, causing a high confirmation time. Enhancing and optimizing data transmission can result in improved throughput. Many studies have been published in layer zero, which can be explained in Table II.

B. *Layer One: Approaches within the Blockchain*

These proposed solutions on this approach focus on tackling the problem of scalability by different strategies, which can be viewed as follows:

- Redesign the structure of blocks.
- Implementing the DAG (Directed Acyclic Graph).
- Deploying Sharding techniques.
- Applying different consensus algorithms.

TABLE II. Comparison of Scalability Solutions within Layer Zero

Approach Name	How it Works	Advantages
BloXroute [70]	The design of the network is based on increasing the block size while decreasing the interval between blocks.	(+) Avoids forks (+) Enables fast propagations.
Velocity [71]	The structure of the protocol ensures an enhanced block propagation by deploying erasure code	(+) Increases throughput
Kadcast [72]	It is based on Kademlia Architecture, where it works similarly to the mechanism deployed for enhanced broadcasting with adjustable redundancy and overhead.	(+) Enables fast propagation (+) Enables secure transmission
Erlay [73]	The protocol improves the network connectivity while keeping the cost at a minimum level.	(+) Affordable cost (+) Private transmission

1) Redesigning the structure of blocks: The simplest approach to tackle the scalability concerns of Blockchain is redesigning the structure of blocks by increasing the block size. Practically, all transactions are appended within blocks in any blockchain platform. Since more transactions are recorded within a particular block, the throughput of transactions per block interval would consequently increase [13]. However, deploying such a simple approach comes with other direct and indirect challenges. One of these challenges is increasing the probability of hard forks in the blockchain platform. Consequently, a split of nodes within the Blockchain would happen as it happened in Bitcoin [14].

Traditionally, the Blockchain platform requires each node to record the complete history of all transactions to become a part of the network. An increase in block size means that each node must increase its storage requirements, making them more expensive to execute. Nodes that are not capable of securing such storage requirements would eventually be ruled out of the blockchain platform. As a consequence, a lesser number of centralized nodes would take control of the Blockchain. It leads Blockchain to lose its decentralized nature, so end users must have more trust in the protocol [15].

Redesigning the structured approach includes other techniques such a block compression. It can enhance the throughput of the Blockchain platform, where it reduces some unessential and redundant data of a block [22]. Compact block relay was designed and deployed according to the block compression approach [22]. It is based on changing the data structure of the original Bitcoin blocks along with shortening the transaction header data. Txilm is a technique based on the same concept of compression of blocks [22]. However, these kinds of techniques are prone to hash collisions.

2) Implementing Directed Acyclic Graph (DAG): The blockchain structure records transactions in chains that are arranged in a sole chain formation. Due to this type of liner formation, blocks are created one at a time with no concurrent operations. Consequently, Blockchain has a limited throughput with high latency. Allowing a concurrent operation would enhance throughput, so a new idea of blockchain structure build on DAG (Directed Acyclic Graph) is proposed [23].

The directed acyclic graph is a finite graph commonly deployed in a computer science major. The DAG-based blockchain Blockchain considers a block as a vertex in the DAG attached to other previous vertices. Moreover, The DAG-based Blockchain permits many vertices to be attached to a preceding vertex that creates simultaneous blocks. The IOTA foundation has designed its IoT-based Blockchain in the above-mentioned technique to address the scalability issues of Blockchain [28].

3) Deploying sharding techniques: The sharding technique was first developed within the database management field as an attempt to optimize large databases. It is based on partitioning a database into several physical fragments, where each fragment saves its distinct subset of the data. This divide of a large group across multiple servers permits the distributed management of operations of a single database, thus improving scalability [31]. Practically, it applies the concept of divide-and-conquer on the blockchain platform, so each platform will be divided into several smaller units called a shard. Fig. 4 shows the concept of the sharding technique on the blockchain platform. A pool of transaction is processed in multiple shards, that reduces the load on each node and makes it possible for nodes to process a small number of transactions. Recently, several studies have been published to tackle the scalability issues using the sharding technique to improve transaction throughput.

4) Applying different consensus algorithms: Various consensus algorithms have been used in different types of Blockchains. These consensus algorithms are used, so Blockchain becomes more resilient to malicious participants and message delays. Several algorithms are deployed in the research literature to solve security issues. However, each one of them has an overhead that affects blockchain throughput and scalability. Therefore, some optimizations are required to enhance the scalability of Blockchain. The essential consensus algorithms are as follows.

Proof of Work (PoW): To add blocks to the Blockchain, each node must perform some exclusive work known as Proof-of-Work (PoW) [36]. In Bitcoin, each node must compute a hash value less than a specific number, which is also known as the difficulty level set by the Blockchain. The difficulty level is changed periodically by the Bitcoin protocol, where it takes between five to ten minutes to produce a single block [36]. The procedure of finding a solution to the PoW puzzle (i.e., to find a winning hash value) is also called mining. Speed is critical in the the operation, so the mining prize is given to the first node that computes a winning hash. Furthermore, the node gets to include its proposed block in the Blockchain. Once a node finds a winning hash and broadcasts it to others. Next, other nodes have to confirm that the proposed hash value is correct and valid [37]. Since several nodes are computing the winning hash simultaneously, there is a possibility that several nodes compute the winning hash at the same time. Sequentially, each wining node includes its block, the Blockchain announces it over the peer-to-peer network. In such a scenario, there are temporary forks in the Blockchain due to some nodes including their block into the first branch of the Blockchain and others include in the second branch and so on. To fix this problem, the protocol will choose the longest branch and delete the other branches [36]. Due to the previous challenges in the original PoW algorithm, many optimization techniques were proposed to enhance the algorithm scalability [38][39][40].

Proof of Stake (PoS): It is deployed to avoid the PoW algorithm weaknesses. It replaces the mining process with an alternative idea where users can own a virtual currency in the blockchain platform. Practically, users can buy any amount of cryptocurrency and then utilize it in the form of the stake to purchase equivalent block creation chances in the blockchain platform by working as a validator. The validator cannot predict its turn ahead of time since the algorithm randomly chooses the validator node to create the block. At its original form, the algorithm has a problem called Nothing-at-Stake, where the algorithm does not provide incentives for nodes to vote for the accurate block. Nodes might vote for blocks supporting several forks and branches to maximize their chances of winning a reward as they do not consume anything from their resources [36]. There are other problems with the PoS where it assumes that the chances of an attack on the blockchain by the nodes having a higher amount of currencies are minimal. [37]. Therefore, several alternative solutions were proposed where [41] deploys randomization techniques to forecast the next validator. It utilizes a mechanism that finds the lowest hash number in combination with the length of the stake. Peercoin [42] selection is based on coin age-based selection, where older coins have a greater possibility of mining the next block. However, Ethereum is trying to switch from Ethash [43] to Casper [44].

Other Consensus Algorithms: Several consensus algorithms focus on tackling many problems where scalability is one of them. Other mentionable consensus algorithms available in the literature include Delegated Proof of stake [81], Practical Byzantine Fault Tolerance [82], Hybrid Consensus [83], Proof of Authority [84], Proof of Capacity [85], Proof of Participation [86]. Surveys comparing consensus algorithms are available in [19], [20],[61],[53], and [73]. We recommend analyzing these algorithms in future works.

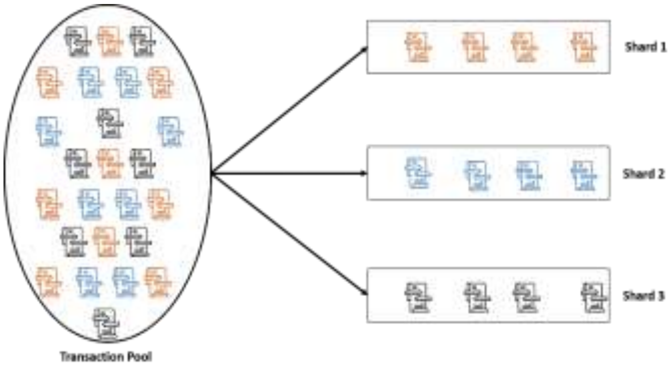

Fig. 4. An Exemplary Illustration of Sharding Techniques.

C. Layer Two: Approaches off the Blockchain

The proposed solutions in this approach focus on tackling scalability by executing some complicated computational work outside the Blockchain platform. These solutions apply different strategies, including payment channel, sidechain, off-chain computation, and cross-chain techniques. Below we provide an analysis of each approach.

1) Payment channels: The strategy of the payment channel is based on creating a temporary off-chain channel where some transactions can be executed off-chain so to reduce the volume on the main network and increase the transaction throughput of the whole Blockchain. Example approaches that employ payment techniques are described in Table III.

Fig. 5 demonstrates the concept of the lightning network technique, which includes three stages as described below:

- Establishing the channel by depositing some number of tokens in the channel (recorded on the main chain)
- Trading between two parties (recorded off the chain).
- Closing the channel where the number of tokens of both parties is recorded on the main chain.

2) Sidechain techniques: The Sidechain technique was first proposed at Pagged Sidechain [61]. Generally, it allows the assets in a specific blockchain to be moved between various sub-blockchains. It guarantees assets to be secure and saved. Several key sidechain algorithms are described in Table IV.

TABLE III. COMPARISON OF SCALABILITY SOLUTIONS USING PAYMENT CHANNEL TECHNIQUES

Approach Name	How it Works	Advantages
Lightning Network [45]	Uses two parties of Blockchain to establish their own off-chain private trading channel. The channel is dedicated to several low latency transactions.	(+) provides private communication
Raiden Network [46][47]	The technique is payment-based. The Raiden Network is deployed on the Ethereum network with support for all ERC20 [47].	(+) enables secure communication

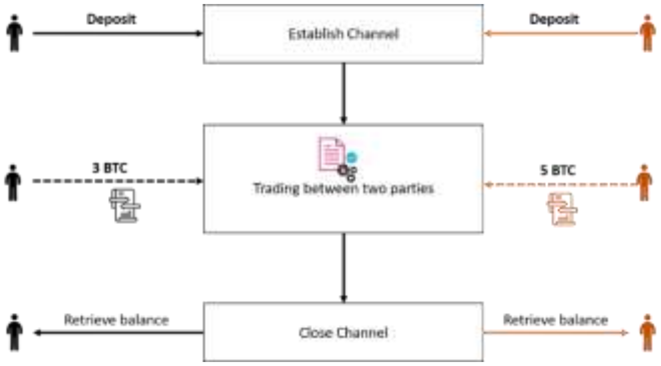

Fig. 5. An Exemplary Illustration of the Lightning Network

TABLE IV. COMPARISON OF SCALABILITY SOLUTIONS USING SIDECHAIN TECHNIQUES

Approach Name	How it Works	Advantages
Plasma [60]	The protocol permits a parent chain to create smaller copies as child chains. The created copy of a parent chain is designed and developed according to a specified use case. The parent chain delegates its work to child chains.	(+) improves the transaction throughput (+) delegates work to child chains
Pegged Side Chain [48]	The approach is based on a two-way peg, transferring the assets from the main chain to a child chain. It ensures that these assets are securely sent from the parent to a child by locking them until the pegged side chain obtains a simplified Payment Verification (SPV) proof. A confirmation period is enforced for security reasons. The newly transferred assets are halted on the sidechain to keep away from double-spending issues. The exact logic is applied once transferring the assets back to the main chain.	(+) provides secure communication
LiQuidity Network (NOCUST) [62]	The network is based on a data architecture named Merkleized Interval Tree. It is formed of a multi-layered tree which is deployed on NOCUST. It allows the party's' balances to be saved on private non-crossing interval space. Practically, all balances are verified against the amount registered in the smart contract on the main network.	(+) ensures the correctness of computations

3) Off-Chain computation: In Ethereum, miners must execute all contracts to validate their states. The operation is known to be costly and time-consuming. Therefore, many techniques help to build a scalable platform. Table V lists example off-chain computation techniques.

TABLE V. COMPARISON OF SCALABILITY SOLUTIONS USING OFF-CHAIN TECHNIQUES

Approach Name	How it Works	Advantages
Truebit [63]	It is designed based on outsourcing computations to trusted third parties known as solvers and challengers. Tokens are deposited to the smart contract by the solver. The challenger verifies the work done by the solver and gets compensation for its work.	(+) guarantees correctness of computations (+) adapts to computationally intensive applications.
Arbitrum[64]	Enables nodes to deploy smart contracts as virtual machines that include all rules of a contract. It has four types of roles: - Verifier: it acts as a global entity to validate transactions and publish accepted transactions. Key: it is a participant entity that can own currency and propose transactions. Virtual Machine: it is a virtual participant in the protocol which can own currency and exchange them. Manager: it manages the virtual machine and makes sure its correctness.	(+) enhances blockchain scalability

4) Cross-Chain techniques: Cross-chain techniques are considered to be potential solutions to improve scalability in Blockchain. Generally, these techniques are based on the interoperability among several separated chains. Therefore, the inter-connection between these chains can result in enhancing scalability. Fig. 6 depicts an example of the main cross-chain techniques. There are two main cross-chain algorithms which are listed in Table VI.

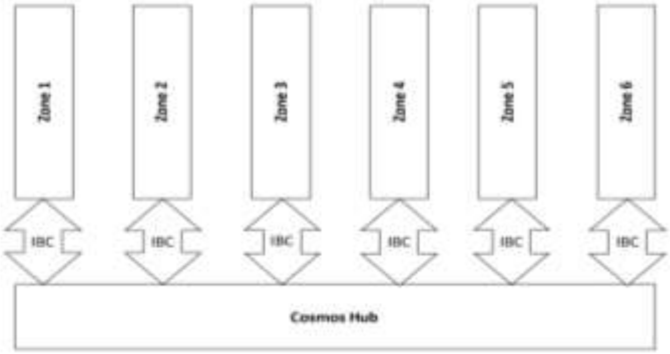

Fig. 6. An Exemplary Illustration of the Cosmos Network.

TABLE VI. COMPARISON OF SCALABILITY SOLUTIONS USING CROSS-CHAIN TECHNIQUES

Approach Name	How it Works	Advantages
COSMOS -+[65]	It is based on parallel independent Blockchain named as zones. The Tendermint BFT consensus algorithm supports each zone. The Cosmos Hub connects these zones.	(+) Increases throughput (+) Deploys Inter-blockchain communication protocol for privacy
POLKADOT [66]	It is based on a multi-chain protocol that attaches various blockchains with a relay chain. The relay chain allows separated blockchains to communicate with each other. The Polkadot acts as a mediator that connects to already functioning blockchains.	(+) Increases throughput (+) Secure communication

IV. Scalability Evaluation Framework and Analysis Result

Scalability can be defined to incorporate some dimensions. The traditional definition stipulates from three perspectives, namely throughput, storage, and latency [74][75][79]. Blockchain is considered a network that can be measured by standard performance metrics like throughput and latency [77]. Since we are talking about Blockchain, throughput can be clearly associated with the number of committed valid transactions within the Blockchain per second [77]. Therefore, we can represent the throughput as follows:

Transaction Throughput=Number of Committed Transaction /Time in Seconds (1)

Latency is also associated with transaction latency which is defined as the proportion of the Blockchain to commit a transaction [77]. Therefore, we can represent the latency as follows:

Transaction Latency= (Confirmation Time * Blockchain Threshold)- Submission Time (2)

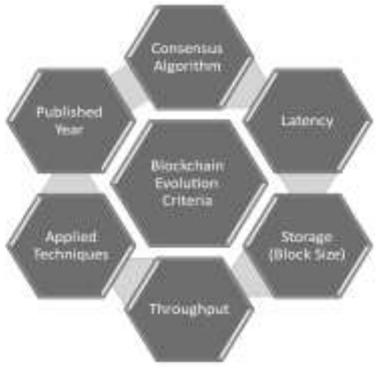

Fig. 7. Our Scalability Evaluation Framework.

Both performance metrics, throughput and latency, are closely related to the block size. Various blockchain networks suffer from issues about standing by for transactions to be committed within the block due to the fixed size of blocks [78]. Therefore, it is a critical parameter that must be included in blockchain network evaluations. Furthermore, Consensus algorithms and applied techniques are closely related to our scalability analysis, so we added them in our evaluation, as depicted in Fig. 7.

A. Comparison of the Scalability Blockchain-based Architectures

As mentioned above, this paper's main contribution is to analyze each Blockchain architecture and its main characteristics affecting IoT scalability. Our scalability evaluation framework incorporates various dimensions. Our selected dimensions include 1) throughput, 2) storage (block size), 3) latency, 4) deployed techniques, and 5) consensus algorithm. We will base our comparative evaluation on these criteria. Table VII details the findings of the comparison.

B. Summary of Scalability Issues

Our detailed analysis of state-of-the-art architectures aimed at resolving scalability challenges pertaining to blockchain solutions that could enhance the IoT domain. The significant challenges are summarized below.

- Challenge One: scalability is closely related to block the size. If the block size exceeds the network capacity, the block will not be attached to the chain. As a consequence, some solutions strive to increase the block size.

- Challenge Two: although increasing the block size enhances performance, it may increase the probability of blockchain forks. Therefore, other solutions enforce mechanisms to prevent the occurrence of forks.

- Challenge Three: scalability can be achieved by reducing some data within the block, so some solutions attempt to deploy compression techniques. However, it may affect valuable information about the block node states and records.

- Challenge Four: transactions are committed in the block only if all peers agree on its validity. As a result, the network suffers slow speed in appending transactions till it reaches consensus between the participating parties. Some solutions focused on implementing consensus algorithms to reduce the time required to achieve total agreement between peers.
- Challenge Five: more innovative solutions tried to redesign the structure of the Blockchain. Consequently, DAG and Sharding structures are deployed to avoid sequential execution of transactions which is adapted by the original blockchain structure. However, these structures inherite by design other issues. Data validity and availability are common issues within the Sharding structures, while computing power and cost are major concerns in the DAG structures.
- Challenge Six: scalability solutions are deployed outside the blockchain environments by outsourcing computationally intensive operations to a third party so the main chain can execute other light operations simultaneously. Accomplishing parallel execution of transactions enhance the prospect of scalability. However, the appeal of blockchain comes from the fact that we do not have to rely on third parties. By outsourcing the operations, we surrender an advantage and restrict the environment. Furthermore, concerns about third party's trustworthiness, security and privacy need to be resolved.

TABLE VII. A COMPARISON OF RECENT BLOCKCHAIN SOLUTIONS USING SCALABILITY DIMENSIONS

Blockchain Technology	**Distributed Technology**	**Throughput (Transactions per Seconds)**	**Latency (Secs)**	**Block Size (MB)**	**Consensus Algorithm**	**Year Originated**
Bitcoin [4]	List of blocks	7	600	1	Proof of Work (PoW)	2009
Segregated Witness [58]	Segregate digital sign	7	NA	4	Witnesses	2015
Inclusive block chain protocols [24]	Block DAG	65	NA	NA	Proof of work (PoW)	2015
IOTA [28]	Tx DAG	500	60	NA	Weight of transactions	2016
Byteball [29]	Tx DAG	20-30	60	NA	Witnesses	2016
Spectre [25]	Block DAG	NA	NA	NA	Proof of work (PoW)	2016
ByzCoin [67]	Apply different consensus algorithm (PBFT)	1000	20-15	NA	PBFT	2016
ELASTICO [32]	Sharding Technique	40	800	1	Proof of work (PoW) & PBFT	2016
ZILLIQA [57]	Sharding technique	2828	NA	NA	PoS	2017
Algorand [68]	Apply different consensus algorithms	875	22	NA	Byzantine Agreement	2017
Ouroboros [59]	Coin-flipping technique	257.6	120	NA	PoS Apply different consensus algorithm (PoS)	2017
Conflux [21]	DAG	6400	270-444	NA	PoS	2018
Phantom [26]	Block DAG	NA	NA	1	Proof of work (PoW)	2018
Nano [30]	Block-lattice	7000	1 to 10	NA	Weighted votes on transactions	2018
RapidChain [34]	Sharding technique	7380	7380	1	PBFT	2018
OmniLedger [33]	Sharding Technique & Block DAG	3500	800	1	PBFT	2018
DLattice [54]	Double DAG	1200	10		PANDA	2019
Monoxide [35]	Sharding technique	11694	13-21	1	Asynchronous consensus & Proof of work (PoW)	2019
CoDAG [55]	Block DAG	1151	NA	NA	NA	2020
Ostraka [56]	Sharding technique	400000	NA	1	Bitcoin-NG	2020
Meepo [69]	Sharding technique	120000	0.4-0.5	NA	consortium consensus	2021

V. Conclusion and Future Work

Enormous efforts have been made towards solving the scalability issues within Blockchain to adapt this promising solution to connecting heterogeneous IoT devices. In this paper, various scalability solutions were presented and compared according to their layer within the blockchain network. Next, the paper evaluated these solutions according to standard performance indicators such as throughput, latency, and storage. The paper attempted to summarize the existing blockchain solutions at different layers so to serve as a roadmap for more improvements by other researchers. In the future, we plan to extend our comparative analysis to investigate other issues impacting the blockchain-based networks, particularly those associated with security aspects.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, Vol. 4 (5), pp. 1125-1142, (2017).

[2] Alrehaili, Ahmed, and Aabid Mir. "POSTER: Blockchain-based Key Management Protocol for Resource-Constrained IoT Devices." 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH). IEEE, (2020).

[3] A. Reyna, C. Mart´ın, J. Chen, E. Soler, and M. D´ıaz, "On Blockchain and its integration with IoT. challenges and opportunities," Future generation computer systems, vol. 88, pp. 173–190, (2018).

[4] S. Nakamoto, "Bitcoin: A peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf (2009).

[5] G. Wood, "Ethereum: A Secure Decentralised Generalized Transaction Ledger", https://gavwood.com/paper.pdf

[6] Nejc Zupan, Kaiwen Zhang, and Hans-Arno Jacobsen. 2017. Hyperpubsub: A decentralized, permissioned, publish/subscribe service using blockchains: demo. In Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. 15–16, (2017).

[7] Seyoung Huh, Sangrae Cho, and Soohyung Kim. Managing IoT devices using blockchain platform. In Proceedings of the 19th International Conference on Advanced Communication Technology. 464–467, (2017).

[8] Merve Can Kus Khalilov and Albert Levi. 2018. A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Commun. Surv. Tutor, 1–44. https://ieeexplore.ieee.org/abstract/document/8325269, (2018).

[9] Bogdan Cristian Florea. Blockchain and internet of things data provider for smart applications. In Proceedings of the 7th Mediterranean Conference on Embedded Computing. 1–4, (2018).

[10] Hyperledger. Hyperledger-fabricdocs documentation release v0.6. Retrieved from https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/v0.6/hyperledger-fabric.pdf,(2017).

[11] Ripple. Solution overview. Retrieved from https://whitepaperdatabase.com/wp-content/uploads/2017/09/Ripple-XRP-Whitepaper.pdf, (2017).

[12] Runchao Han, Vincent Gramoli, and Xiwei Xu. 2018. Evaluating blockchains for IoT. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security. 1–5, (2018).

[13] Jeff Coleman. State channels wiki, https://github.com/ledgerlabs/state-channels/wiki, (2016).

[14] Mattias Scherer. Performance and scalability of blockchain networks and smart contracts, 2 https://umu.diva-portal.org/smash/get/diva2:1111497/ FULLTEXT01.pdf, (2017).

[15] Luke-jr. Block size limit controversy, https://en.bitcoin.it/wiki/Block_size_limit_controversy, (2015).

[16] BitInfoCharts. URL: https://bitinfocharts.com/ethereum/, https://ycharts.com/indicators/ethereum_chain_full_sync_data_size Accessed 2021-07-14.

[17] Blockchain.com URL: https://www.blockchain.com/ko/charts/blocks size, https://ycharts.com/indicators/bitcoin_blockchain_size Accessed 2021-07-14.

[18] Ometoruwa, T. (2018), Solving the blockchain trilemma: Decentralization, security & scalability, www.coinbureau.com/ analysis/solving-blockchaintrilemma/, (2018).

[19] Nguyen, Giang-Truong, and Kyungbaek Kim. "A survey about consensus algorithms used in blockchain." Journal of Information processing systems 14.1, 101-128,(2018).

[20] Bamakan, Seyed Mojtaba Hosseini, Amirhossein Motavali, and Alireza Babaei Bondarti. "A survey of blockchain consensus algorithms performance evaluation criteria." Expert Systems with Applications 154 ,113385,(2020).

[21] C. Li, P. Li, D. Zhou,W. Xu, F. Long, and A. Yao, ``Scaling nakamoto consensus to thousands of transactions per second,", arXiv:1805.03870. [Online]. Available: https://arxiv.org/abs/1805.03870, (2018).

[22] Bip152. Comact Block Relay [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki Accessed on May 5, 2021.

[23] Shrier, Ian, and Robert W. Platt. "Reducing bias through directed acyclic graphs." BMC medical research methodology 8.1, 1-15,(2008).

[24] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, ``Inclusive block chain protocols," in Proc. Int. Conf. Financial Cryptogr. Data Secur. San Juan, Puerto Rico: Springer, pp. 528_547, (2015).

[25] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, ``Spectre: A fast and scalable cryptocurrency protocol," IACR Cryptol. ePrint Archive, vol. 2016, p. 1159, (2016).

[26] Y. Sompolinsky and A. Zohar, ``Phantom: A scalable blockdag protocol," IACR Cryptol. ePrint Archive, vol. 2018, p. 104, (2018).

[27] Lin, Iuon-Chang, and Tzu-Chun Liao. "A survey of blockchain security issues and challenges." Int. J. Netw. Secur. 19.5: 653-659,(2017).

[28] Iota. [Online]. Available: https://www.iota.org/ accessed on May 5, 2021.

[29] A. Churyumov. Byteball: A Decentralized System For Storage and Transfer of Value. [Online]. Available: https://byteball.org/Byteball.pdf accessed on May 5, 2021, (2016).

[30] C. LeMahieu. Nano: A Feeless Distributed Cryptocurrency Network. [Online]. Available: https://nano.org/en/whitepaper accessed on May 5, 2021.

[31] Weinan Wang, Joseph E Magerramov, Maxym Kharchenko, Min Zhu, Aaron D Kujat, Alessandro Gherardi, and Jason C Jenks. Facilitating data redistribution in database sharding, April 23, 2013. US Patent 8,429,162,(2013).

[32] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur.-CCS, pp. 17_30,(2016).

[33] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, ``OmniLedger: A secure, scale-out, decentralized ledger via sharding," in Proc. IEEE Symp. Secur. Privacy (SP), pp. 583_598, (2018).

[34] M. Zamani, M. Movahedi, and M. Raykova, ``RapidChain: Scaling blockchain via full sharding," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 931_948, (2018).

[35] J. Wang and H. Wang, ``Monoxide: Scale out blockchains with asynchronous consensus zones," in Proc. 16th USENIX Symp. Netw. Syst. Design Implement. (NSDI), pp. 95_112,(2019).

[36] A. Baliga, "Understanding blockchain consensus models," Tech. rep., Persistent Systems Ltd, Tech. Rep., (2017).

[37] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. 'An overview of blockchain technology: Architecture, consensus, and future trends', Proceedings of the 2017 IEEE BigData Congress, Honolulu, Hawaii, USA, pp.557–564,(2017).

[38] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, ``Bitcoin-NG: A scalable blockchain protocol," in Proc. 13th USENIX Symp. Netw. Syst. Design Implement. (NSDI), pp. 45_59,(2016).

[39] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, ``Spectre: A fast and scalable cryptocurrency protocol," IACR Cryptol. ePrint Archive, vol. 2016, p. 1159,(2016).

[40] Y. Sompolinsky and A. Zohar, ``Secure high-rate transaction processing in bitcoin," in Proc. Int. Conf. Financial Cryptogr. Data Secur. San Juan, Puerto Rico: Springer, pp. 507_527, (2015).

[41] P. Vasin, “Blackcoins proof-of-stake protocol v2,” [Online]. Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf, (2014).

[42] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” Self-Published Paper, August, vol. 19, (2012).

[43] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, (2014).

[44] V. Zamfir, “Introducing casper the friendly ghost,” Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casperfriendly-ghost, (2015).

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

[46] Raiden Network. [Online]. Available: https://raiden.network/ accessed on May 5, 2021.

[47] Erc20 Token Standard. [Online]. Available: https://theethereum.wiki/w/index.php/ERC20_Token_Standard accessed on May 6, 2021.

[48] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. (2014). Enabling Blockchain Innovations with Pegged Sidechains. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingblockchaininnovations-with-pegged-sidechains,(2014).

[49] S. Sorrel, “The Internet of Things: Consumer, Industrial & Public Services 2018-2023,” Eds. Juniper, (2018).

[50] G. W. Peters and E. Panayi. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of money. banking beyond banks and money. In Banking Beyond Banks and Money, pages 239–278. Springer, Cham, (September 2016).

[51] K. Gagneja, R. Kiefer, “Security Protocol for Internet of Things (IoT): Blockchain-based Implementation and Analysis” 2020 Sixth International Conference on Mobile and Secure Services (MobiSecServ), (March. 2020).

[52] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623, March 2017.

[53] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T.. A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), 1432-1465,(2020).

[54] T. Zhou, X. Li, and H. Zhao, ‘‘DLattice: DLattice: Permission-Less Blockchain Based on DPoS-BA-DAG Consensus for Data Tokenization,’’ IEEE Access vol. 7, pp. 39273–39287, (2019).

[55] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, ‘‘An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4134-4145, (Jun. 2020).

[56] Manuskin, A., Mirkin, M., & Eyal, I. "Ostraka: Secure blockchain scaling by node sharding". In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW) (pp. 397-406). IEEE,(2020, September).

[57] Team, Z.. The ZILLIQA technical whitepaper. https://doi.org/10.2139/ssrn.3442330, (2017).

[58] L. Eric, L. Johnson, and W. Pieter. (2015). Segregated Witness Github Repository. Accessed: Jan. 15, 2021. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki,(2015).

[59] A. Kiayias, A. Russell, B. David, and R. Oliynykov, ``Ouroboros: A provably secure proof-of-stake blockchain protocol," in Proc. Annu. Int. Cryptol. Conf. Santa Barbara, CA, USA: Springer, pp. 357_388,(2017).

[60] Poon, J., & Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. White paper, 1-47,(2017).

[61] Sankar, L. S., Sindhu, M., & Sethumadhavan, M.. Survey of consensus protocols on blockchain applications. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1-5). IEEE, (January 2017).

[62] "Liquidity Network" https://liquidity.network.

[63] Teutsch, J. & Reitwießner, C. (2019). A scalable verification solution for blockchains. arXiv preprint arXiv:1908.04756,(2019).

[64] 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),(2018).

[65] https://v1.cosmos.network/resources/whitepaper.

[66] Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White Paper,(2016).

[67] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khof_, L. Gasser, and B. Ford,``Enhancing bitcoin security and performance with strong consistency via collective signing," in Proc. 25th USENIX Security Symp. USENIX Secur., pp. 279_296, (2016).

[68] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, ``Algorand: Scaling byzantine agreements for cryptocurrencies," in Proc. 26th Symp. Operating Syst. Princ.-SOSP, pp. 51_68,(2017).

[69] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Sharded Consortium Blockchain," IEEE 37th International Conference on Data Engineering (ICDE), 2021, pp. 1847-1852, doi: 10.1109/ICDE51399.2021.00165, (2021).

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

[71] Chawla, N., Behrens, H. W., Tapp, D., Boscovic, D., & Candan, K. S. 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, (May 2019).

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

[73] Bouraga, S. A taxonomy of blockchain consensus protocols: A survey and classification framework. Expert Systems with Applications, 168, 114384 (2021).

[74] Naumenko, G., Maxwell, G., Wuille, P., Fedorova, A., & Beschastnikh, I. 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, (November 2019).

[75] Zhou, Qiheng, Huawei Huang, Zibin Zheng, and Jing Bian. "Solutions to scalability of blockchain: A survey." IEEE Access 8: 16440-16455,(2020).

[76] Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S.. Blockchain and scalability. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 122-128). IEEE,(July 2018).

[77] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P.. 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 , (October 2016).

[78] Hang, Lei, and Do-Hyeun Kim. "Optimal Blockchain Network Construction Methodology Based on Analysis of Configurable Components for Enhancing Hyperledger Fabric Performance." Blockchain: Research and Applications : 100009,(2021).

[79] Kim, Soohyeong, Yongseok Kwon, and Sunghyun Cho. "A survey of scalability solutions on blockchain." 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, (2018).

[80] Nartey, Clement, et al. "On blockchain and IoT integration platforms: current implementation challenges and future perspectives." Wireless Communications and Mobile Computing 2021 (2021).

[81] Larimer, Daniel. "Delegated proof-of-stake (dpos)." Bitshare whitepaper 81:85,(2014).

[82] Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." OSDI. Vol. 99. No. 1999. (1999).

[83] Pass, Rafael, and Elaine Shi. "Hybrid consensus: Efficient consensus in the permissionless model." 31st International Symposium on Distributed Computing (DISC 2017). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017,(2017).

[84] De Angelis, Stefano, et al. "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain." (2018).

[85] Sharma, Kapil, and Deepakshi Jain. "Consensus algorithms in blockchain technology: A survey." 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, (2019).

[86] Nandwani, Arpit, Mudit Gupta, and Narina Thakur. "Proof-of-participation: Implementation of proof-of-stake through proof-of-work." International Conference on Innovative Computing and Communications. Springer, Singapore, (2019).