IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 May 2024, accepted 27 May 2024, date of publication 3 June 2024, date of current version 12 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3408868

SURVEY

A Survey of Blockchain Based Systems: Scalability Issues and Solutions, Applications and Future Challenges

TURKI ALI ALGHAMDI [1], RABIYA KHALID [2], AND NADEEM JAVAID [3,4], (Senior Member, IEEE)

[1] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia
[2] School of Computing, University of Leeds, LS2 9JT Leeds, U.K.
[3] Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[4] International Graduate School of Artificial Intelligence, National Yunlin University of Science and Technology, Douliu 64002, Taiwan

Corresponding author: Nadeem Javaid (nadeemjavaidqau@gmail.com)

ABSTRACT Blockchain technology originated alongside Bitcoin as a novel method of conducting financial transactions. It has garnered significant attention from both industry and academia in recent years, emerging as a prominent area of research. It is a decentralized record-keeping system that holds transactional information. The scale of a blockchain network expands according to the growth in the number of nodes and transactions, resulting in issues related to storage capacity, data processing speed, and time delay. These issues have a direct impact on the scalability of a blockchain network. Currently, scalability is one of the prominent concerns in the field of blockchain technology and an active research area. This study conducts a comprehensive survey of the scalability challenges faced by blockchain technology in several sectors. It also examines potential solutions based on consensus mechanisms, smart contracts and directed acyclic graph (DAG). It is observed that the proposed scalability solutions target enhancing system throughput, reducing costs, and improving blockchain efficiency. Therefore, we examine, compare, and evaluate the literature using these specific criteria. Moreover, a survey of existing blockchain based survey papers is presented. A comparative analysis of these survey papers is presented along with their recency score, which is determined by the number of recent publications reviewed in a survey paper. By "recent," we mean the current year (or the publication year of a survey paper) and the three years prior to it. Additionally, this paper offers an elaborate discussion on the forthcoming open research challenges and applications of blockchain.

INDEX TERMS Blockchain, consensus algorithms, transactions, ledger, scalability, smart contract, data immutability.

I. INTRODUCTION

The emergence of modern technologies has revolutionized the world [1]. Blockchain is one of the such technologies, which provides transparency, decentralization, security and equality of nodes on the Internet [2], [3]. It was proposed in 2008 by Satoshi Nakamoto [4] for the implementation of Bitcoin (a cryptocurrency). Blockchain is a chain of immutable distributed ledgers, which grows continuously. New blocks of data are appended to the chain containing multiple transactions in a system. The building blocks of this technology include consensus algorithms, cryptographical hashes, digital signatures, etc. Each block has two parts: header and main body. The Former contains hashes of previous and current blocks and the latter includes transactions of the chain.

The success of Bitcoin has paved the way for blockchain in the present age and it is being deployed in different fields of everyday life. Major applications of blockchain include health services, smart grids, autonomous industry, educational and business applications, Internet of things (IoT), supply chains, voting and many more [5]. Previously,

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

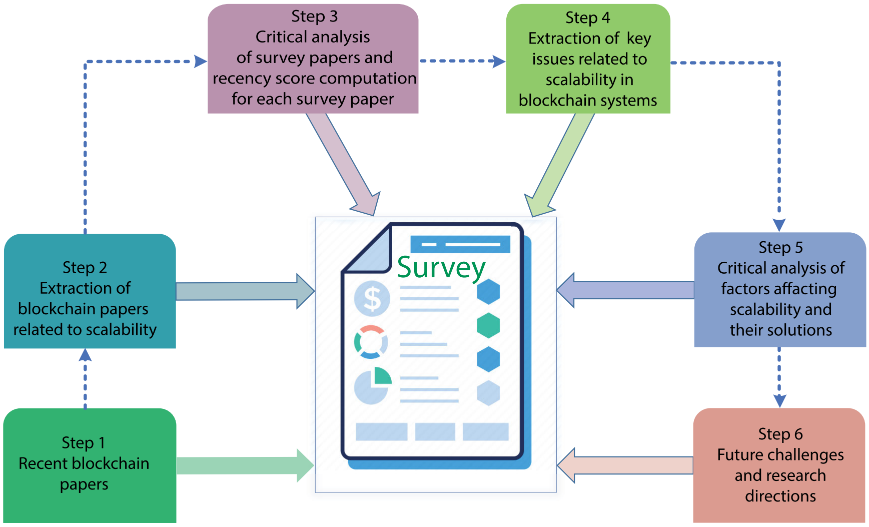

Step 3
Critical analysis of survey papers and recency score computation for each survey paper
Step 4
Extraction of key issues related to scalability in blockchain systems
Step 2
Extraction of blockchain papers related to scalability
Survey
Step 5
Critical analysis of factors affecting scalability and their solutions
Step 1
Recent blockchain papers
Step 6
Future challenges and research directions

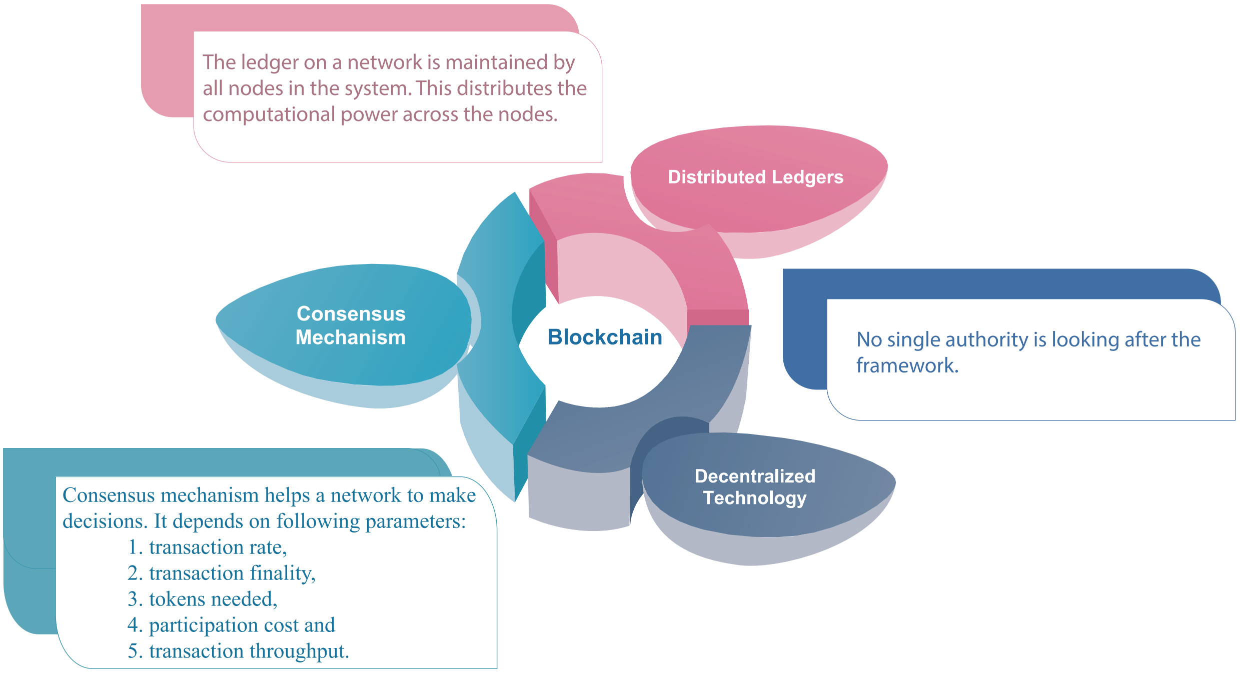
FIGURE 1. Road map of survey paper.

trading between two parties was dependent on a central party. All the agreements were made through the central entity instead of direct communication. However, the addition of the central entity has several issues. Fore example, in case of data sharing, the shared data resides in the database of a central entity and it is prone to security and privacy issues. Moreover, the maintenance cost of central entities is also there, which participants of the networks have to pay. Furthermore, there are several other issues (single point of failure, network bottleneck, denial of service attacks, etc.) for which, blockchain has emerged as a promising solution.

Blockchain is an emerging area and researchers are actively working on its deployment in several fields. Despite this, it has some limitations in its practical implementation, such as limited storage, low rate of transactions, determining a suitable block size, etc. [6], [7], [8]. The size of blockchain increases rapidly and each network node stores a complete copy of it. So, the nodes need to have large storage space to become part of the blockchain network. The low transactional rate slows down the system and with the increase in the network density, the transactional delays also increase. Moreover, determining the optimal block size is also an issue as a smaller block means frequent mining and larger block size increases the validation time and requires larger bandwidth. All of these fall under the scalability issue, which is the major challenge being faced by blockchain nowadays. Researchers are actively working on these issues and proposing novel solutions. These solutions are discussed in Section VI in detail.

Scalability is the property to handle a growing amount of work by adding resources to the system [9]. It directly affects the robustness, performance and adaptability of any system. To check the scalability of a system, it is observed that either increment in the input size affects the system performance or not. If this increment does not affect the system's performance and the system continues the operations efficiently then it is considered to be a scalable system [10]. In a blockchain system, the scalability issues are categorized into three different categories: throughput, storage and cost [11]. These categories depend on each other, e.g., in many cases, transactions in a blockchain face latency issues due to the limited size of the block. When a block is appended to the chain, it requires miners to solve a complex mathematical puzzle, which requires computational efforts and time. The block generation time cannot be minimized. Hence, throughput is affected [12]. Additionally, the requester is required to pay a cost, known as gas, for each transaction. This fee is a small payment imposed by the system for every transaction. Within the context of the blockchain, throughput is measured by the pace at which blocks are produced per second. The choice of consensus method determines how blockchain nodes interact to verify a transaction‘s legitimacy and maintain data confidentiality. Another important factor affecting scalability is storage. As the size of a blockchain increases daily, so, there is a need for an efficient storage system. Off-chain data storage can be a promising solution [2]. Furthermore, in the blockchain system, execution and transaction costs are measured in terms of gas consumption. If there is a linear increase in gas consumption while increasing the number of inputs, then the system is considered scalable. Moreover, their is a limit for gas consumption during a specific interval, for example, Ethereum has the gas limit of 15s [13].

In this paper, we present a survey of survey papers in the field of blockchain. This existing survey papers are examined by focusing on their significant contributions. The literature reveals the lack of survey papers that comprehensively study scalability concerns in the blockchain domain along with their corresponding solutions. Hence, In this paper, we have discussed and highlighted the blockchain scalability



The ledger on a network is maintained by all nodes in the system. This distributes the computational power across the nodes.

No single authority is looking after the framework.

Consensus mechanism helps a network to make decisions. It depends on following parameters:
1. transaction rate,
2. transaction finality,
3. tokens needed,
4. participation cost and
5. transaction throughput.

FIGURE 2. Core components of blockchain.

problems present in the existing systems along with the solutions. This type of survey is vital to give the new readers an overview of existing problems and help them in gaining knowledge of this research area. In this work, the blockchain scalability issues are discussed in Section V. In addition to this, a detailed survey of scalability solutions is also presented in Section VI. Figures 1 and 2 depict the road map of our survey and core components of the blockchain technology, respectively. The contributions of our work are as follows.

- Through a thorough examination of numerous sectors, this study offers a methodical literature assessment of scalability issues in the blockchain and explores potential solutions based on data sharing, smart contracts, consensus methods, and scalable IoT devices.
- This paper also provides an overview of similar survey articles, offering a comparative analysis among them. Additionally, recency score for each article is also computed.
- A critical analysis is presented and important findings are highlighted.
- The future open research challenges and applications of blockchain are discussed in detail.

The rest of the paper is organized as follows. Section II contains similar work. In this section, survey papers of blockchain are discussed and their work is analyzed. In Section III, the preliminaries of blockchain are discussed. Section IV highlights applications of blockchain. Moreover, in Section V, scalability issues are highlighted in the existing literature. Section VI contains a detailed discussion on solutions to scalability issues proposed in the literature. Section VII contains a critical analysis of the paper and highlights some important issues. Future challenges are discussed in Section VIII. Finally, the paper is concluded in Section IX.

TABLE 1. Criteria for calculating recency score.

Percentage (%)	Weight	Recency score
0-10	0.1	*
11-20	0.2	
21-30	0.3	**
31-40	0.4	
41-50	0.5	***
51-60	0.6	
61-70	0.7	****
71-80	0.8	
81-90	0.9	*****
91-100	1.0	

II. RELATED WORK

In this section, the existing survey papers in the blockchain domain are discussed. A comparative study of the surveys is provided based on the contributions and completeness. Moreover, a recency score is computed for each paper to check its ability to provide information of recent advancement in blockchain domain.

The criteria used to determine the recency score are outlined in Table 1. Multiplying the sum of all recent papers by one hundred and then dividing by the total number of papers yields the recency percentage. We define "recent" as the year a work is published and its previous three years.

TABLE 2. Summary of related work.

Survey	Addressed problem	Contributions	Future challenges
Challenges and opportunities of blockchain [14]	Blockchain configuration, storage computation and degree of decentralization are discussed	Analysis on blockchain contribution is discussed with significance	Data storage capacity is a future challenge for dense networks
Blockchain security and challenges [15]	Majority attack is identified as a major threat	Advantages and disadvantages of four types of blockchain are discussed	Not discussed
Survey on consensus mechanisms and mining strategies [16]	Survey on consensus mechanism is performed	Both incentive and distributed consensus mechanisms are discussed	Major issues of designing phase are discussed in detail
Blockchain technologies and opportunities [17]	Blockchain in terms of technological and application perspective is discussed	Blockchain taxonomy and consensus algorithms are discussed	Limitations in smart contract languages are discussed
Blockchain and IoT integration [18]	Blockchain features and their resource consumption for IoT are discussed	Device manipulation and data management are discussed	Protection against innovative attacks are still need to be settled
Blockchain and its applications [19]	Comparison of consensus mechanism and their usability is discussed	Blockchain applications in terms of business, finance, etc., are presented	Not discussed
Comparative study of blockchain [20]	Blockchain and its impact on emerging domain are discussed	From literature, it is highlighted that blockchain's second phase is revolutionizing the IoT field	Lack of security and privacy are discussed as future challenges
Open issues of blockchain [21]	Six important layers are presented along with their components	Some major features of blockchain are discussed with classification	Issues and challenges of blockchain are discussed by considering existing system
A survey on blockchain in industries [22]	Security and privacy issues in industries are discussed	Using blockchain, many industrial issues are resolved	Scalability, security and privacy issues are considered as future challenges
Blockchain and AI survey [23]	Learning capabilities in blockchain systems are discussed	Brief literature survey is presented and its outcomes are analyzed	Research challenges in terms of blockchain and AI are presented
Blockchain-based identity management systems [24]	Lack of data security in traditional IDMS for IoT devices is discussed	Using blockchain, major issues are solved, such as security, privacy, etc.	IDMS future challenges are discussed in terms of access control
Blockchain-based applications [25]	A comprehensive study of blockchain in various fields is presented	Analysis is performed while considering two different parameters	Suitability, latency and data management are the future challenges
Comprehensive survey of blockchain [26]	Challenges of consensus algorithms and P2P network are discussed	Architecture is designed for data, network, consensus and application layer	Future challenges about privacy and reputation are mentioned
Blockchain technology in smart city [27]	Building a smart city without third party involvement is discussed	Blockchain-based smart city applications are presented	Scalability is the future challenge in blockchain-based smart city
A comprehensive survey on blockchain applications [28]	Data management and monetization of IoT industry are discussed	IPFS and BigchainDB are considered as solutions of scalability	Suitability and scalability are considered as future challenge
A comprehensive analysis of blockchain [29]	Security problems in IoT are discussed	Enhanced consensus mechanism increases throughput of the system	Consensus mechanisms must be improved
Performance benchmarking and optimization for blockchain systems [30]	Low-performance in blockchain is discussed	Consortium blockchain is suitable for implementation, anonymity and low scalability are highlighted as issues	Not discussed
A survey on blockchain-based Internet service architecture [31]	Analysis is performed on features of traditional Internet services	This survey addresses blockchain integration factors to secure Internet services	Not discussed
The blockchain state-of-the-art techniques and research challenges [32]	Survey of blockchain is presented	Blockchain challenges and related impact on blockchain-based system	Resource sharding and privacy protection are considered as future challenges
Blockchain in industry and academia system [33]	Blockchain considers security, efficiency and scalability as key parameters	Flexibility and scalability of blockchain are discussed	Future research directions are given for highly dynamic and complex systems
An overview on smart contracts is provided [34]	Challanges related to smart contracts are highlighted	Important research advances and challenges are identified along with the applications	Future challenges related to smart contracts are discussed in detail
A survey on blockchain systems [35]	Security issues related to blockchain systems are discussed	Summarize practical academic achievements for enhancing the security of blockchain along with real attacks on systems	Privacy leakage and mining process are highlighted as future research directions

TABLE 2. *(Continued.)* **Summary of related work.**

A survey on IoT and blockchain [36]	Securing IoT in distributed blockchain	Detailed discussion on security issues, their cause and state of the art taxonomy	System scalability, storage, cost, etc., are identified as research challenges
A survey on blockchain applications, challenges and opportunities [37]	Challenges and trade-offs in blockchain are discussed	A detailed comparison of possibilities and benefits with its challenges	Standardization, asset protection, big data, etc., are discussed
Information system management [46]	Addressed all issues in the information systems management area	Blockchain-based information system analysis	Global information systems, Multi level information security protection, etc., are highlighted as future directions
A survey on blockchain security [39]	Analysis of blockchain evolution, architecture and security	Detailed analysis of blockchain architectures and evolution	Privacy, security and accountability are discussed
A survey on blockchain storage optimization [40]	Storage solutions for blockchain systems	In-depth analysis of storage optimization	Hybrid optimization, generality of content, lack of holistic approaches, etc.
A survey on blockchain and machine learning [41]	Discussion on how blockchain is integrated with machine learning	Researches advances in machine learning based blockchain systems	security issues, strategic planning, information processing, and scalable workflows are highlighted
A survey on blockchain technology and privacy regulation [42]	Reconcile blockchain with privacy rules for secure, privacy-aware digital framework	Identified friction between blockchain and general data protection regulation	Challenges related to blockchain integrated general data protection regulation are discussed

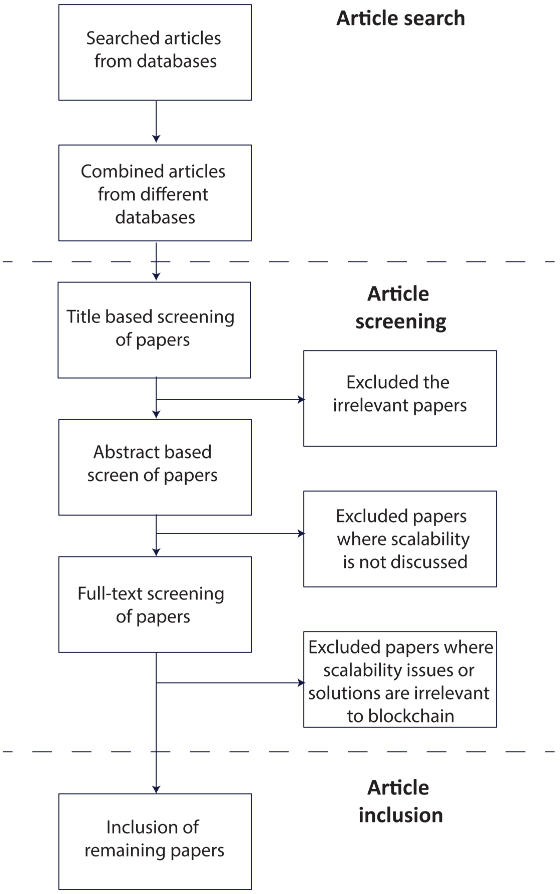

Searched articles from databases
Article search
Combined articles from different databases
Title based screening of papers
Article screening
Excluded the irrelevant papers
Abstract based screen of papers
Excluded papers where scalability is not discussed
Full-text screening of papers
Excluded papers where scalability issues or solutions are irrelevant to blockchain
Inclusion of remaining papers
Article inclusion

FIGURE 3. **Flow chart of papers selection phases.**

We allocated stars to indicate the proportion of recently published papers. Five stars are awarded to a paper if its allocated weight exceeds 0.9; if its assigned weight is less than or equal to 0.1, the document receives only one star. The number of stars in a survey indicates how frequently current works are cited. Moreover, a higher recency score increases the worth of a survey by indicating that the content discussed in a survey paper is not outdated. For example, [27] is published in 2019. The total number of recent papers cited in this survey (papers published during 2016-2019) is 219 and the total number of cited papers is 288. The ratio of recent papers and total papers cited in the survey implies that the content of the paper is not outdated. To calculate the recency score, we will multiply 219 with 100 and divide the resultant value by 288. In this way, the percentage of recent papers is obtained, which is then used to assign stars to a survey paper. In the case of [27], 76% recent papers are cited. So, according to Table 1, its weight is 0.8 and the corresponding recency score is ****, which is a high recency score. Similarly, recency scores of the rest of the papers are calculated.

The review of previous research is shown in Table 2, while Table 3 provides a summary of the comparative analysis of various survey studies. In [24], [25], [26], and [28], surveys on IoT integrated with blockchain are presented. The authors also described how IoT devices are integrated into different domains. The main issues and future challenges are privacy, security and storage. The survey presented in [28] is better than other surveys because it discusses the integration of IoT in several domains concerning storage and also enlightens the different external storage systems used to solve the issues of scalability. In [27], authors discuss attacks on blockchain based IoT solutions. It is a comprehensive survey; however, taxonomy of storage is missing. In [29], a comprehensive analysis is presented for

TABLE 3. Comparative analysis of related work.

Domain	Critical analysis	Opportunities	Future challenges	Recency score	Significance
Not domain specific [14]	✗	✓	✓	***	A survey of blockchain classification, opportunities and its challenges
Not domain specific [15]	✗	✗	✗	****	A brief survey of blockchain security issues and challenges
Not domain specific [16]	✗	✗	✓	***	Detailed survey of consensus mechanisms and mining management in blockchain
Not domain specific [17]	✗	✓	✓	***	A survey of blockchain challenges and opportunities
IoT [18]	✗	✗	✓	***	A survey of blockchain and its integration in IoT enabled devices
Not domain specific [19]	✗	✓	✗	****	A brief survey of blockchain and its application in several fields
Not domain specific [20]	✗	✓	✓	****	The review of current research topics in blockchain and its issues
Not domain specific [21]	✗	✓	✓	****	The survey of blockchain functions, applications and open issues
AI [22]	✓	✓	✓	***	A brief review of blockchain and open research challenges in AI
Industries [23]	✗	✓	✓	***	A survey of blockchain technology's applications in industry
IoT [24]	✗	✗	✓	****	Identify digital identity management for IoT in detail
Not domain specific [25]	✗	✗	✓	*****	A review on blockchain-based applications
IoT [26]	✓	✗	✓	***	A survey on blockchain classification and its issues
Smart cities [27]	✓	✓	✓	****	A survey on blockchain's open challenges in different domains of smart cities
IoT [28]	✓	✓	✓	****	A survey on blockchain challenges and opportunities for decentralization of IoT
IoT [29]	✓	✓	✓	***	A survey on security and research challenges in IoT
Blockchain systems [30]	✓	✗	✗	*****	Analysis is performed on the basis of consensus mechanism and types of blockchain
Internet [31]	✓	✗	✗	***	Challenges for integration of blockchain and Internet services are surveyed
Not domain specific [32]	✓	✓	✓	****	Reviewing the current state of blockchain technology and its potential future applications across a range of industries
IoT [33]	✓	✗	✓	***	A survey on solutions for scalability and privacy in IoT
Not domain specific [34]	✗	✓	✓	****	A survey on smart contracts, their challenges and platforms
Not domain specific [35]	✓	✗	✓	****	A survey on security of blockchain with future challenges

TABLE 3. *(Continued.)* **Comparative analysis of related work.**

IoT [36]	✓	✓	✓	***	A survey on secured IoT in distributed blockchain
Not domain specific [37]	✓	✓	✓	****	Challenges, opportunities and applications of blockchain are discussed
Information system management [38]	✗	✓	✓	****	First blockchain-based information system analysis
Not domain specific [39]	✓	✓	✓	****	A survey on blockchain architecture, frameworks and security issues
Not domain specific [40]	✗	✗	✓	***	A survey on storage optimization
Not domain specific [41]	✗	✓	✓	*****	A survey on blockchain and machine learning techniques
Not domain specific [42]	✓	✗	✓	*****	A survey on blockchain integrated general data protection regulation
Our survey is not domain specific	✓	✓	✓	*****	**A survey on blockchain scalability issues and their possible solutions**

IoT systems considering the blockchain-based applications. The network of blockchain is divided into layers, which are discussed in detail. In this survey, a comprehensive analysis of the blockchain and its impact on IoT systems are discussed. The authors provide a solution by improving the consensus protocol for the IoT environment. In [30], the survey is based on the blockchain types. A consortium blockchain is employed for the purpose of achieving consensus among participants. Nevertheless, it is susceptible to encountering scalability challenges. The paper [31] provides a thorough examination of the incorporation of blockchain technology into conventional Internet services. Future challenges, such as achieving consensus performance and addressing data storage limitations, have been identified. The article referenced as [32] examines many concerns regarding the blockchain, including limitations in data storage and security-related challenges. The scalability challenges are addressed in [33] by the utilization of a software-defined network and blockchain technology. The various types of blockchain are also explored for their applicability to IoT applications. The surveys mentioned in [34], [35], [36] are also commendable. The recency score of both [34], [35] is commendable (four stars); nonetheless, the former lacks in-depth research and the latter fails to address the prospects associated with blockchain. In addition, [36] provides comprehensive coverage of the topic; nonetheless, it has a poor recency score. The articles [30], [31], [32] provide a thorough analysis of the scalability challenges and propose effective solutions. Regarding the recency score, citations [22], [23], [24], [25] rank highest compared to other sources. In addition, we have conducted a comparative analysis between our survey and the aforementioned survey publications. The recency score of our survey has received a rating of 5 stars. Additionally, it provides an examination of blockchain applications, potential future challenges, and a thorough analysis.

In the literature, some survey papers are exclusively focused on blockchain scalability. Authors in [43], [44] discuss the scalability solutions for blockchain implementation. However, [43] is dedicated to the scalability challenges and their solutions in the health care domain only. The solutions discussed in this paper revolve around storage optimization and redesigning of the blockchain. Authors in [44] discuss the scalability solutions. However, the solutions are not discussed with respect to any application domain and also a comparative study of discussed solutions is missing. In [44], the discussed scalability issues and their solutions are summarized at the end; however, the discussion in these surveys is on a very abstract level. Moreover, the authors present the survey of blockchain scalability [45], [46], [47]. These papers contain a comprehensive discussion on blockchain scalability issue. However, the paper on blockchain scalability survey [45], delves into chain partitioning-based scalability, DAGs-based scalability, and horizontal scalability through sharding and authors in [46] focus only on public blockchain type. Additionally, the survey [47] lacks comparative analysis of the similar blockchain scalability solutions. Hence, to provide a comprehensive survey on blockchain scalability issues and solutions, our paper expands the discussion to encompass a broader spectrum of scalability considerations. In contrast to existing surveys, our paper addresses scalability concerns not only in terms of chain partitioning and public blockchain but also explores aspects such as consensus mechanisms, transaction throughput, and network efficiency, accommodating all blockchain types. Moreover, a comparative analysis of similar solutions is also presented. By examining scalability through multiple lenses, including partitioning strategies and consensus protocols, our paper provides a more comprehensive understanding of the challenges and potential solutions in achieving scalable blockchain systems.

A flow chart of papers selection phases is depicted in Figure 3. The first phase is article search phase, where research papers from different databases are searched and combined at one place. In the second phase, the screening of papers is carried out. Firstly, the papers are analyzed based on their title and irrelevant papers are filtered out. Secondly, the selection of papers is done on the basis of their abstract. Lastly, the papers are selected by full-text screening. At this stage, the information related to scalability is extracted from the papers and only those papers are selected for the survey where scalability issues and solutions are discussed with respect to blockchain.

III. PRELIMINARIES

The blockchain consists of a list of records, which are stored in blocks. The blocks are chained together using hash values. For the purpose of creating a chain, each block has its own unique hash address and it also keeps the hash of the previous block. A blockchain is a decentralized distributed digital ledger and every node on the network has its copy. Hence, it is immutable and a promising choice to store records related to some valuable assets. There are three types of blockchain: public, private and consortium. Public blockchain is an open-source and permissionless distributed ledger. Any node can join it and become its part. On the contrary, private blockchain is a permissioned blockchain, which is usually created for an organization. Only a limited number of nodes have permission to join the network. Access control levels are also defined to keep sensitive data secure. Moreover, consortium blockchain is similar to private blockchain but differs in terms of levels of permissions. It is established between multiple organizations, which intend to share data. A blockchain has the following features.

A. NODES

One component of a network is the node. A desktop, laptop, mobile phone, or wireless router might all fit the bill. There are three distinct types of nodes, and they all play a crucial part in the blockchain. Some examples of nodes are as follows [48].

1) FULL NODES

It is a very important type of nodes. When full nodes are connected to a blockchain network, they download the whole copy of the blockchain. They are responsible for copying and distributing all the blocks in a blockchain. These nodes also play the role of validators of transactions. Note that, the validation of transactions and mining are not the same. Full nodes have access to the entire blockchain. They can track the records from the last block to the genesis block (which is the first block of the blockchain). So, these nodes ensure the immutability of the blockchain network. To create new blocks and add them to the blockchain, full nodes engage in mining. To create a new block, miners sort the legitimate transactions in a certain order and solve a complex mathematical puzzle. A block has a predefined size and it can contain a limited number of transactions. Full nodes have high computational power to compete with their fellow nodes in solving puzzles.

2) LIGHT NODES

As the name shows, these nodes are not computationally very powerful. They get registered on the network and download a subpart of the blockchain. They download only headers of all blocks and maintain a summary of the blockchain. These nodes do not take part in the validation or mining process.

B. SMART CONTRACTS

An executable program that regulates financial dealings between multiple nodes is called a smart contract. Smart contracts are quite similar to regular contracts; the main distinction is that smart contracts are executed by code, whereas regular contracts are implemented by courts or laws. Solidity is the commonly used language to write smart contracts [49]. The smart contracts contain a series of events that can be executed in a specific order according to certain criteria and conditions. There is no way to change or edit a smart contract once it's live on the network. It lays out all the requirements that two nodes must follow in order to make a transaction. Whenever a smart contract is deployed in a blockchain, it is assigned a hash address, which becomes its identity. A node accesses a smart contract using its hash value. A blockchain network can have multiple smart contracts and each one of them can have the same or different functionalities depending on the needs of users. A smart contract has the following highlighting features.

- It has to be accurate because all the transactions strictly follow all the rules specified in it. So, the accuracy depends on how well the rules are coded in a smart contract.
- It automates the whole process of transactions, so, there are no unnecessary delays in decision making and validating a request.
- It is embedded in the blockchain and every node has its hash address, so, there is no chance of its lostness.
- As it processes all transactions between nodes directly, it cuts out the middleman, which means it is cheap.
- The elimination of a central party removes the central control and monopoly of a single entity while the network is managed by several nodes of the network.

C. CONSENSUS ALGORITHMS

The consensus is an important feature of the blockchain. During this process, all nodes of a blockchain network agree on a common point, this point can be the current state of the blockchain or its blocks. As there is no central authority to validate the transactions, so, nodes verify the transaction and keep the blockchain immutable. In case of an attack, the attacker who wants to edit a block, has to modify all blocks that come before it on 51% of the nodes in the network within a specific interval. In case of failure, the altered chains will be detected and hacked nodes will revert their chains to their original state. This change is identified by the consensus of nodes. Thus, modifying existing blockchain is computationally very expensive for an attacker and also not practical. The consensus method further guarantees that each newly added block to the blockchain is distinct and contains only legitimate transactions. Here are some examples of consensus algorithms [50].

1) PROOF OF WORK (POW)

In terms of consensus mechanisms, this is by far the most prevalent. All of the participating miners work together to solve a difficult mathematical puzzle and verify the transactions that will be included in the next block. The first miner to solve the puzzle will be crowned as winner and given rewards [50]. The rest of the miners stop the mining process, update the transactions from transactions' pool and restart the mining procedure again. Each time a new block is generated, the transaction pool is updated and transactions that have been added to the block are eliminated. Miners now select a new set of transactions and start mining again. This algorithm is computationally very expensive and a lot of power is wasted because only one miner is declared winner and processing power of the rest of the nodes is wasted because they again start from the scratch. The selection of a transaction from updated transactions' pool is important because two miners might select the same transactions and one of them may succeed in generating a new block and if the second node does not update its transactions then there is a chance that the same transactions will be added to the second block.

2) PROOF OF STAKE (POS)

It is a popular consensus mechanism after PoW where each miner puts some amount of cryptocurrency on stake to become the validator of the next block. The algorithm then selects the next validator from the group of candidates. There are two ways of selection: age-based selection and random selection. In the former, a node is selected based on the time duration it has been a minor. The oldest node becomes the new validator. In the second selection process, a validator is chosen randomly on the bases of its stake value and its hash value [50]. If a node misbehaves or performs a suspicious activity, it is excluded from the group of miner candidates while keeping its stakes.

3) PROOF OF AUTHORITY (POA)

In this algorithm, a reputation value is attached to each node, which depends on its contribution to mining new blocks [50]. Each time a node generates a new valid block, it is awarded an incentive value, which also increases its reputation value. In case a node misbehaves or gets involved in a suspicious activity, it gets a negative reputation. A node with a negative reputation cannot take part in the mining process.

4) PROOF OF BURN

This consensus mechanism is similar to the PoS, where a miner puts some amount of its cryptocurrency on stake [50]. The only difference is that here miners burn their coins or cryptocurrency to be a part of the mining process. By burning coins, it means that they send it to some unreachable account using a hash value. In this way, they face a small loss for a long term profit. Miners are selected randomly and a miner who burns more coins has a high probability of being selected.

5) PROOF OF TIME

In this type of consensus algorithm, fair selection criteria of the mining node is implemented [50]. Here, each node is assigned a waiting time and a node who finishes its waiting time is selected as a miner. It is mostly used in private or consortium blockchains, where the number of nodes is limited and each node needs permission before accessing the network.

6) PROOF OF CAPACITY

This is a type of consensus algorithm, where miner nodes are selected based on the space available on their hard disks. Nodes put their hard disks on stake, larger the hard disk space a node will have, more chances of its selection as a miner will be [50].

7) BYZANTINE FAULT TOLERANCE (BFT)

As its name shows, this algorithm is designed for fault tolerance. In a BFT-based blockchain network, when some nodes misbehave or send the incorrect message, the network still reaches consensus and malicious nodes do not affect the working of the overall network [50]. The missing or incorrect messages are discarded and voted as the false messages. It prevents the network from possible failures and makes decisions according to the majority nodes. This algorithm is fault-tolerant, consumes less energy, and every node who participates in the network and contributes to reaching consensus gets reward according to its contributions.

D. TAXONOMY

Figure 4 shows the taxonomy of blockchain with its features and important components. In this paper, we have categorized the blockchain scalability solutions into four categories: off-chain, smart contract based, consensus mechanism based and directed acyclic graph (DAG) based solutions. These types are discussed in Section VI in detail.

IV. APPLICATIONS OF BLOCKCHAIN

Bitcoin was the first application of the blockchain. It is gaining popularity with each passing day. Researchers are actively working on it and proposing solutions for several problems in almost every field of life. In this section,

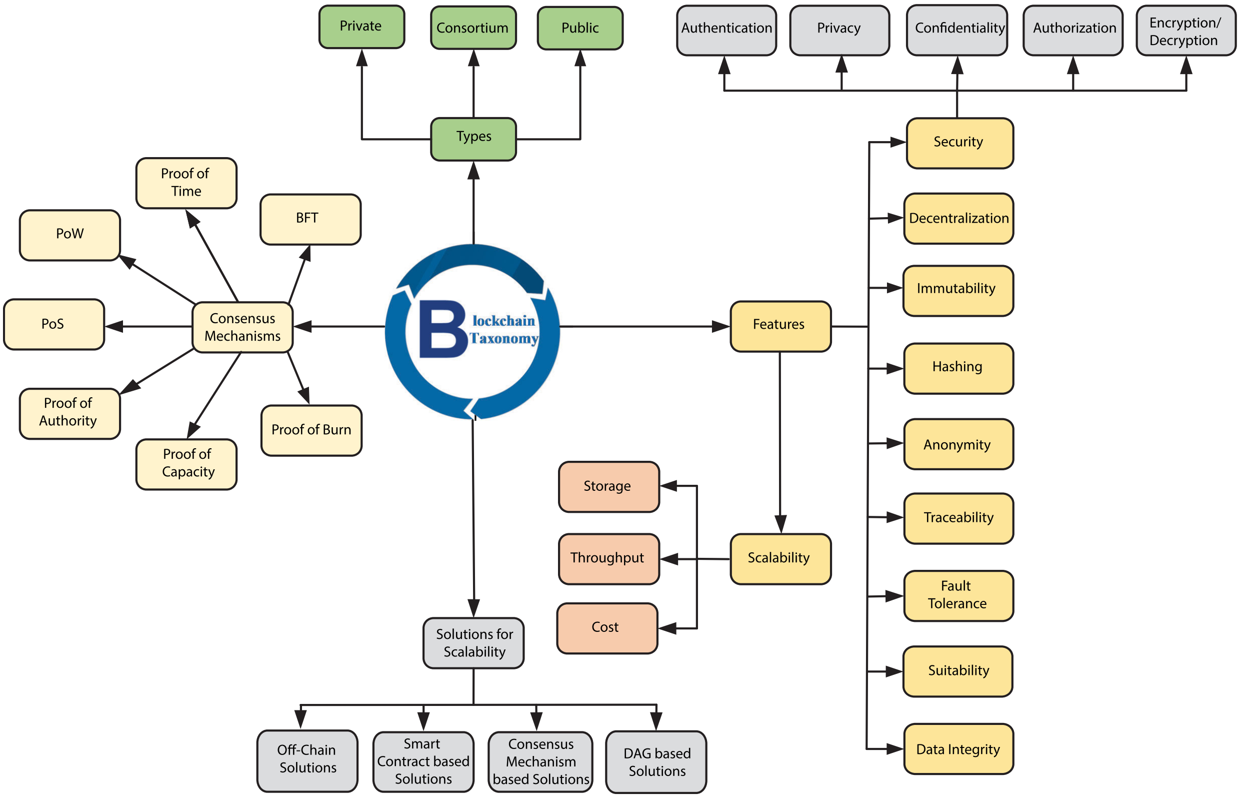


FIGURE 4. Taxonomy of blockchain and scalability, its features and important components.

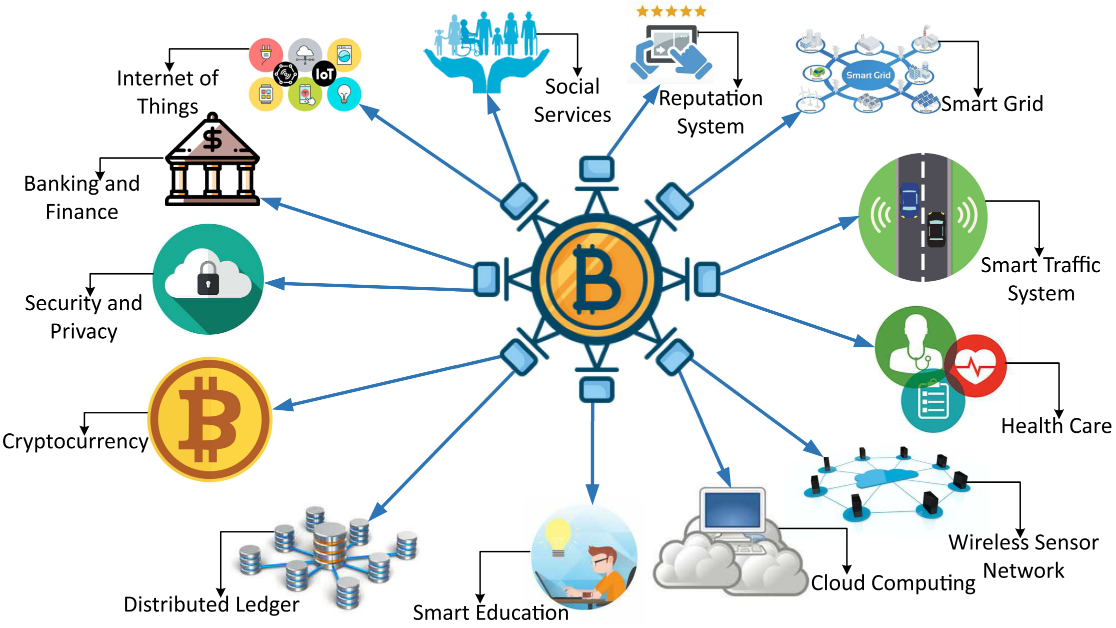


FIGURE 5. Applications of blockchain.

important applications of blockchain are discussed in detail. The applications are shown in Figure 5.

- The reputation of a person or company is of high importance. It is a way of evaluation to know how trustworthy someone is. In recent years, a high number of reputation falsification cases have been encountered, both on individual and service providers' level, such as web community and academic institutes. The issue can be solved by keeping individuals' records and registered customers' information of a service provider on the blockchain [51], [52], [53].

- Increased amount of renewable energy generation requires efficient market mechanisms for energy trading. A new market platform is required to enable the electricity buyers and sellers to exchange energy independently without the involvement of a third entity. The blockchain has evolved as a promising solution to this problem [54], [55], [56]. It enables the electricity buyers and sellers to efficiently trade energy directly.
- Self-driving vehicles are gaining the attention of researchers. It is a hot topic nowadays in both industry and academia. An autonomous vehicle is composed of several subsystems, which are prone to attacks. To avoid these attacks, these subsystems' firmware needs to be updated to the latest version. This enables the manufacturers to focus on new inventions and remove bugs from existing systems. The blockchain technology can be used to manage these updates and keep track of all the updates according to their released date. All the autonomous vehicle manufacturers can become part of the blockchain and store firmware updates in a distributed environment [57], [58].
- Application of the blockchain in health-care seems to be beneficial [59], [60], [61]. It can be used to maintain the patients' health records and share them across authorized hospitals, where patients visit. Medicine companies can get permission from patients to access their disease history by providing them incentives, in this way, these companies would be able to extract useful patterns from patients' historical records and improve their medical formula.
- The utilization of blockchain technology has the potential to improve the dependability and efficiency of a wireless sensor network [62], [63], [64]. It can identify the bad actors in a network that are causing disruptions and data breaches. By monitoring the actions of every sensor in the network, it is possible to root out the selfish nodes. Tracing the behavior of problematic nodes can also be done.
- Application of blockchain in cloud computing grabbed the attention of enterprises, which require security, reliability, accountability, auditability and compliance of their data [65], [66], [67]. In such cloud systems, it is possible to keep track of every action, e.g., sources of data access, alteration, processing, storage and usage. The blockchain provides complete traceability of data on the cloud and in case of any unauthorized action, the responsible entity can be identified.
- The implementation of blockchain in the education sector is also very beneficial. The records of students related to their academic achievements, important notes and titles are stored in the blockchain. In case of some accidental damage or any other unpleasant event, educational institutions can access this information from the blockchain. Moreover, tampered documents can also be detected [68], [69].
- The blockchain implementation for data storage on the cloud makes it faster. A file is sharded into small chunks, which are encrypted and uploaded on the blockchain. As these chunks are stored in a distributed manner, so, they can be accessed in a parallel manner [70], [71].
- The blockchain-based decentralized digital currencies, such as Bitcoin, are evolving as a potential alternative to the traditional banking system. In [72], Peters et al. have discussed its potential of deranging the traditional banking system. It can resolve the financial settlements between two parties, in this way, it reduces the cost and risks of involving a third party.
- Networks are prone to malicious nodes and attackers, which need to be identified. The blockchain technology plays a very important role in the identification of malicious nodes and attackers [73], [74]. Public key infrastructures can be made using the blockchain technology as it is a decentralized technology and a common issue of central point of failure of public key infrastructure can be tackled efficiently. Also, some social websites are extracting the personal data of their users and storing them on clouds. This data is prone to malicious attacks. Blockchain can also preserve sensitive data while ensuring its privacy.
- IoT is the promising technology for integrating smart devices with the Internet to facilitate the users. The blockchain has improved the IoT sector in several ways. The privacy of IoT enabled devices is enhanced using the blockchain and it also allows the devices to communicate on a network without revealing their identities [75], [76]. Moreover, sensors' data can be obtained anonymously in exchange for digital currency and without any involvement of a third party.
- The blockchain also provides potential solutions for insurance as well [77]. The data related to travel, health, crops, properties and causality insurance of an individual can be integrated. This integrated data then plays a vital role in fraud detection and speeding up the insurance claim process.
- Smart cities are using blockchain to enhance the standard of living and improve the privacy and integrity of data [78]. In the future, it can be used to create a virtual source for every business for trading securely and efficiently. An employment registry can be maintained to store the employment history of all employees, which can be accessed by authorized entities when required. Moreover, transparent trading between buyers and sellers and direct fund transfer between businessmen are also possible. Additionally, fraudulent activities can be detected easily.
- Another application of the blockchain is voting. It can provide a transparent platform for elections without any

chance of election rigging. It has been used by the Danish political party for fair elections [79]. An on-line voting platform has also been introduced, which enables secure on-line elections [80].

Blockchain has significant real-world implications across several domains; however, limited scalability of blockchain can hinder the ability of blockchain based systems. For instance, scalability issue can affect energy trading by limiting the throughput of energy transactions and potentially affecting the peer to peer energy transactions in real time. In addition, the performance of wireless sensor networks depends on throughput and efficiency of data transmission and validation, which is affected by blockchain scalability issue. Moreover, blockchain scalability challenges also limit the real-time data processing and communication between self driving vehicles, which can potentially affect the safety and efficiency of vehicles. In healthcare, voting, insurance and education sectors, data storage, access, sharing and processing require both speed and efficiency. However, a blockchain based system has a limited ability to support large volume of data; hence, data sharing on a large scale, scalability of decentralized learning management systems and collaboration among healthcare providers, patients and patients becomes challenging. Additionally, it becomes difficult to handle large volume of insurance transactions and support scalable insurance services. Blockchain scalability issue also affects the cloud computing application because of the low storage and computing networks because cloud computing involves large workloads handling in real time. Moreover, blockchain scalability issue affects the speed and efficiency of data transmission, validation and processing in decentralized IoT environment and smart cities applications. Owing to the aforementioned challenges, solutions to blockchain scalability issues become vital.

V. COMPREHENSIVE SURVEY OF SCALABILITY ISSUES

Scalability is a major concern of blockchain technology. A system is considered scalable if it has the ability to manage increasing loads without compromising the performance. Scalability is a key factor in determining a system's resilience and flexibility. A system is considered scalable when it continues to function well with an increasing number of inputs while maintaining the performance with a decreasing number of inputs [81]. In blockchain prospective, scalability can be defined as how well blockchain network can expand to accommodate more users, transactions or data without experiencing degradation or congestion in speed. In this paper, the existing blockchain based systems are evaluated for scalability issues with respect to three important perspectives of scalability: throughput, storage, and cost.

Throughput of a blockchain system is considered in terms of transactions, which are added in blocks per second. This transactional throughput is fully dependent on the type of consensus algorithm used, which specifies how blockchain nodes make consensus to ensure the validity of the transaction and confidentiality of the transactional data [82]. In the blockchain, scalability also depends on the data storage capability of a system. As the size of a blockchain increases daily, there is a need for an efficient data storage mechanism. Furthermore, the execution and transaction costs are measured in terms of gas consumption and type of a blockchain. If there is a linear increase in gas consumption, while adding more inputs, it shows that the system is scalable. Whereas, the increase in a network size requires high computational resources, which ultimately increase the network cost. Various characteristics and features of the blockchain used in existing studies are shown in Tables 4 and 5.

In this section, the scalability issues in existing blockchain systems are highlighted. The authors in [81], [82], [83] propose a blockchain-based system for crowdsensing networks. These systems are implemented on the public blockchain and are made secure using encryptions methods. In [81], [83], PoW consensus algorithm is used while [82] uses credit-based verifier. The latter is better than the former as it is computationally less expensive and does not affect the scalability of the network. Moreover, the re-identification attacks handling method in [81] increases the computational overhead because agents maintain two blockchains; however, the positive aspect is that the rewards of nodes are computed off the chain. In [82], a double consensus method affects the scalability and rewards for nodes are also computed on the chain. The proposed system in [83] is based on task matching between nodes. The number of requests is always higher than the number of nodes. It causes network congestion and may affect the throughput and latency of the network.

In [84], [85], [86], the blockchain-based systems for IoT are proposed. The authors in [84] provide data integrity on a public blockchain system. In [85], a personal data sharing system is proposed using private blockchain, whereas [86] provides secure transactions between nodes using consortium blockchain. All three systems achieve security using cryptographic techniques. For consensus, instead of using commonly used PoW algorithm, round-robin, KAFKA and lightweight consensus algorithms are used in [84], [85], [86], respectively. These algorithms are computationally less expensive and good for the scalability of a system. From careful observation, it is noticed that in [84], the computational overhead increases in the system when the nodes are increased because of the verification of the nodes. It can be reduced by adding more resources to the system; however, it increases the system cost and adding more cooperative nodes in the system also makes the system vulnerable to attacks. In [85], the data is stored off the chain. Hence, the issues of latency arise when nodes try to access data. Due to the double verification on both local and global blockchains, the throughput of the system also decreases.

A malicious node detection method for blockchain-based WSNs is proposed in [87]. For consensus, the PoW algorithm is used on the public blockchain. For malicious node detection, packet forwarding rate, response time and delay in transmission of each node are monitored. So,

TABLE 4. Blockchain characteristics used in the existing systems.

Scope	Blockchain Type	Language	Immutability	Encryption Scheme	Security
Location-based privacy preserving [81]	Public and private	Not mentioned	Yes	Encryption used for privacy preserving	No privacy leakage problem
Crowdsensing quality control [82]	Public	Solidity	Quality control mechanism	Public key encryption	Quality control and grading evaluation
Crowdsensing and task matching [83]	Public	Solidity	Yes	Public key encryption	Data confidentiality and anonymity
IoT data integrity [84]	Public	Solidity	Yes	Asymmetric public key encryption	Majority-based verification
Personal data sharing and tracking [85]	Private	Maltab	Unique address immutable system	Not mentioned	Secure data sharing mechanism
Secure transactions in IoT [86]	Consortium	Go	Yes	Encryption key pairs	Secured using encryption
Malicious node detection in WSNs [87]	Public	Solidity	Yes, voted consensus are recorded	Public key cryptosystem and elliptic curve digital signature algorithm	In terms of malicious node detection
Trading [88]	Public	Solidity	Achieved through permanent log file of transactions	Not mentioned	Not mentioned
Trading [89]	Private	Solidity	Maintain log of transactions	Not mentioned	Not mentioned
Trading [90]	Private	C and C#	Secure log transactions	Not mentioned	Secure comunication between grid and consumers
Trading [91]	Consortium	C	Secure log transactions	Not mentioned	Data is secured using blockchain
Trading [92]	Consortium	C and C#	Transactions are non modifiable	Not mentioned	Data is secured using blockchain
Medical health data storage [93]	Consortium	Solidity	Secure log transactions	Not mentioned	Not mentioned
Medical health data storage [94]	Distributed clustered network	Solidity	Achieved through data logs	SKAESP	Through encryption
Medical health data storage [95]	Private	Go	Achieved through data logs	Not mentioned	Data is secured using blockchain
IoT [96]	Consortium	Solidity	Secure log transactions	Eliptic curve digital signature	Data is secured using encryption
IoT [97]	Public	Solidity	Achieved through data logs	Advanced encryption standard algorithm	Data is secured using encryption

when the number of nodes is increased, this monitoring mechanism becomes complex and deploying more nodes for monitoring and mining purposes makes the system vulnerable and increases the network cost as these nodes should be computationally powerful to execute PoW consensus.

The blockchain-based energy trading systems are proposed in [88], [89], [90], [91], [92]. In [90], [92], practical BFT (PBFT) algorithm is used for consensus on private and consortium blockchains, respectively. In [88], [89], [91], the PoW algorithm is used, which is implemented on public, private and consortium blockchains, respectively. For energy trading, electric vehicles (EVs) are also considered as network nodes in [88], [92] while in [89], [90], [91] energy trading only between smart meters and utilities is considered. In [88], a basic energy trading system is proposed and monetary transactions are performed on the chain, which affect the throughput of the system and increase the network latency. Only keeping the record of financial transactions on blockchain and rest of the data off the chain, can increase the scalability of the system as in [81]. Moreover, EVs are also considered as prosumers; however, they are not computationally powerful. In [89], the computational overhead increases because complex computations are performed in the smart contracts and PoW is used for consensus. Besides, the data acquired from smart devices is stored in blockchain. Moreover, nodes are categorized as full and half nodes. The full nodes still need to save a huge volume of data, which causes scalability issues when the network size is increased. In [90], as the bidding process and equilibrium state of nodes are controlled by smart contracts, so, increasing the network size can cause delays in the network. The scalability issues arise in [91] while increasing the number of nodes because the negotiation time between nodes depends on the number of nodes in a network. The range of EVs in [92] is limited

TABLE 5. Comparison between blockchain-based systems.

Hashing	Authentication	Gas Cost	Execution Time	Consensus Mechanism	Platform	User/Device Management
SHA 256 [81]	Anonymous authentication scheme	✗	✗	PoW	Not mentioned	Smart contracts
SHA 256 [82]	By consensus mechanisms	✗	✓	Credit-based verifier	Ethereum	Public key encryption
SHA 256 [83]	Authenticate task matching process	✓	✓	PoW	Ethereum	Smart contracts
SHA 256 [84]	Secret key authentication mechanism	✗	✗	Light weight consensus algorithm	Ethereum	Smart contracts
SHA 256 [85]	Through consensus mechanism	✗	✗	Round robin	MATLAB	Unique address
SHA 256 [86]	Local certification authority	✗	✓	KAFKA	Hyperledger fabric	Anchor peer
SHA 256 [87]	Smart contracts	✗	✗	PoW	Ethereum	Smart contracts
SHA-256 [88]	Not mentioned	✗	✗	PoW	Not mentioned	Smart contracts
Dagger-Hashimoto [89]	Block validation through authentic nodes	✗	✗	PoW	Ethereum	Smart contracts
SHA-256 [90]	Block validation through authentic nodes	✗	✗	PBFT	Hyperledger fabric	Smart contracts
SHA-256 [91]	Block validation through authentic nodes	✗	✗	PoW	JADE and MATLAB	Smart contracts
SHA-256 [92]	Block validation through authentic nodes	✗	✗	PBFT	Hyperledger fabric	Smart contracts
SHA-256 [93]	Not mentioned	✗	✗	Customized scheme	Ethereum, Remix	Smart contracts
SHA-256 [94]	Verification process	✗	✗	PoW	Ethereum	Smart contracts
Diffie-Hellmen [95]	Block validation through authentic nodes	✗	✗	PBFT	Ethereum	Smart contracts
SHA-256 [96]	Block validation through authentic nodes	✗	✗	PoC	Ethereum	Smart contracts
SHA-256 [97]	By attribute authorities	✓	✗	PoW	Ethereum	Smart contracts

to 2 km only. Adding more nodes means increasing the area, which requires a proper mechanism when EVs go out of the range of the other EVs, as in [88].

Authors in [93], [94], [95] propose blockchain-based systems for health care domain. In [93], consortium blockchain is used with the PoW consensus algorithm, whereas authors in [94], [95] use distributed clustered architecture and private blockchain along with PBFT and a novel consensus algorithm, respectively. In [93], the data is sent to smart contracts for analysis. Increasing the network nodes can cause congestion and latency issues. Moreover, any attack on electronic health record can result in loss of data as no backup of data is available; however, events' records are saved on blockchain and are secured. Similarly, due to the local data storage, the latency and throughput issues arise in [95]. In [94], the throughput of the system is affected due to the clustered architecture, which creates scalability issues for the system. It is overall a good system; however, data storage on multiple clouds increases the cost of the system. Hence, increasing the network size also increases its cost and creates scalability issues.

The access control mechanisms are proposed in [96], [97]. In [96], consortium blockchain is used with proof of concept (PoC) consensus algorithm. On the other hand, [97] uses public blockchain with the PoW consensus algorithm. In [96], instead of defining roles for different nodes, the attribute distribution method is used. All the information related to attributes of all devices and data access requests is stored in the blockchain. The IoT devices are resource constraint, so, the system can face scalability issues on increasing the network size. The authors in [97] propose a data-sharing system. For data encryption/decryption, files are downloaded and encrypted/decrypted. In this way the computational overhead of the network is reduced; however, it increases the latency and affects the throughput of the system. A summery of current systems' scope, components, and scalability is offered in Table 6. In addition, the data from Table 7 [98] compares several consensus procedures that are utilized often.

Considering the global success of fifth generation technology, the researchers are working on the development of the sixth generation (6G) in a full swing. However, security and scalability are the major concerns. The authors in [99] consider blockchain as a promising technology to solve the privacy and security issues. A blockchain radio access network (B-RAN) is proposed in [99] for blockchain based 6G network. In a similar study [100], a B-RAN is proposed for a mobile ad-hoc network. Unlike [99], the selfishness of nodes is tackled by keeping track of the collaborating nodes and reward is given to only the honest collaborating nodes. Moreover, an architecture and prototype are designed in [101] for B-RAN. The core aims of this study include security, privacy, efficiency and flexibility of the system during resource sharing. In [102], [103], authors propose B-RAN. However, like other blockchain systems, the above discussed B-RAN systems also face scalability issues. From a brief literature review of the existing systems, it is observed that there is a trade-off between system latency (an important feature of scalability) and security. Moreover, specially designed consensus algorithms are required to address the computational constraints of a blockchain system. During resource sharing and incentive provisioning, on-chain exchange of data or monetary incentives further increase the scalability issues.

VI. SCALABILITY SOLUTIONS FOR BLOCKCHAIN PROPOSED IN THE LITERATURE

In the literature, scalability issues of the blockchain have attained significant attention of researchers. Several methods have been proposed to overcome these issues, which are discussed in the following sub-sections.

A. OFF-CHAIN TRANSACTIONS FOR SCALABILITY

In this section, the off-chain transaction systems are discussed, which play an important role in making a blockchain-system scalable. In [104], it is stated that the scalability issue in blockchain arises due to its finite rate of transactions in an interval. Besides, keeping the record of all these transactions also requires additional storage capacity, which becomes an issue for the local user. In case of deploying the blockchain technology for credit cards, on-chain transactions will limit its scalability and keeping the record of such transactions (in case of one transaction per second) will require 20 GB of additional memory and in case of 500 transactions per second, the required storage capacity will increase up to 10 TB per year. To solve this issue, the authors suggest to keep the transactions, related to payments, off-chain. Once the smart contract is executed and complex issues between two parties are settled down, then payments are made off-chain using the network of payment of service providers.

Bitcoin is a popular application of the blockchain, which gained attention because monetary payments are made securely and in a decentralized manner. There is no overhead of involving a third-party and the amount is directly transferred from sender to receiver. As the number of Bitcoin users is increasing, the PoW consensus mechanism is consuming more time and limiting its performance. An off-chain transactions solution can be used to tackle this problem. The trusted execution environment (TEE) chain [105] is an off-chain solution for the scalability issue of blockchain. It asynchronously accesses the blockchain and handles the fund transactions between multiple parties efficiently and securely while achieving the scalability. The funds of the blockchain participants are managed by the TEE globally. A party having TEE runs the TEE chain locally. A two-way communication channel is established between two parties to transfer payments efficiently. To ensure the valid transactions of funds, multiple TEEs substantiate each other. They ensure that the TEEs and code running to deploy the rules of fund transfer on these TEEs are not fake. Intel SGX is used to validate the performance of the proposed system and it is stated that it has a throughput of 33000 transactions per second with only 0.1 seconds of latency.

Authors in [106] address the issue of secure and scalable data sharing in clinical decision making. It is stated that the conventional methods of the data sharing are not up to the mark to acquire sufficient data related to patients. Moreover, it becomes difficult to take important decisions related to patients' treatment because of the inadequate details of past treatments. A blockchain-based solution is proposed for this issue. The scalability issue of data sharing in the blockchain is still there because of its limited resources for data storage. The authors address this issue by proposing a blockchain-based architecture called a fast health care interoperability resources chain (FHIRChain). In this architecture, a peer to peer (P2P) information exchange protocol is used, which makes the shared data light weighted and increases the scalability of the system. Instead of original data, its hash along with the reference pointer is stored in a chain, which allows the system to accumulate more data.

Machine learning models and large scale computational models often use big data and experiments are performed for days and weeks to learn some useful patterns and deduce the useful results. Based on these results, several important strategies are designed and precautionary measures are taken to prevent some unpleasant events. For example, OpenMalaria is a computationally expensive simulation, which helps to understand how this disease spreads, what are the useful strategies to intervene and which precautionary measures should be taken [107]. To share such information, the companies should have trust in each other that the data being shared is correct and valid. In [107], a blockchain-based solution is provided to tackle this problem. The scalability issue of blockchain is also highlighted along with

TABLE 6. Comparison of scalability.

Scope	System components	Input/dataset scalability
Privacy, re-identification attacks [81]	No. of workers (10, 40, 70, 100, 130, 160)	No. of tasks (1-1000), range of MaxD (15km, 25km, 35km, 45km, 55km, 65km)
Quality of data [82]	No. of workers (0, 20, 40, 60, 80, 100)	No. of tasks (10, 30, 50, 70, 90, 110)
Privacy, identity anonymity, reliability of task [83]	No. of workers (10*3) ranging between (1-10)	No. of ciphertext (1-10)
Wireless sensors network [87]	Sensor nodes (1, 2, 3, ..., 45)	Not specified
Trading [88]	No. of energy domains from 1 to 10	Total number of households are 3851 and price is from 400 to 11000 ($)
Trading [89]	No. of DEP are not specified	Energy consumption from 0 to 14000 (kWh)
Trading [90]	Not specified	Load (30, 40, 50, ..., 130 (MW)) and price from 0 to 5000 ($)
Trading [91]	No. of prosumers (50, 100, 150, ..., 300)	Negotiation time from 0 to 800 (ms)
Trading [92]	No. of EVs (charging /discharging) is from 1 to 30 and No. of charging stations are from 1 to 39	Satisfaction function is from 60 to 180
IoT [96]	No. of communication participants (0, 20, 40, 60, 80, 100)	No. of attributes (0, 10, 20, 30, 40, 50)
IoT [97]	Not specified	No. of files (1, 5, 10, 15, 20)

TABLE 7. Comparison of commonly used consensus algorithms.

Consensus mechanism	Transaction finality	Transaction rate	Token needed	Cost of participation	Scalability of peer network	Transaction throughput
PoW	Probabilistic	Low	✓	✓	High	Low
PoS	Probabilistic	High	✓	✓	High	Low
PBFT	Deterministic	High	✗	✗	High	Medium
Federated BFT	Deterministic	High	✗	✗	Low	Low

its solution. A new compression schema for data and a distributed mechanism, which integrates parallel validation, is proposed. The performance is measured by computing the average computational cost. The results depict that the proposed coarse compression method has the lowest cost than the base case and large frame.

Data sharing has become inevitable because of emerging technologies, and its need for research and business. In data sharing, decentralized methods are preferred because in centralized systems, the data is prone to several security and privacy threats. The blockchain has emerged as a promising solution for sharing data; however, its scalability issue is also there. A novel data sharing method using blockchain is proposed in [108]. Instead of sending whole data on the blockchain, the original data is stored on a cloud system and the sender sends the hash of that data to the receiver. The receiver uses this hash and cloud address to access data remotely. The data is stored on more than one cloud servers and their hashes are shared between the sender and receiver using a blockchain system. In this way, the scalability of blockchain in terms of storage and low latency is achieved.

Topics related to the control of access and scalability in IoT devices are discussed in [109]. Rapid growth in the number of IoT devices used for data collection and communication has led to concerns with scalability and access control. The proposed solution is a fully decentralized blockchain-based architecture, supported by the PoW scheme. It has several components and each one has its unique responsibility. Due to memory and processing power limitations, IoT devices cannot be directly integrated into the blockchain system. Alternatively, they link up with the central hub for management, which communicates with the nodes located throughout the blockchain. The management hubs are computationally powerful devices and are used to translate the messages sent by IoT devices to JSON-RPC. For access control, manager nodes are used. These nodes have computational constraints; however, they are computationally more powerful than other nodes of the network. In order to properly integrate new IoT devices into the system, the manager nodes communicate the device's credentials to the management hubs and then notify the device of the optimal hub's position. The management hub communicates with the nodes in the blockchain. Here, blocks are mined and record of the transactions is kept by executing smart contracts. In this way, the blockchain is made scalable and access management overhead is tackled. For performance evaluation, the system is checked for the throughput while increasing the number of messages by IoT devices and management hubs. The performance of the proposed system ensures its scalability.

The authors in [110] propose a scalable blockchain architecture for IoT devices. A prevalent perspective posits that blockchain technology is well-suited for IoT devices due to its immutability, security, and privacy features. However, it is computationally expensive and has a higher delay, which decreases its suitability. To overcome these issues, a multi-tier lightweight scalable blockchain architecture is proposed. It is deployed in a smart home environment. The IoT devices with low resources are connected to a centralized manager, which performs all the necessary computations for them. To distinguish between these devices, a shared key mechanism is used. The devices with high computational and storage resources (overlay manager) manage the blockchain network collectively. This accomplishes decentralization. The public blockchain is overseen by the cluster chiefs, who are in charge of one of many overlay manager clusters. Extensive simulations are carried out to check the performance of the proposed architecture. Performance is measured in terms of packet overhead and delay. Simulation results show that the proposed architecture is scalable and suitable for IoT devices.

B. SCALABILITY SOLUTION FOR CONSENSUS MECHANISMS

The interest of researchers in blockchain-based solutions is growing rapidly. Decentralization is a highlighting feature of the blockchain, which makes it consummate for several applications. The consensus algorithms are vital for the blockchain to create distributed ledger and perform efficient operations. For consensus, the PoW algorithm is widely adopted in the blockchain technology; however, it is denounced for its energy wastage and scant throughput. Initially, the consensus mechanism of the Bitcoin was demonstrated as a very promising attribute of the blockchain. The performance issues regarding its throughput and scalability were not major in those days because these issues were considered tolerable because of the limited number of users. However, today these issues highly affect the efficiency of a system because the number of users has been increased. So, there is a dire need to resolve these issues and the researchers are taking an interest in BFT. The BFT-based consensus mechanism has emerged as a promising solution [111]. A comparative study of BFT and PoW demonstrates that prior is better than posterior. All of the nodes in BFT are permissioned. It also requires 8% of less power for voting than PoW. Moreover, it provides proof of correctness while PoW does not provide any proof.

The existing BFT scheme suffers from node scalability issues because it is scalable to only tens of nodes as it has $O(n^2)$ message complexity to reach a consensus. To overcome this issue, the authors in [112] have proposed a FastBFT algorithm, which achieves higher throughput and lower latency. The newly proposed protocol is compared with existing BFT and Zyzzyva protocols. The simulation results depict better performance of FastBFT in terms of scalability as it is 6 times faster than Zyzzyva.

Miners of blockchain systems are computationally very powerful; however, the scalability issue is still there. A computationally scalable system is proposed in [113]. The highlighting features of the system are its financial incentives and dispute resolution layer. On the first layer, the task givers provide incentives to the task solvers in exchange for solving a computationally complex problem and verifiers check if the solution is correct or not. On the second layer, task solvers and verifiers play the roles of solvers and challengers, respectively. The miners of Ethereum play the role of referees on the incentive layer and judges at dispute resolution layer. When a dispute arises, the judges resolve it interactively, whereas referees ensure the timely data submission to the incentive layer.

In [114], the authors propose a scalable blockchain architecture for industrial applications. The authors point out the limitation of existing blockchain technology for industries. It is stated that the use of BFT-based blockchain is limited in terms of scalability and network transactions can be viewed by all nodes of a blockchain, which creates several security and privacy issues. The proposed architecture is inspired by satellite chains where several consensus algorithms are executed parallelly and independently from each other. This feature increases the scalability of the blockchain network significantly. It is a permission-based blockchain where every node registers itself and enrolls for a specific role. The client nodes can only send requests to the system for transactions, whereas only validator nodes can take part in the consensus mechanism of the blockchain. The auditors have the authority to check any group of transactions on the network. The regulator nodes of the proposed blockchain system enforce the policies and rules. They can choose either to take part in a consensus mechanism or not. In this way, the proposed architecture is made scalable and secure for industrial applications.

The study by [115] compares and evaluates the SBFT blockchain system's performance to that of PBFT. The scalability and decentralization problems of BFT were intended to be solved by the SBFT system. To get the most out of the SBFT system, its parameters are fine-tuned and tested in various algorithmic contexts. From the experiments, it is concluded that the fine-tuned SBFT gives 2 times more throughput and 1.5 times less latency rate than a fully optimized PBFT system. Its performance makes it more scalable and efficient for deployment where scalability is important. To achieve the good performance, the SBFT needs thresholds for communication reduction up to a linear number, favorable fast path for a solution and the same servers for similar paths. The presence of these characteristics was ensured to be present in order to increase scalability of the system and make it fast. The performance comparison of SBFT and PBFT is done on the basis of the values of latency and throughput.

A consensus protocol is designed in [116]. The highlighting feature of the protocol is that it is scalable in terms of block selection and creation. The scalability depends on the computational power available in a system. It means that a system with high computational power would be able to select multiple blocks and work parallelly. Moreover, the consensus is reached without broadcasting the actual block data and verification of blocks is also efficient. In this way, the privacy issue of the blockchain is resolved. In the proposed system, several committees are formed and each processor belongs to a committee during an epoch. After joining a committee, the processors communicate with each other within a committee to know their identities. In the next step, the consensus of each committee is achieved and sent to the final committee. The final value is computed here and a random value generated by the final committee is broadcasted to the network. The proposed consensus algorithm is evaluated based on the throughput and utilization of bandwidth. The comparison is made between Bitcoin and proposed scalable byzantine consensus protocol. The performance of the byzantine consensus protocol was found to be significantly better.

To solve the scalability issues in B-RAN, a novel consensus algorithm is proposed in [99], named as proof of device. It requires less computational power than PoW consensus algorithm. Evaluation of hash function only once makes this consensus algorithm suitable for B-RAN by improving the scalability of the system. In [117], a satellite-empowered blockchain system is proposed for B-RAN to increase the scalability. The significance of this work is that the proposed system is highly scalable terrestrial blockchain architecture that takes the advantage of wide coverage and ubiquitous connectivity. Moreover, in [118], hash time lock contract (HTLC) is suggested to be a promising solution to increase the scalability of a B-RAN system. In an HTLC based system, the payments between two peers are made off-chain in a trustless environment.

C. DAG BASED SOLUTIONS

According to [119], TrustChain is a permissionless data structure that eliminates the need for a central authority when conducting transactions between unknown parties. In comparison to the PoW mechanism, this one is efficient and can scale. The authenticity and reliability of financial dealings are further guaranteed. It stores transactional records of each agent, which are immutable and every agent has its separate block. It is a parallel chain. It uses the NetFlow algorithm to determine the trustable agents on the network. The algorithm ensures that the agent, which becomes a valid member of the network and accesses the resources, contributes back to what is expected from it. Scalability and data security are both enhanced by doing away with the idea of global consensus and instead relying on immutable records of past transactions. Based on the experimental results, it is clear that the suggested system outperforms Bitcoin in terms of scalability and throughput.

The authors in [120] state that medical research and care providers need patients' data to increase the value of health care services. The advancement in technology made the data availability easy using wearable and mobile technologies. However, several privacy and security issues arise while sharing personal data of an individual. The issues are resolved using decentralized blockchain technology. The data is collected using a mobile application and synchronized with cloud-based storage to later share it with health care and insurance companies. A participant first registers with on-line cloud services and then shares data. The integrity of data is preserved within each blockchain record using proof of integrity and validation scheme. In this work, the scalability of the blockchain is increased using a tree-based data processing and batching system. In this system, large datasets are handled by building a Merkle tree. The records are stamped with the time at which they are generated and then using these timestamps, they are ordered. Two records are grouped and their higher-level group node is generated, which uses a concatenated hash of these grouped records. Two grouped nodes follow the same steps to generate a higher-level node. In this way, a binary tree is generated and a root node is achieved. The hash of this root node is then stored in the blockchain as a transaction. Scalability performance evaluation involves looking at how the average time of integrity proof validation and generation changes as the number of participants increases. Simulation results confirm the scalability performance of the suggested blockchain-based technique.

D. SMART CONTRACT-BASED SOLUTION

In [121], a cryptocurrency system is proposed, which is similar to traditionally used Ethereum. The highlighting feature of the proposed system is that it does not have privacy and scalability issues. It provides the virtual environment to its users and allows them to create smart contracts and perform required operations just like the Ethereum. Four types of roles are defined for this environment and each role has its significant importance. The first role is the verifier who is responsible for the confirmation and verification of the new transactions and publish them. The second role is key, which is a participant of the blockchain network and requests for the transactions. A public key is used as its identifier and it uses a private key for signing the transactions. A virtual machine is the third role of this environment. The virtual machine has its code and related data to control the behavior of the machine. It also interacts with the smart contract. The manager of virtual machines is the fourth role. It monitors the behavior of the virtual machines and it is identified by its public key. Arbitrum provides incentives to the participants who agree to follow the rule pattern off-line, which is implemented on-line through smart contracts. Its architecture is designed in such a way that it reduces the on-line dispute resolution cost.

E. COMPARATIVE ANALYSIS

In this section, the above-discussed papers are comparatively analyzed based on the methods used in the proposed systems to increase scalability. The summary of different solutions proposed to solve the problem of scalability is presented in Table 8.

TABLE 8. Scalability solutions.

Blockchain type	Objective	Proposed solution	Achievement	Performance parameters
Public [99]	Network access and authentication	Proof of device consensus algorithm	Scalability	Throughput, latency
Private [104]	Data sharing	Off-chain solution	Scalability	Not discussed
Private [105]	Not specified	TEE chain	Scalability, throughput, low latency	Throughput, latency
Consortium [111]	Not specified	BFT	Proved BFT is better than PoW	Theoretical comparison
Public [112]	Secret sharing	FastBFT	Scalability, throughput	Throughput, latency
Public [113]	Not specified	Disputes solving system	Scalability, efficiency	Scalability
Consortium [114]	Industries	Satellite chains within hyperledger fabric	Scalability, security	Not discussed
Public [115]	Not specified	SBFT	Scalability, throughput, low latency	Throughput, latency
Consortium [116]	Not specified	Scalable byzantine consensus	Scalability, throughput	Throughput, bandwidth utilization
Public [119]	Not specified	Parallel chain system	Scalability, throughput	Throughput
Public [120]	Data sharing	Merkle tree	Increased scalability	Time complexity
Public [106]	Data sharing	FHIRChain	Secure, scalable data sharing	Theoretical comparison
Public [107]	Data sharing	Parallel validation	Scalability in terms of storage	Theoretical comparison
Public [108]	Data sharing	Cloud-based data sharing	Scalability, security	Theoretical comparison
Consortium [109]	IoT	Multilayer architecture	Efficient access management, scalability	Theoretical comparison
Public [110]	IoT	Multitiered architecture	Scalability	Packet overhead, delay
Public [121]	Cryptocurrency	Arbitrum	Scalability, privacy	Theoretical comparison
Public [117]	Scalability	Satellite-empowered blockchain	Scalability	Throughput
Public [118]	Scalability	HTLC	Scalability	Throughput

An off-chain payment method for Bitcoin is proposed in [104]. In this system, the payments between network nodes are made off-chain using the duplex micropayment channel. Only records of transactions are kept in the blockchain. In this way, the throughput of the system is increased. A similar off-chain payment method is proposed in [105] using the TEE chain. It is a payment method where monetary transactions are made off-line and only records are kept on the blockchain. Instead of using a traditional consensus algorithm as in [104], the fast-freeze algorithm is used, which is simple to implement, computationally less expensive and easily understandable. The proposed system achieves high throughput. This solution seems promising for energy trading unlike [88].

In order to make blockchain-based systems more scalable, the authors in [111], [112], [113], [114], [115], [116], [119] employ several consensus mechanisms. In [111], [112], [115], different versions of BFT algorithm are employed, whereas in [113], [114], [116], [119], TruBit, parallel consensus, scalable byzantine, and parallel TrustChain approaches are utilized to attain consensus, respectively. In addition to TEEs, a fast BFT consensus technique is employed in [112]. A reputable third party or the manufacturer is in charge of TEEs. The system's latency is reduced, throughput is improved, and efficiency and scalability are achieved by this technology. On the contrary, authors in [115] propose an SBFT consensus method and compare it with PBFT. It addresses the scalability and decentralization issues of the basic BFT algorithm. The threshold encryption method is used to secure the data on the blockchain. Moreover, the proposed blockchain system reduces the latency and achieves high throughput.

In TruBit consensus [113], the minor nodes select the transaction to be included in the next block and their verification and validation are carried out off-chain by solver nodes. Incentives are provided to the solver nodes and the whole process is monitored by judges and referees. This method is computationally efficient than PoW; however, the system is less secure and prone to attacks. This system can be considered as a good solution for the scalability issue of [88]. Another method proposed in [114] uses parallel consensus to increase the throughput of the system. Several independent chains work in parallel. They run consensus algorithms independently and maintain their separate ledgers. Node from one chain can communicate with the nodes on other chains. They are free to choose their roles in the network and become part of both the local chain and the satellite chain. This system achieves both security and scalability. A similar system is proposed in [119]. It achieves throughput and Sybil attack resistance using Netflow with TrustChain. Each agent maintains a separate chain and each block contains signatures of both parties involved in a transaction. The block contains the hashes of previous blocks of both agent A and agent B. Instead of a global consensus, the local consensus is achieved. The SBFT [116] also uses a similar concept of parallel consensus. The BFT algorithm is executed in a parallel manner. After the generation of independent blocks, a committee integrates them and generates a final block. Each node belongs to a committee and the actual block data is not broadcasted in the network, hence, privacy of data is achieved This system is both secure and scalable. Unlike [113], [114], [115], [116] achieve both scalability and security.

Blockchain-based data storage and sharing systems are proposed in [106], [107], [108], [120]. The authors in [120] propose a tree-based data structure to store data in a scalable blockchain model. In this model, a Merkle tree is built by joining multiple records. In this way, multiple records are saved against a single hash. Similarly, in [106], a secure and scalable clinical data sharing model is proposed. In this system, instead of saving actual data in a blockchain, reference pointers are stored and anchors are connected to the database. For the security of data and prevent it from unauthorized access, a token-based permission model is used. Only an authorized user with a valid key can decrypt the data. However, [120] seems more efficient in terms of storage-saving as it saves multiple records against a single hash. Similarly, two data sharing models are proposed in [107], [108]. The authors in [107] proposed a parallel validation and compression schema. From the simulation results, it is observed that the proposed model has a low computational cost and is scalable. On the contrary, in [108], the data is stored on a cloud and instead of sending data, the hash of stored data is sent to the blockchain. It makes the network scalable.

A method for controlling access to IoT devices is suggested in [109]. Although the devices are linked to hubs and manager nodes, these devices do not perform the function of network nodes themselves. Instead, the hub and manager nodes are responsible for all the mining and computations. The manager nodes register the new IoT devices and pass their credential information to the hubs. The new device is informed about the location of a suitable hub. The throughput of the system is increased and the system is considered scalable. A similar system is proposed in [110]. The blockchain is implemented on overlay managers and IoT devices are connected to them. These devices are computationally powerful and make the blockchain system scalable as they have low packet overhead and delay. A dispute resolution system for blockchain is proposed in [121]. This scalability solution is based on smart contracts. Different roles are defined for the nodes and smart contracts are designed in such a way that the computational cost of dispute resolution is reduced.

VII. CRITICAL ANALYSIS

In this section, a critical analysis of our comprehensive survey is provided. In this review, we have compiled the key points from the aforementioned literature on blockchain types, consensus mechanisms, and key features. This section provides a concise overview of the survey's key points and conclusions.

Critical comment 1: It has been noted in the literature [81], [82] that scalability and efficiency are inversely related. In existing work, if a system is efficient and it is designed in such a way that its performance meets the requirements of end-users for high computations or throughput, then it will not be scalable. Increased scalability will reduce its efficiency and throughput.

Critical comment 2: Blockchain is computationally very expensive. It is observed from existing studies [81], [96], [97], that the blockchain executes a complex algorithm for consensus and it uses encryption techniques for the security of data. Both steps require high computational power, which increases with increment in both data and network. The cost of computational power cannot be ignored as its demand is already increasing drastically.

Critical comment 3: A thorough analysis has shown that the blockchain is very complicated. While data encryption and decryption do improve data security, they also lengthen the time it takes for transactions to complete. The blockchain is distributed and before confirmation of any transaction, a consensus algorithm is executed. When all or the majority of nodes on the network confirm this transaction only then it is added to the block and considered complete. This whole procedure makes the blockchain slow as compared to other available options like traditional payment methods.

Critical comment 4: The blockchain is like other distributed networks. It learns to defend attacks when it faces them and with time it becomes stronger. For this reason, the blockchain network should be large, comprising of a variety of nodes. On the other hand, when the network gets larger than a certain limit, then its scalability issues arise and it becomes slow [82], [83], [84], [85], [86], [87], [88], [96], [97]. So, this problem needs to be addressed. Researchers are proposing new solutions, i.e., [99], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116], [117], [118], [119], [120], [121], to overcome scalability issues;

however, there is plenty of room for improvements as it has just started to grow.

Critical comment 5: The blockchain removes the third party between two nodes that want to trade with each other. It is claimed that it works free of cost; however, it is not the case. The request initiator has to pay some cost, how small it may be, in the form of gas [82], [83], [105]. The amount of gas required for a transaction increases with the size of the transaction. Large transactions are split into small transactions and each transaction requires a separate gas amount. It makes transactions on the blockchain costly. However, this cost is less than the cost users pay to an intermediary third party.

Critical comment 6: A major critic on the PoW consensus algorithm is the 51% attack. In a PoW based blockchain system [81], [83], [84], [87], [88], [89], [91], [94], [96], [97], if more than half of the network nodes are hacked or they act maliciously, then whole network will be under the control of these nodes. As Bitcoin is using the same algorithm for consensus, so, their mining pools are always monitored by the security community, which prevents such attacks and also ensures that network is not under the control of any specific group.

Critical comment 7: While blockchain technology does involve some degree of distributed computing, the literature suggests that it is more accurately described as a distributed network. There is no parallelism or synergy of mutual assistance. All the transactions are validated following the same rules written in the smart contracts and each node saves the same copy of data. Moreover, in the PoW algorithm [81], [83], [84], [87], [88], [89], [91], [94], [96], [97], all the miner nodes perform the same computation to guess the next hash, which is not efficient, as millions of nodes are consuming high amount of energy and when a node succeeds, efforts of rest of the miner nodes are wasted.

Critical comment 8: Another blockchain attraction is that it is claimed to be anonymous and open, e.g., it is claimed that in a public blockchain [82], [83], [84], [87], [88], [96], [97], when two parties trade with each other and party A pays dues to party B, party B can acquire the information of party A's bank balance and its payments' pattern. This information breach of party A can lead to some serious financial damage. This kind of sensitive information should be kept secret even if both trading parties are anonymous, as too much information revelation poses dangers.

Critical comment 9: The literature study reveals that PoW and PoS, two widely used consensus algorithms, are inefficient and susceptible to attacks. Researchers are proposing alternative methods, i.e., BFT, fastBFT and PBFT. Such methods need extensive testing under different scenarios to check whether these algorithms reduce the overkill dimensions of legacy consensus algorithm or not. This analysis is not simple as it needs detailed knowledge for the implementation of these methods and record their behavioral patterns to check their superiority.

Critical comment 10: The data size of the blockchain network increases rapidly as the record of all the transactions on the network is maintained. Any node, which becomes part of this chain has to download and store this data to be part of this network and participate in the system. Data downloading and user verification process can take days to complete; meanwhile, the user is unable to send or receive payments on the network. These issues can greatly affect users' decisions about using blockchain. An alternative way to avoid these issues is to not download data of the whole network. This solution negates the "trustless" foundation of the blockchain and also the concept of P2P communication between nodes is destroyed, as users need to trust some central entity.

VIII. FUTURE CHALLENGES

The blockchain technology is adopted in many research fields and business areas to provide opportunities and solutions to different problems. In order to make it more efficient and dependable, we need to fix the problems that hinder its uses. Here we will go over some of the most typical blockchain shortcomings and how to fix them. These improvements are considered as fruitful areas for future research directions.

- Suitability is a great feature of the blockchain. If a user wants to do a transaction with a trustless source or see its historical data, then blockchain is the solution as it has an immutable nature. If multiple users of a network want to change the whole system and trace previous transactions to see every state of the system, then using the blockchain they can easily do it. For transactions that need to be tracked, the blockchain is a good fit as well. Data recorded in a blockchain cannot be traced beyond its hash value because of the network's size limitations. Tracing data in a blockchain is computationally very expensive and involves huge monetary cost [28].
- Privacy is considered as the main concern in a blockchain network. On completion of a transaction, its hash is maintained in the ledger of every node. So, all network nodes can easily view the data using its hash. It is also observed that the malicious attacks occur in a blockchain by nodes, which are part of it. There is a need to work on the privacy of every participant in the network because everyone wants privacy. The major concern is that no one should be able to access data of other nodes using the hash of a transaction. In a blockchain network, address of every participant is anonymous; however, it is traceable.
- The authorized nodes are granted permission to /hlaccess data through the access control mechanism. It is a significant obstacle in the blockchain network, and academics are attempting to address it by utilizing smart contracts to establish various access control approaches. This factor directly affects the privacy and trust of users. Every participant in the network wants to get access to their data through the transaction log; however, no one wants that any other node on the network access their

transactional detail, which is maintained in a distributed ledger.

- Trust is an important aspect in the blockchain and it is directly related to security. In a blockchain network, users are nodes who can act as both service providers and receivers. So, they want to do trading and data sharing without any third party in the P2P network. No one wants to compromise his personal information. The reputation and feedback systems are also established by many companies to do P2P decentralized sharing. There is a need to establish a system, which maintains trust in the blockchain. It should also increase the security level of the P2P system. It is an important point, which needs to be improved in the future.
- As in a decentralized system, access control management and secure data storage are the key aspects in the fields of health care, IoT and wireless sensor networks. There is a variety of applications; however, there are some challenges due to which scope of the system becomes limited. Most of the proposed blockchain based solutions are platform-dependent and restricted to a specific environment, for which they are developed. Besides, some blockchain solutions require on-chain and off-chain transactions. These transactions are the requirement of resource constraint devices. So, some studies suggest that there is a need for grand software exposure [122] to minimize the security problems. Other future challenges are cache attacks that are required to be investigated in the future.
- To improve the performance of a blockchain network, there is a need for an efficient consensus mechanism, which runs many transactions concurrently. There is a huge difference between the performance of the existing systems and blockchain-based systems. By considering the throughput of blockchain-based systems, there is still a need for improvement in methods to fulfill real-time market requirements. By considering the integrity and adaptability of a system, various use cases are found for the private and public systems. A large blockchain system like Bitcoin is secure. However, scalability issues arise, which are not suitable for IoT and other networks. There is still need for solutions for blockchain-based applications in such scenarios.
- Interoperability is a feature, which is used to increase the efficiency of different systems in multiple domains. When the blockchain is integrated into different systems then the heterogeneous type of data is compressed, processed, extracted and stored in the blockchain. Various blockchain-based artificial intelligence (AI) applications are used for transactions and cryptocurrency is used to pay the transaction fee. So, there is a need to make applications and systems more interoperable to deploy efficient smart contracts, which require minimum computations to save gas.
- In a blockchain network, the storage is made scalable by storing data at a decentralized external storage; however, the cost for decentralization has increased. It is also one of the emerging issues of blockchain, which needs to be addressed in future that how to minimize the cost of decentralized storage for users.
- Majority attacks can happen when 51% nodes control mining in the blockchain network. If an attacker attains less than 50% mining power even then it is dangerous for the blockchain network. The attacker can gain the information using hashes of blocks and transactions and can modify the block data after attaining 51% majority in the network. So, a small fee is required to give as an incentive to miner nodes to motivate maximum network nodes to take part in mining. There is a need to introduce some incentive mechanisms for miners to improve the efficiency and performance of the network.
- Editability is an issue due to the immutable nature of blockchain. Immutability means non-modifiable. If a transaction is added to the block and its hash has been calculated, it cannot be modified. If anyone wants to add information or modify existing data, a new transaction is created and new data is added related to that transaction. It increases the blockchain size and storage cost. So, there should be some mechanism, which allows to delete and edit some blocks. It is a new direction to improve blockchain. In fact, the editable blockchain will be designed with cryptographic algorithms to maintain the security.

IX. CONCLUSION

Blockchain is an emerging technology, which became mature with time. It has captivated the attention of many researchers with its applicability and features. However, many problems also arise with its applications: scalability, privacy, security, maliciousness of nodes, high computational cost, etc. In this survey, we conducted a comprehensive survey on blockchain scalability and its impact on several domains. The main objective of this survey was to identify major scalability issues, which affect the performance of a blockchain network. Moreover, we also carried out a survey of solutions used to solve these issues. From a comprehensive analysis, we concluded that scalability mainly depends on three factors: data storage, throughput and monetary cost.

Additionally, this article has provided an outline of blockchain technology and the various domains that have been affected by them. Also covered, in relation to the current literature, most popular consensus methods and how they affect system throughput. According to the research, one of the most important aspects of a network's scalability is the type of blockchain used. Additionally, data storage scalability solutions are provided in a nutshell. These solutions, which are referred to as off-chain solutions, are crucial for maximizing throughput at a low cost. We take a look at the current blockchain-based solutions and make some suggestions for where the field should go from here in light of the blockchain's impending problems.

In the future, we aim to provide a comprehensive examination of different aspects and limitations of blockchain technology and its effects on other technologies. Moreover, it is observed that privacy and security are the two vital aspects of a blockchain based systems. They not only affect the scalability of a blockchain based system but also have a great impact on efficiency and throughput of a system. Considering these point in mind, an in-depth analyses of these aspects on scalbility, throughput and efficiency of blockchain based system is required, which we will do in future.

REFERENCES

[1] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.

[2] W. Al-Saqaf and N. Seidler, "Blockchain technology for social impact: Opportunities and challenges ahead," *J. Cyber Policy*, vol. 2, no. 3, pp. 338–354, Sep. 2017.

[3] J. Song, P. Zhang, M. Alkubati, Y. Bao, and G. Yu, "Research advances on blockchain-as-a-service: Architectures, applications and challenges," *Digit. Commun. Netw.*, vol. 8, no. 4, pp. 466–475, Aug. 2022.

[4] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Nov. 11, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] S. Davidson, P. D. Filippi, and J. Potts, *Economics of Blockchain*, document SSRN 2744751, 2016.

[6] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," 2017. Accessed: Jun. 4, 2024. [Online]. Available: https://www.plasma.io/plasma-deprecated.pdf

[7] (2018). *Komodo An Advanced Blockchain Technology, Focused on Freedom*. Accessed: Sep. 3, 2023. [Online]. Available: https://komodoplatform.com/wpcontent/uploads/2018/03/2018-03-12-Komodo-White-paper-Full.pdf

[8] J. Poon and D. Thaddeus. (2016). *The Bitcoin Lightning Network: Scalable Off-chain Instant Payments*. Accessed: Dec. 12, 2019. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[9] Wikipedia Contributors. (2020). *Scalability*. Accessed: Apr. 9, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Scalability/citenote-1

[10] A. Hayes. (2019). *Scalability: What It Is, and How It Works*. Investopedia. [Online]. Available: https://www.investopedia.com/terms/s/scalability.asp

[11] H. Kohad, S. Kumar, and A Ambhaikar, "Scalability issues of blockchain technology," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2385–2391, Feb. 2020.

[12] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-Work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.

[13] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Comput. Commun.*, vol. 151, no. 2020, pp. 395–418, 2020.

[14] N. Farah, "Blockchain technology: Classification, opportunities, and challenges," *Int. Res. J. Eng. Technol.*, vol. 5, no. 5, pp. 3423–3426, 2018.

[15] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[16] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[17] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[18] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[19] S. Thakur and V. Kulkarni, "Blockchain and its applications—A detailed survey," *Int. J. Comput. Appl.*, vol. 180, no. 3, pp. 29–35, Dec. 2017.

[20] Y. Lu, "Blockchain and the related issues: A review of current research topics," *J. Manage. Analytics*, vol. 5, no. 4, pp. 231–255, Oct. 2018.

[21] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.

[22] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[23] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[24] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1568–1573.

[25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019.

[26] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[27] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[28] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[29] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, 2019.

[30] R. Wang, K. Ye, and C.-Z. Xu, "Performance benchmarking and optimization for blockchain systems: A survey," in *Proc. Int. Conf. Blockchain*, 2019, pp. 171–185.

[31] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang, "A survey on blockchain-based Internet service architecture: Requirements, challenges, trends, and future," *IEEE Access*, vol. 7, pp. 75845–75872, 2019.

[32] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019.

[33] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[34] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

[35] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.

[36] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Gener. Comput. Syst.*, vol. 100, pp. 325–343, Nov. 2019.

[37] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[38] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102397.

[39] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Banking Financial Technol.*, vol. 3, no. 1, pp. 1–17, Apr. 2019.

[40] J. W. Heo, G. S. Ramachandran, A. Dorri, and R. Jurdak, "Blockchain data storage optimisations: A comprehensive survey," *ACM Comput. Surveys*, vol. 56, no. 7, pp. 1–27, Jul. 2024.

[41] S. Kayikci and T. M. Khoshgoftaar, "Blockchain meets machine learning: A survey," *J. Big Data*, vol. 11, no. 1, pp. 1–9, Jan. 2024.

[42] O. Akanfe, D. Lawong, and H. R. Rao, "Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities," *Int. J. Inf. Manage.*, vol. 76, Jun. 2024, Art. no. 102753.

[43] A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid, and M. F. Yusof, "Scalability challenges in healthcare blockchain system—A systematic review," *IEEE Access*, vol. 8, pp. 23663–23673, 2020.

[44] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[45] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, pp. 373–406.

[46] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Appl. Sci.*, vol. 11, no. 20, p. 9372, Oct. 2021.

[47] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, Dec. 2021, Art. no. 103232.

[48] S. Park, S. Im, Y. Seol, and J. Paek, "Nodes in the Bitcoin network: Comparative measurement study and survey," *IEEE Access*, vol. 7, pp. 57009–57022, 2019.

[49] M. Pratap. (2020). *Everything You Need to Know About Smart Contracts: A Beginner's Guide*. Accessed: Mar. 12, 2020. [Online]. Available: https://hackernoon.com/everything-you-need-to-know-about-smart-contracts-a-beginners-guide-c13cc138378a

[50] (2020). *Consensus Algorithms in Blockchain—Geeksforgeeks*. Accessed: Mar. 12, 2020. [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/

[51] A. S. Almasoud, F. K. Hussain, and O. K. Hussain, "Smart contracts for blockchain-based reputation systems: A systematic literature review," *J. Netw. Comput. Appl.*, vol. 170, Nov. 2020, Art. no. 102814.

[52] Y. Cai and D. Zhu, "Fraud detections for online businesses: A perspective from blockchain technology," *Financial Innov.*, vol. 2, no. 1, pp. 1–10, Dec. 2016.

[53] M. Möhlmann, T. Teubner, and A. Graul, "Leveraging trust on sharing Economy platforms: Reputation systems, blockchain technology and cryptocurrencies," in *Handbook of the Sharing Economy*. Ann Arbor, MI, USA: Edwards, 2019.

[54] M. J. A. Baig, M. T. Iqbal, M. Jamil, and J. Khan, "Design and implementation of an open-source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, node-red and, MQTT protocol," *Energy Rep.*, vol. 7, pp. 5733–5746, Nov. 2021.

[55] J. Yang, A. Paudel, H. B. Gooi, and H. D. Nguyen, "A proof-of-stake public blockchain based pricing scheme for peer-to-peer energy trading," *Appl. Energy*, vol. 298, Sep. 2021, Art. no. 117154.

[56] F. Jamil, N. Iqbal, Imran, S. Ahmad, and D. Kim, "Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid," *IEEE Access*, vol. 9, pp. 39193–39217, 2021.

[57] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102426.

[58] S. S and H. Wang, "Security enhancement in smart vehicle using blockchain-based architectural framework," *J. Artif. Intell.*, vol. 3, no. 2, pp. 90–100, Jun. 2021.

[59] A. Banotra, J. S. Sharma, S. Gupta, S. K. Gupta, and M. Rashid, "Use of blockchain and Internet of Things for securing data in healthcare systems," in *Multimedia Security*. Springer, 2021, pp. 255–267.

[60] A. Ali, H. A. Rahim, M. F. Pasha, R. Dowsley, M. Masud, J. Ali, and M. Baz, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, no. 16, p. 2034, Aug. 2021.

[61] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022.

[62] P. Anitha Rajakumari and P. Parwekar, "Optimizing the valid transaction using reinforcement learning-based blockchain ecosystem in WSN," in *Intelligent Systems*. Springer, 2021, pp. 551–559.

[63] C. Çeken and E. Karakoç, "Black hole attack prevention scheme using a blockchain-block approach in SDN-enabled WSN," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 37, no. 1, p. 37, 2021.

[64] M. Sridhar and P. B. Pankajavalli, "Standardization of security in geographic routing protocol using blockchain and optimization based clustering technique," *Natural Volatiles Essential Oils J.*, vol. 1, pp. 12441–12454, Dec. 2021.

[65] A. Lakhan, M. Ahmad, M. Bilal, A. Jolfaei, and R. M. Mehmood, "Mobility aware blockchain enabled offloading and scheduling in vehicular fog cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4212–4223, Jul. 2021.

[66] C. Lin, D. He, X. Huang, and K. R. Choo, "OBFP: Optimized blockchain-based fair payment for outsourcing computations in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3241–3253, 2021.

[67] A. Ali, A. Khan, M. Ahmed, and G. Jeon, "BCALS: Blockchain-based secure log management system for cloud computing," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 4, p. e4272, Apr. 2022.

[68] I. Alnafrah and S. Mouselli, "Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries," *Int. J. Educ. Develop.*, vol. 85, Sep. 2021, Art. no. 102460.

[69] G. Caldarelli and J. Ellul, "Trusted academic transcripts on the blockchain: A systematic literature review," *Appl. Sci.*, vol. 11, no. 4, p. 1842, Feb. 2021.

[70] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, "A blockchain-based multi-cloud storage data auditing scheme to locate faults," *IEEE Trans. Cloud Comput.*, vol. 10, no. 4, pp. 2252–2263, Oct. 2022.

[71] Z. Lejun, P. Minghui, W. Weizheng, S. Yansen, C. Shuna, and K. Seokhoon, "Secure and efficient medical data storage and sharing scheme based on double blockchain," *Comput., Mater. Continua*, vol. 66, no. 1, pp. 499–515, 2020.

[72] 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," in *Banking Beyond Banks and Money*. Cham, Switzerland: Springer, 2016, pp. 239–278.

[73] M. A. Almaiah, "A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology," in *Studies in Big Data*. Cham, Switzerland: Springer, 2021, pp. 217–234.

[74] R. Goyat, G. Kumar, M. Alazab, R. Saha, R. Thomas, and M. K. Rai, "A secure localization scheme based on trust assessment for WSNs using blockchain technology," *Future Gener. Comput. Syst.*, vol. 125, pp. 221–231, Dec. 2021.

[75] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Rep.*, vol. 7, pp. 8075–8082, Nov. 2021.

[76] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," *IEEE Access*, vol. 9, pp. 103651–103669, 2021.

[77] F. Loukil, K. Boukadi, R. Hussain, and M. Abed, "CioSy: A collaborative blockchain-based insurance system," *Electronics*, vol. 10, no. 11, p. 1343, Jun. 2021.

[78] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101954.

[79] (2014). *Blockchain Voting Used by Danish Political Party*. Accessed: Mar. 1, 2020. [Online]. Available: https://www.cryptocoinsnews.com/blockchain-voting-used-by-danish-political-party/

[80] *Voting Solutions to Improve Integrity of Voting*. Accessed: Mar. 8, 2020. [Online]. Available: https://followmyvote.com/contact/

[81] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.

[82] J. An, D. Liang, X. Gui, H. Yang, R. Gui, and X. He, "Crowdsensing quality control and grading evaluation based on a two-consensus blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4711–4718, Jun. 2019.

[83] Y. Wu, S. Tang, B. Zhao, and Z. Peng, "BPTM: Blockchain-based privacy-preserving task matching in crowdsourcing," *IEEE Access*, vol. 7, pp. 45605–45617, 2019.

[84] Y.-J. Chen, L.-C. Wang, and S. Wang, "Stochastic blockchain for IoT data integrity," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 373–384, Jan. 2020.

[85] M. M. H. Onik, C.-S. Kim, N.-Y. Lee, and J. Yang, "Privacy-aware blockchain for personal data sharing and tracking," *Open Comput. Sci.*, vol. 9, no. 1, pp. 80–91, Jan. 2019.

[86] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019.

[87] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[88] L. Park, S. Lee, and H. Chang, "A sustainable home energy prosumer-chain methodology with energy tags over the blockchain," *Sustainability*, vol. 10, no. 3, p. 658, Mar. 2018.

[89] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 2, p. 162, Jan. 2018.

[90] Y. Yu, Y. Guo, W. Min, and F. Zeng, "Trusted transactions in micro-grid based on blockchain," *Energies*, vol. 12, no. 10, p. 1952, May 2019.

[91] F. Luo, Z. Y. Dong, G. Liang, J. Murata, and Z. Xu, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4097–4108, Sep. 2019.

[92] X. Huang, Y. Zhang, D. Li, and L. Han, "An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains," *Future Gener. Comput. Syst.*, vol. 91, pp. 555–562, Feb. 2019.

[93] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jul. 2018.

[94] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.

[95] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.*, 2017, p. 650.

[96] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[97] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[98] *Know Which Blockchain or DLT Platform Works Well Within Your Usecase: Comparison of Different Blockchain*. Accessed: Dec. 3, 2020. [Online]. Available: https://medium.com/@kotsbtechcdac/know-which-blockchain-or-dlt-platform-works-well-within-your-usecase-comparison-of-different-a8dc34782af3

[99] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[100] S. Velliangiri, R. Manoharan, S. Ramachandran, and V. Rajasekar, "Blockchain based privacy preserving framework for emerging 6G wireless communications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4868–4874, Jul. 2022.

[101] X. Ling, P. Chen, J. Wang, and Z. Ding, "Data broker: Dynamic multi-hop routing protocol in blockchain radio access network," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 4000–4004, Dec. 2021.

[102] Y. Le, X. Ling, J. Wang, R. Guo, Y. Huang, C.-X. Wang, and X. You, "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12025–12043, Dec. 2021.

[103] T. Sachinidis, A. A. Boulogeorgos, and P. Sarigiannidis, "Dual-hop blockchain radio access networks for advanced coverage expansion," in *Proc. 10th Int. Conf. Modern Circuits Syst. Technol. (MOCAST)*, Jul. 2021, pp. 1–5, doi: 10.1109/MOCAST52088.2021.9493339.

[104] C. Decker and R. Wattenhofer, "A fast and scalable payment network with Bitcoin duplex micropayment channels," in *Proc. 17th Int. Symp. Stabilization, Saf., Secur. Distrib. Syst. (SSS)*, vol. 9212. Cham, Switzerland: Springer, 2015, pp. 3–18.

[105] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, "Teechain: A secure payment network with asynchronous blockchain access," in *Proc. 27th ACM Symp. Operating Syst. Princ.*, Oct. 2019, pp. 63–79.

[106] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, May 2018.

[107] R. Kiran Raman, R. Vaculin, M. Hind, S. L. Remy, E. K. Pissadaki, N. Kibichii Bore, R. Daneshvar, B. Srivastava, and K. R. Varshney, "Trusted multi-party computation and verifiable simulations: A scalable blockchain approach," 2018, *arXiv:1809.08438*.

[108] H. U. Chaoxin and K. Lu, "Secure and scalable data transfer using a hybrid blockchain-based approach," U.S. Patent 55 515 154, Nov. 16, 2017.

[109] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[110] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.

[111] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. workshop open problems Netw. Secur.*, 2015, pp. 112–125.

[112] J. Liu, W. Li, G. O. Karame, and N. Asokan, "Scalable Byzantine consensus via hardware-assisted secret sharing," *IEEE Trans. Comput.*, vol. 68, no. 1, pp. 139–151, Jan. 2019.

[113] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains," in *Aspects of Computation and Automata Theory With Applications*. Singapore: World Scientific, 2023, pp. 377–424.

[114] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, "Towards scalable and private industrial blockchains," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, Apr. 2017, pp. 9–14.

[115] G. Golan Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. Reiter, D.-A. Seredinschi, O. Tamir, and A. Tomescu, "SBFT: A scalable and decentralized trust infrastructure," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2019, pp. 568–580.

[116] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena. *SCP: A Computationally-Scalable Byzantine Consensus Protocol for Blockchains*. Accessed: May 8, 2019. [Online]. Available: https://www.weusecoins.com/assets/pdf

[117] X. Ling, Z. Gao, Y. Le, L. You, J. Wang, Z. Ding, and X. Gao, "Satellite-aided consensus protocol for scalable blockchains," *Sensors*, vol. 20, no. 19, p. 5616, Oct. 2020.

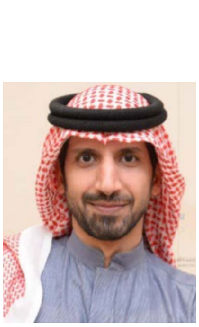
[118] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: A new paradigm towards 6G," *Nat. Sci. Rev.*, vol. 8, no. 9, 2021, Art. no. nwab069, doi: 10.1093/nsr/nwab069.

[119] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.

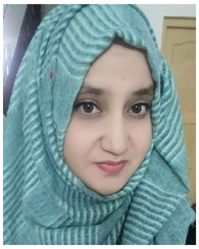
[120] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.

[121] H. A. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *Proc. USENIX Security Symp.*, 2018, pp. 1353–1370.

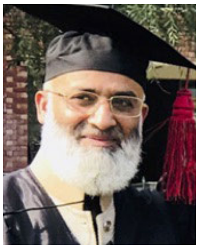
[122] F. Brasser, U. Müller, A. Dmitrienko, K. Kostiainen, S. Capkun, and A. R. Sadeghi, "Software grand exposure: SGX cache attacks are practical," in *Proc. 11th USENIX Workshop Offensive Technol.*, 2017, pp. 1–12.



TURKI ALI ALGHAMDI received the bachelor's degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, the master's degree in distributed systems and networks from the University of Hertfordshire, Hatfield, U.K., in 2006, and the Ph.D. degree from the University of Bradford, U.K., in 2010. He holds CDCDP and CDCMP certificates. He is currently a Professor with the Computer Science Department, Faculty of Computer and Information Systems, Umm Al-Qura University (UQU), Makkah, and the Founding Director of the SMarT Laboratory. He has more than 15 years of research and development, academia, and project management experience in IT. He is passionate about developing the translational and collaborative interface between industry and academia. His research interests include wireless sensor networks, energy and QoS aware routing protocols, network security, the IoT, and smart cities.



RABIYA KHALID is a research fellow in University of Leeds, Leeds, England (U.K.). She has received the MCS degree from Mirpur University of Science and Technology (MUST), Mirpur (Azad Kashmir), Pakistan, in 2014. She obtained the M.S. degree in Computer Science with a specialization in Energy Management in Smart Grids from the Communications over Sensors (ComSens) Research Lab, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus, under the supervision of Prof. Nadeem Javaid, Pakistan in 2017. She did her Ph.D. in Computer Science under the same supervision and from the same Lab in 2021. Her research interests include Data Science/AI, Blockchain, Smart Grids, etc. She has authored more than 20 research publications in international journals and conferences.



NADEEM JAVAID (Senior Member, IEEE) received the Ph.D. degree from the University of Paris-Est, France, in 2010. He is currently a Tenured Professor and the Founding Director of the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus. He has served as Visiting Professor at University of Technology Sydney (UTS), Australia. Now, he is working as Visiting Professor in International Graduate School of Artificial Intelligence, National Yunlin University of Science and Technology, Taiwan. He has supervised 203 Master's and 34 Ph.D. theses. He has authored over 950 articles in technical journals and international conferences and a U.S. Patent. His research interests include energy optimization in smart/micrograds, health care, wireless sensor networks using blockchain and data analytics/AI. He received the Best University Teacher Award (BUTA'16) from the Higher Education Commission (HEC), Pakistan, in 2016, and the Research Productivity Award (RPA'17) from the Pakistan Council for Science and Technology (PCST), in 2017. He has delivered many Keynote and Invited Speeches in national and international conferences. With 28,000 Citations and H-Index 83, he is Pakistan's Best Scientist in Engineering & Technology/Computer Science in the Stanford University's List of Top 2% Scientists in the World.