

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/369305733>

A Survey on Role of Blockchain for IoT: Applications and Technical Aspects

Article in *Computer Networks* · March 2023

DOI: 10.1016/j.comnet.2023.109726

CITATIONS

24

READS

1,085

5 authors, including:



Anshuman Kalla

Uka Tarsadia University

49 PUBLICATIONS 1,317 CITATIONS

[SEE PROFILE](#)



Gürkan Gür

Zurich University of Applied Sciences

110 PUBLICATIONS 2,662 CITATIONS

[SEE PROFILE](#)



Madhusanka Liyanage

University College Dublin

333 PUBLICATIONS 10,482 CITATIONS

[SEE PROFILE](#)

A Survey on Role of Blockchain for IoT: Applications and Technical Aspects

Shikha Mathur, Anshuman Kalla*, Gürkan Gür, Manoj Kumar Bohra*, Madhusanka Liyanage

Abstract—In recent times, IoT has emerged as a new paradigm for the interconnection of heterogeneous, resource-constrained, and communication-capable smart devices. It has been anticipated as a key enabler for various domains of applications such as health care, automotive, agriculture, industrial operations, automation, energy, and the next generation of living. However, the current IoT applications face significant challenges in terms of the huge amount of collected data, intensive data exchange, security, privacy, centralized processing, and interoperability. To mitigate many of these issues, blockchain has been identified as a promising innovative technology. Blockchain, in conjunction with smart contracts, has received significant attention both from the industry and academia and offers features such as irreversibility, non-repudiation, proof of provenance, fault tolerance, pseudonymity, decentralized operations and decision-making, and distributed ledger. The integration of blockchain with IoT requires essential insights concerning the application areas, scalability, security, privacy, data storage and management, performance, and governance. Thus, this paper intends to expound on the opportunities and key aspects of using blockchain in the IoT landscape. Specifically, this paper surveys the utilization of blockchain for various IoT applications. Besides, the paper distinguishes different technical aspects and presents the associated research challenges. At last, future research directions are discussed depending on the lessons learned.

Index Terms—Blockchain, Smart Contracts, DLT, Internet of Things (IoT)

I. INTRODUCTION

The Internet of Things (IoT) is a network of physical objects called “things”, such as home appliances, machines, and various digital objects. These things or devices are mostly resource-constrained and can perform operations such as sensing, monitoring, pre-processing (i.e., lightweight computing), and exchanging of data [1]. Moreover, these devices are communication-capable and are connected over the Internet using different underlying technologies and protocols such as RFID, Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, LoRa, and Sigfox [2]. According to [3], the number of such connected devices will reach 75 billion by the end of 2025.

* Corresponding authors

Shikha Mathur is with the Department of Computer and Communication Engineering, Manipal University Jaipur, India. e-mail: shikhamathur806@gmail.com

Anshuman Kalla is with the Department of Computer Engineering, CGPIT, Uka Tarsadia University, Bardoli, Gujarat, India. email: anshuman.kalla@ieee.org

Gürkan Gür is with the Zurich University of Applied Sciences (ZHAW), Switzerland. e-mail: gueu@zhaw.ch

Manoj Kumar Bohra is with the Department of Computer and Communication Engineering, Manipal University Jaipur, India. e-mail: manojkumar.bohra@jaipur.manipal.edu

Madhusanka Liyanage is with the School of Computer Science, University College Dublin, Ireland. e-mail: madhusanka@ucd.ie

Further, it is expected that by 2030 the number of IoT devices will touch the mark of 500 billion [4].

In 1982 the first practical application of IoT was implemented when a Coca-Cola machine installed at Carnegie Mellon University was connected with APRANET to find if the available drinks were cold or not [3]. Later, the term Internet of Things was given by Kevin Ashton in 1999, and in the 2000, LG launched the world’s first internet-enabled refrigerator [5]. Since then, the world has witnessed enormous growth in IoT-driven devices and applications.

The evolution from the early days of the Internet to the present IoT comprises five phases [6]. Initially, it started with connecting computers, whereas in the second phase, the concept of the World Wide Web (WWW) came and led to connecting computers all around. The third phase started with the emergence of the mobile internet, which connected mobile devices to the Internet. In the next phase (i.e., the fourth phase), people started joining the Internet by using social networking platforms, and finally, the concept of IoT originated [1], [6]. Some of the promising applications of IoT are healthcare, smart home, smart city, smart grid, and Unmanned Aerial Vehicles (UAVs) [1]. Despite the hype, several issues revolve around IoT, like centralization, massive data gathering, scalability, security threats, privacy issues, resource limitation, mobility, and interoperability [3], [7]. Blockchain (BC) can play a cardinal role in mitigating these issues thereby paving the way for a blockchain-enabled IoT ecosystem.

BC is one of the most prominent types of Distributed Ledger Technology (DLT) where the ledger (i.e., database of transactions) is distributed among all the nodes in the Peer-to-Peer (P2P) network [8]. The word *blockchain* implies the data structure used to build and manage the distributed ledger. Fundamentally, the data structure used for the ledger in BC is a growing sequence of logically linked (i.e., cryptographically chained) blocks to build a chain of blocks [9]. A block is a unit that contains a set of verified transactions that occurs during a given time window and are cryptographically secured. Every block is connected with the previous block using a hash-based chain. This means the hash of the previous block is stored in the current block. The first block of a blockchain is called the genesis block [10], which does not have any transaction. Moreover, the value of the ‘previous block hash’ field is set to zero in the genesis block [11].

BC intensively uses cryptographic techniques such as hashing, public-private key pair, digital signature, Merkle tree, and time-stamping. Moreover, it employs a consensus mechanism to establish an agreement in a decentralized environment [12]. Some unique features of BC technology are temper-

TABLE I: Summary of the main Acronyms used in this paper introduced in Table I.

Acronym	Definition
BC	Blockchain
BTC	Bitcoin
CTN	Communication Things Network
CH	Cluster Head
CHC	Centralized Healthcare Controller
DLT	Distributed Ledger Technology
DAG	Directed Acyclic Graph
DPoS	Delegated Proof of Stake
DApps	Decentralised Applications
DCS	Decentralised, Consistent & Scalable
DoS	Denial of Service
EHR	Electronic Health Record
EV	Electric Vehicle
FSC	Food Supply Chain
HC	Healthcare
HIPAA	Health Insurance Portability & Accountability Act
IoT	Internet of Things
ICO	Initial Coin Offering
ITO	Initial Token Offering
IIoT	Industrial Internet of Things
IV	Intelligent Vehicle
ITS	Intelligent Transportation System
LMDS	Lamport Merkle Digital Signature
MAS	Multi-Agent System
MEC	Mobile Edge Computing
MT	Mobile Terminals
NONCE	Number Used Only Once
NT	Network Theory
PoW	Proof of Work
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PoET	Proof of Elapsed Time
PoI	Proof of Importance
PoB	Proof of Burn
P2P	Peer to Peer
PAT	Principal Agent Theory
PK	Public Key
RBV	Resource-Based View
SC	Smart Contracts
SATS	Satoshi
SCM	Supply Chain Management
SHS	Smart Home System
Tx	Transaction
TxID	Transaction Identification
TCA	Transaction Cost Analysis
UAV	Unmanned Aerial Vehicle
UTC	Coordinated Universal Time
WBAN	Wireless Body Area Network

persistent, transparency, non-repudiation, proof of provenance, fault tolerance, pseudonymity, decentralized decision-making, and distributed ledger. From the application point of view, Bitcoin is the most popular and the first use case of blockchain technology specially designed for monetary transactions. Nevertheless, with time, BC has been found beneficial for many other domains such as healthcare, supply chain, education, insurance, and logistics [13].

The meanings of the abbreviations used in this paper are

A. Advantages of Blockchain in IoT

BC ends up being quite possibly the most promising advancement to unleash the maximum potential of IoT. The advantages of using BC for IoT are discussed as follows [14]:

1) **Reduced Cost:** For every emerging technology, the cost is an essential factor of consideration. IoT follows a centralized approach, and numerous intermediary (third-party) services are also used. Each of these services charges some fee which gets added to the overall cost [15]. As a result, the overall cost gets inflated. On integrating BC with IoT, the BC P2P decentralized network acts as backend; thus, the centralized server is no longer required. Furthermore, using smart contracts helps eliminate the need for third-party services. Therefore, BC for IoT reduces intermediate cost or brokerage fees [14], [16], [17].

2) **Trust Among Parties:** Trust is defined as when all the participating nodes in the network can communicate and share data without worrying about the integrity of the data [18]. For communication and data sharing in the network, maintaining trust is important [18]. It can be achieved by removing malevolent nodes from the network [18]. IoT involves a lot of interconnected devices and an overwhelming amount of data is shared and processed, which requires trust among the users to share data. But these IoT devices do not communicate with each other due to possibility of a loss of data [19]. But, by integrating BC with IoT brings trust among the participants. Because of its decentralized and distributed trust mechanism, all the participating nodes can view each transaction's details and validation is done by establishing the consensus, which helps in maintaining the transparency and trust between the users [16].

3) **Privacy:** Privacy is defined as protection of information from exposure to unauthorized ones [20]. It can be either data privacy or user privacy or location privacy. The availability of private sensor data such as personal identifying information or indirect information like location [21], through which users identity can be revealed to malicious users is loss of privacy [20]. It is important to maintain privacy for successful implementation of IoT. In particular, involves several centrally connected devices, continuously transmitting data and numerous companies are monitoring this data, and sometimes they can misuse personal data or identity [22]. But by combining BC with IoT, a blockchain-generated address is provided to all the participants and interactions occur between these addresses. The physical world identity of these participants is not revealed. For IoT applications that involve sensitive information, this feature will be of great use to hide the real identity [23], [24].

4) **Security:** Security is defined as the protection against the cyberattacks and vulnerabilities. Authentication, authorization, integrity, interoperability, or adaptability are the key aspects for any system to maintain security [18]. Maintaining security means security of device, data transmission and data storage [25]. Security in terms of IoT is protecting devices present in the network, from intruders [25]. In the large-scale deployment of IoT, handling security vulnerabilities is

a major challenge due to heterogeneity of the network. BC intrinsically supports security by establishing trust through its immutable and decentralised nature [26]. Since it intensively uses cryptographic mechanisms like PKI, hashing, Merkle tree, and timestamp as well as uses distributed consensus algorithm for adding new content in the distributed ledger. Hashing makes it impossible to alter the data and a decentralized peer-to-peer approach makes the network resilient against failures [27].

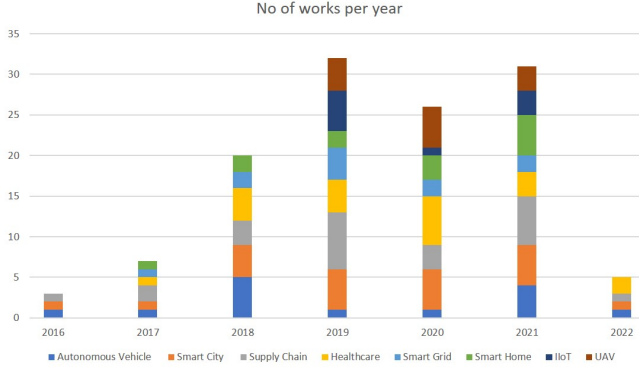


Fig. 1: Statistics of the surveyed research works

B. Motivation

The central aim of this survey is to focus on what BC can bring to the IoT landscape. To this aim, we carried out an in-depth study of various contributions made by academia and industry in the domain of BC-integrated IoT. Moving forward, we focused on different use cases emerging from BC-integrated IoT, such as healthcare, smart cities, smart grids, autonomous vehicle, and UAVs. Moreover, efforts have been made to explore numerous technical aspects when integrating BC with IoT and identify the challenges related to these technical aspects. Furthermore, the open issues and future research directions are also discussed in this survey paper.

In view of the above discussion, although numerous survey papers exist, not many specifically address the integration of BC and IoT for a wide range of IoT applications, along with the technical aspects. A survey of existing BC protocols

for the IoT was presented in [28]. Numerous surveys on BC technology based on different viewpoints, such as its architecture, types, consensus algorithm, and characteristics, were introduced in [29]–[31]. Various studies exploring the role of BC in IoT and the impacts of integrating BC with IoT were presented in [32]–[37] and the challenges in coordinating BC and IoT were presented in [7], [14], [16], [23], [38]. Works [14], [39], [40] discussed the future directions in BC technology.

Table IV summarizes the recent survey papers on using BC for IoT. In particular, the table shows (in brief) the main contribution of the recent surveys, the IoT applications they study, and the BC technical aspects they emphasize. Although the existing survey papers cover different IoT applications and BC technical aspects, it is difficult to find one paper that studies the use of BC for a wide range of IoT applications in detail. Moreover, most existing surveys focus on the individual aspects, i.e., either application areas or the technical aspects with challenges. Thus, the *motivation* of this paper is four-fold:

- To study and investigate the applications and technical aspects of integrating blockchain and IoT in-depth.
- To cover as many as eight different BC-IoT applications, including healthcare, smart homes, smart cities, supply chain, autonomous vehicles, smart grid, IIoT, and UAVs.
- To classify the existing research works into different categories for each of the eight applications considered.
- To explore the challenges related to the technical aspects (such as scalability, security, privacy, data storage, and power consumption) and their possible solutions for the BC-integrated IoT ecosystem.
- To conduct an exhaustive survey by including the most recent research in the space of BC-enabled IoTs. Figure 1 depicts year-wise statistics of the research works surveyed in this paper.

We started with a first-level bibliometric analysis to further strengthen our motivation behind conducting this survey. To do so, the Scopus database is used to extract the bibliometric data that covers the research work done in the blockchain and IoT landscape. The data exported from Scopus included details like the publication year, author, institution, and source journal. The search is done using the title. In total, 477 valid papers were exported using Scopus. Next, the VOSviewer tool is used to visualize the extracted data and plot the graphs [41]. Fig. 2 shows the geographic distribution, i.e., the countries participating in BC-IoT research. As shown in Table II, China has the highest number of publications and citations on Blockchain-IoT, followed by India and the United States. Fig. 3 shows the BC-IoT co-citation journal network, which helps in analyzing the number of articles from different journals and the frequency of citations. The bigger the node size, implies more the number of articles published. Moreover, Table III depicts the top five productive journals in Blockchain for IoT research. IEEE Internet of Things Journal has the highest number of publications.

TABLE II: Top 10 Countries Based on Publication in the Field of BC IoT

Rank	Country	Publications	Citations
1	China	191	1802
2	India	158	889
3	United States	116	1124
4	South Korea	55	976
5	United Kingdom	53	403
6	Australia	44	1417
7	Canada	40	599
8	Saudi Arabia	38	225
9	France	37	399
10	United Arab Emirates	34	824

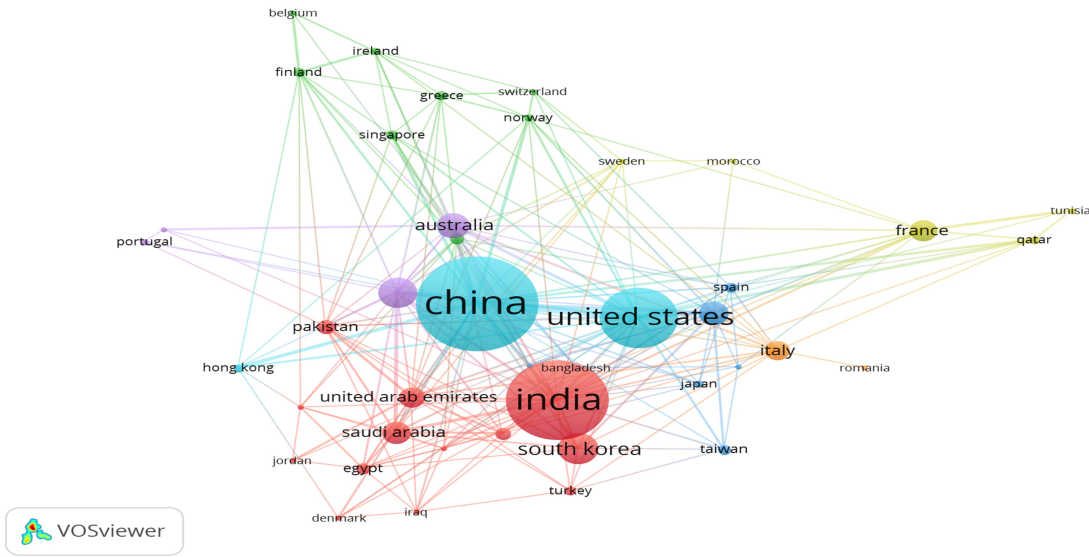


Fig. 2: Countries Participating in BC-IoT Research

C. Our Contribution

One of the key contributions of this work is to explore the capabilities of BC technology and to study how BC can resolve the potential challenges of emerging IoT applications. In particular, the current survey covers the role of BC in numerous IoT application areas such as healthcare, smart homes, supply chain and logistics, smart city, smart grid, autonomous vehicles, UAVs, and Industrial IoT (IIoT). Moreover, the present survey puts the important technical aspects (that need to be considered for BC-enabled IoT applications) under a magnifying lens. In this direction, the challenges related to these technical aspects are explored, and several

proposed solutions to overcome these challenges are discussed. Towards the end, the lesson learned from the literature survey is presented, which aims to consolidate answers to how the maximum benefits can be leveraged by integrating BC with emerging IoT applications.

The contributions of this survey are as follows:

- **To present blockchain technology and smart contracts in a nutshell:** The paper presents a synopsis of blockchain technology and smart contracts keeping in mind the broader canvas of the IoT ecosystem. The aim here is to enable the readers to develop the essential foundation of blockchain technology, its salient

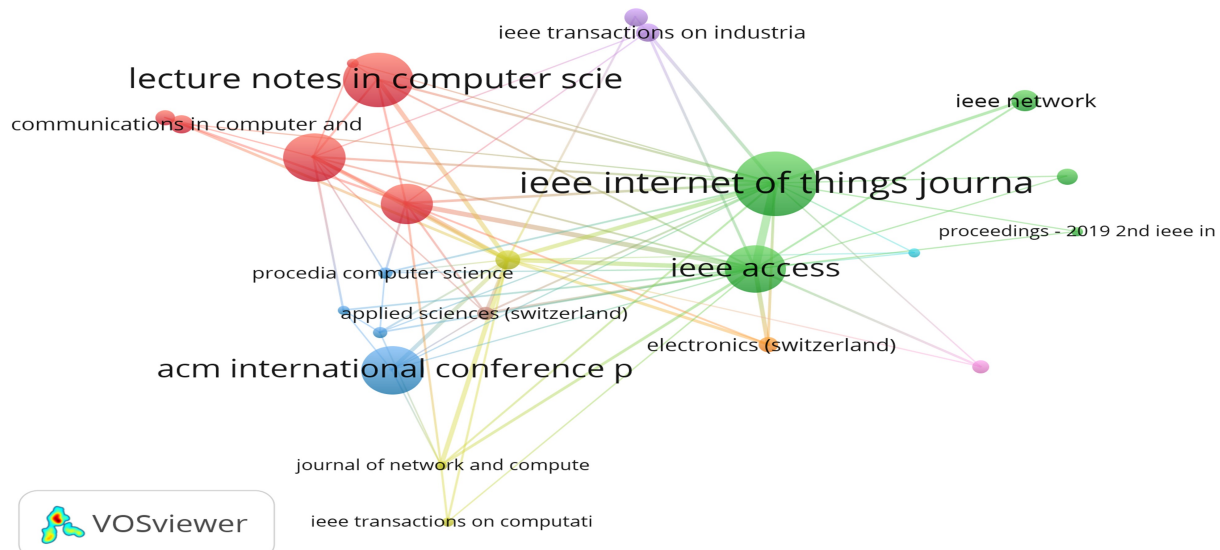


Fig. 3: BC-IoT Co-Citation Journal Network

features, relevant taxonomy, and typical process flow in the blockchain.

- **To assimilate and study various BC-enabled IoT applications:** The paper outlines a handful of BC-enabled IoT key application areas such as healthcare, smart city, smart home, smart grid, autonomous vehicle, unmanned aerial vehicle, and Industrial IoT. In particular, the role of BC in these IoT application areas, and the classification of the research works under various categories have been discussed.
- **To investigate pertinent technical aspects and highlight the challenges related to the integration of BC for IoT:** Identify and discuss the open challenges in integrating BC and IoT and their possible solutions. The effect of these challenges and the work done in these aspects are also discussed.
- **To discuss future research directions based on the lessons learned:** Based on our findings, we have featured the possible and significant research challenges that have to be addressed. This will help researchers in related domains to find their future directions.

D. Organization

The remainder of the paper is organized as follows: Section II provides an overview of Distributed Ledger Technology (DLT), BC technology (related terminologies, types, and transaction flow), smart contracts, and salient features of BC. Section III revolves around various BC-empowered IoT applications. This section includes an introduction to these applications, their importance, the challenges in implementing them, how BC can mitigate these challenges, and the related work done in these areas. Section IV discusses the technical aspects such as scalability, security and privacy, IoT data storage, consensus algorithms, and processing power. This section outlines these technical aspects by first introducing them, their importance for Blockchain, and their importance for BC for IoT as well. Section V presents the lessons learned and future research directions. Finally, section VI concludes the paper. The outline of the paper is presented in Fig. 4.

II. BACKGROUND

This segment explains the fundamentals of DLT and BC, key attributes of BC, its terminologies and types, and smart contracts.

TABLE III: Top 5 Productive Journals in BC IoT Research

Rank	Sources	Documents	Citations
1	IEEE Internet of Things Journal	41	696
2	Lecture Notes in Computer Science	34	82
3	Advances in Intelligent Systems and Computing	30	176
4	ACM International Conference Proceeding Series	30	165
5	IEEE Access	29	722

A. Distributed Ledger Technology (DLT)

A conventional centralized network uses client-server architecture where one or more clients are directly connected to the central server. On the other hand, in a decentralized P2P network, multiple nodes are connected in a P2P fashion. Any node is equally capable of serving a client attached to this decentralized P2P network. DLT comprises a decentralized P2P network of nodes and distributed ledger. **Moreover, DLT uses cryptographic techniques and a consensus mechanism to secure and synchronize the underlying system. A distributed ledger is a type of shared ledger where the ledger is replicated at all the nodes in the network [15].**

DLT has the potential to address the many shortcomings of traditional centralized approaches. **The key highlights of DLT are (i) decentralized governance, (ii) immutability, (iii) reliability, and (iv) authentication [50].** Creating **immutable records** helps in achieving transparency, immutability, and verifiability and also reduces costs associated with distributing and maintaining the ledger [51]. In general, DLT is a class, and BC is one of the most popular members of that class. In other words, BC is a type of DLT.

B. Blockchain Technology

BC, a type of DLT, consists of a distributed ledger and a P2P network of nodes and uses cryptographic techniques and consensus mechanisms. The distinguishing factor for BC is the data structure (i.e., the chain of blocks) used to build the distributed ledger. Any update in the ledger is achieved by using a consensus mechanism that establishes agreement among the nodes, which helps in achieving consistency. Any change in the ledger is synchronized and reflected at each participating node [52].

Before moving forward it is necessary to understand the basic block structure and the related terminologies used in BC [30], [53]. Fig. 5 shows the detailed view of BC.

1) **Block:** As mentioned above, BC is a chain of blocks where each block contains a set of finite and valid transactions. The blocks are connected using a cryptographic hash-based chain. In general, a block is divided into two parts - block header and block body. The block header is used to hold various fields such as version, timestamp, previous block's hash, the difficulty level in form of nbits, Merkle root hash, and nonce. **The block body contains transactions and at times smart contracts as well [54], [55].** Usually, the **number of transactions that can be accommodated in one block depends on the maximum allowable block size**, which is platform-dependent. For instance, the maximum size of the bitcoin block is 1 MB.

2) **Merkle Tree Root Hash:** It is one single hash value that uniquely and compactly represents all the transactions present in the block body. This hash digest is calculated using the Merkle tree technique. Moreover, it enables easy verification of the correctness of the transactions in a given block.

3) **Timestamp:** It is the time of creation of a block, which is stored as one of the fields in the block's header [56]. This field is useful in keeping a record of the time when the transactions were confirmed which later helps in knowing when and what

TABLE IV: Summary of Recent Surveys on Blockchain for IoT

Ref.	Main Contribution	Applications								BC Technical Aspects					Relevance to IoT
		HC	SC	SCL	SG	AV	UAV	SH	IIoT	Sca	Sec	DS	CA	PP	
[35]	Discussed the issues in IoT systems and how BC can mitigate these issues. Also discussed why the BC platform is needed to implement IoT.	-	-	-	-	-	-	-	-	✓	-	✓	-	-	Presented how BC as a service can be implemented for IoT applications and discussed the future research directions in BC-IoT.
[37]	Discussed the use of BC in IoT considering four scenarios - access control, data provenance, integrity, trusted third party, and automatic payment platform.	-	✓	-	-	-	-	-	-	-	-	-	-	-	Discussed explicitly the research challenges for all the four different application scenarios considered.
[42]	Briefly introduces BC technology with its challenges and limitations with exploring its potential applications.	✓	✓	✓	✓	-	-	✓	-	✓	✓	✓	-	-	Provides a detailed discussion over the convergence of BC and IoT. Highlighted the challenges and opportunities in IoT and BC integration, IoT application areas using BC.
[43]	Compared several consensus algorithms for resource-constrained IoT systems using numerous parameters such as BC type, decentralization, scalability, latency, computation, storage, and network overheads.	-	-	-	-	-	-	✓	-	✓	-	✓	-	✓	Discussed the limitations of current IoT system and how BC can overcome them while considering the use case of the smart home.
[44]	Presented a detailed survey on various attacks while mapping each attack to different layers of IoT/IIoT architecture, and discussed how BC can address these security challenges.	-	-	✓	✓	-	-	-	✓	✓	✓	-	-	-	Presented a taxonomy for IoT/IIoT security and focused on two specific use cases (smart factory and smart grid) for IIoT and (healthcare and VANET) for IoT.
[45]	Presented evolution and working principles of BC. Reviewed security solutions offered with the use of BC in IoT.	-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	Discussed the most relevant BC-IoT applications and highlighted the challenges in BC-IoT integration that need to be considered.
[33]	Outlined the architecture that implements BC in managing heterogeneous IoT systems.	-	-	-	-	-	-	-	-	-	-	-	-	-	Also discussed the limitations of the previous IoT system and the challenges in integrating BC and IoT.
[46]	Surveyed the recent works done in BC-IoT, BC-Cloud IoT, and BC-Fog IoT with a focus on smart cities, homes, and vehicular networks.	-	-	-	-	-	-	-	-	-	-	-	-	-	Briefly reviewed the role of BC in various application areas of IoT such as SDN-enabled IoT, mobile IoT, and IoT supply chain.
[47]	Provides a detailed survey covering the taxonomy of BC-based IoT security, various attacks on BC-IoT system, and framework for BC IoT security.	-	-	-	-	-	-	-	-	-	✓	✓	-	✓	Talked about core security issues in IoT, how BC can address them as well as presented new attack surfaces that arise with BC-enabled IoT system.
[48]	Presented a survey on using BC to address security and privacy challenges in IoT and proposed a BC-based IoT framework.	-	-	-	-	-	-	-	-	-	✓	✓	-	✓	Listed out various security issues and their adverse effects on different layers of IoT architecture.
[49]	Author has discussed BC and fuzzy blockchain framework for threat detection in IoT network.	-	-	-	-	-	-	-	-	-	-	-	-	-	Author has used an adaptive neuro-fuzzy inference system, fuzzy control system, and fuzzy matching modules. Also, compared the results with fuzzy classifiers.
Our Paper	The paper presents an exhaustive survey on BC for IoT including BC (types, salient features, and smart contracts), BC-enabled IoT applications, important technical aspects along with the challenges in integrating BC and IoT.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Eight distinct IoT applications are studied in-depth which are envisioned to be immensely benefited with the integration of BC. Moreover, future directions for these IoT applications are discussed based on the lessons learned.

HC - Healthcare; SC - Smart City, SCL - Supply Chain & Logistics, SG - Smart Grid, AV - Autonomous Vehicles, UAV - Unmanned Aerial Vehicles, SH - Smart Home, IIoT - Industrial Internet of Things, Sca - Scalability, Sec - Security, DS - Data Storage, CA - Consensus Algorithm, PP - Processing Power.

has happened on the blockchain and makes it more difficult for an intruder to alter the blockchain. It is the current time in seconds in GMT since 1 January, 1970 [57], [58]. The value of timestamp (T) is valid if T is greater than the median timestamp of the previous eleven blocks and $T - 2h$ is smaller than the network time (median of the timestamps returned by all nodes connected to the node) (h is a cryptographic hash function) [59].

4) **Nonce**: is a number used once. It is a four bytes field used to compute the hash of a block's header such that the

hash value meets the difficulty level. More specifically, it is a random number that the miner keeps guessing to calculate the block header's hash value. In a brute-force manner, a miner starts with zero as a value for the nonce field and keeps increasing it for every iteration of hash calculation [58]. A miner stops when the computed hash value meets the difficulty level, and a new block is said to be mined for the specific nonce value (used in that iteration).

5) **Previous Hash**: The previous block hash field of any given block stores the block hash of the immediate previous

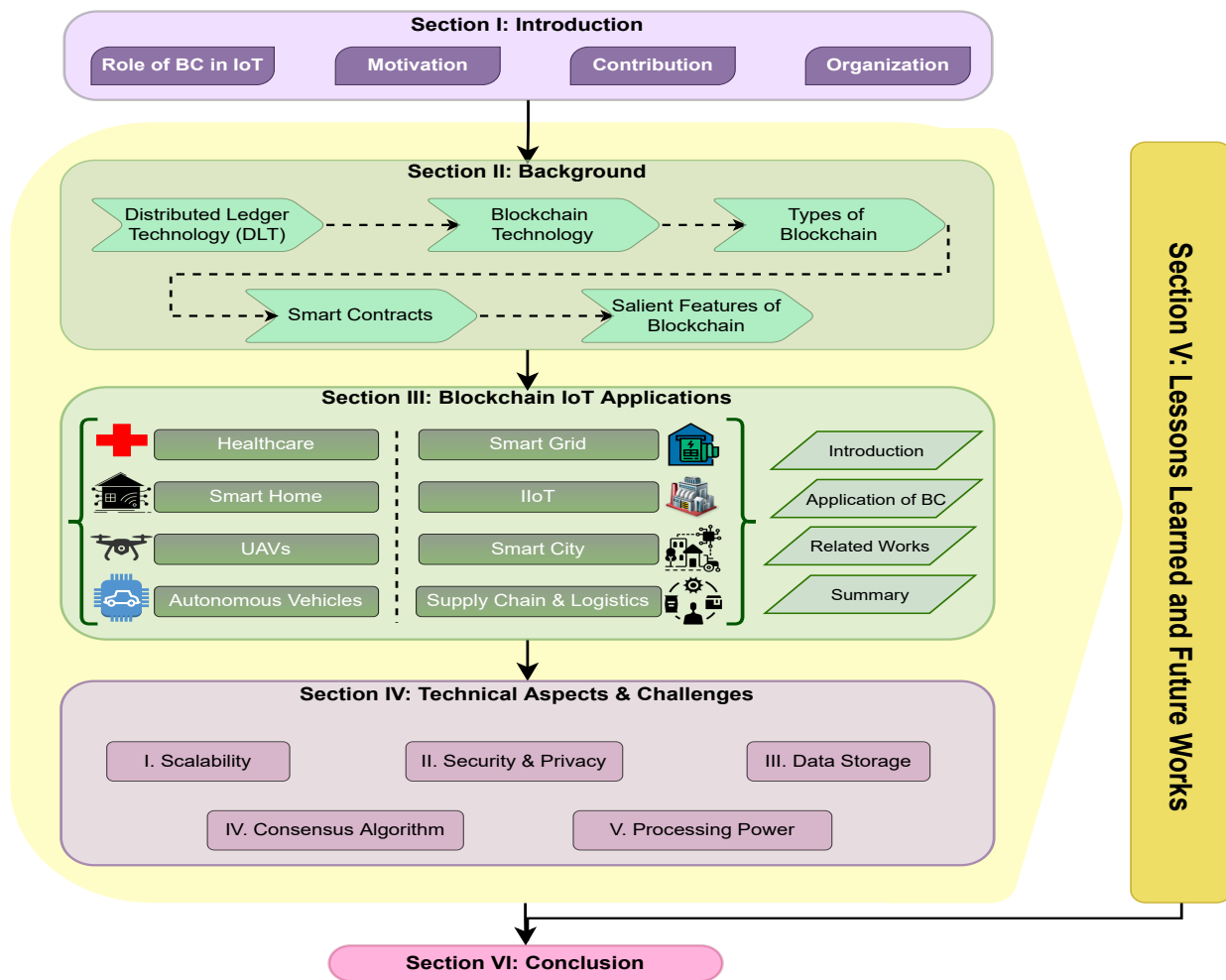


Fig. 4: The Outline of the Paper

block. This leads to the formation of a chain of blocks and makes the blockchain an append-only data structure. Any change in a transaction of any block by an attacker will produce a different block hash, which should be reflected in all the subsequent blocks. Thus the ledger becomes inconsistent and the changes can be easily detected. The value of the previous hash field in the genesis block is set to zero.

Another interesting concept in BC is forking [60]. At any given time, a large number of nodes (i.e., miners) can participate in BC network. Thus, there can be circumstances when different miners mine different (valid) blocks at the same time. In this situation, these valid but different blocks are being broadcasted in the BC network. Hence, different parts of the BC network will append different blocks resulting in inconsistency in the blockchain. In other words, different nodes will have different recent blocks in their local copy of the ledger, and this is known as the forking problem. BC resolves this issue by considering simply the longest chain while all the blocks in the other smaller chains will be discarded or considered orphaned, as shown in Fig. 5.

C. Types of Blockchain

There are numerous ways based on which BCs can be divided into different types. Fundamentally, BCs can be considered of three types - public, private, and consortium BC.

1) **Public Blockchain:** It is open and accessible for all who want to participate in the network. Public BC is fully decentralized, where no entity controls the BC, and every participating node has equal rights [30]. Moreover, all the participating nodes can participate in the validation of transactions and block mining [62] [63]. Examples of public BC implementation are Bitcoin and Ethereum or Litecoin [64].

2) **Private Blockchain:** It is specifically designed for a single organization, and participants need permission to join the network. After entering the network, participants can access the transactions in the ledger. Only a few selected nodes from the governing organization have exclusive rights to add new blocks and update the ledger. Participating nodes in the private BC do not need to solve the computationally intensive puzzle to reach a consensus. Moreover, usually, the nodes are not provided with any financial incentives. Hyperledger fabric is the most widely used private permissioned BC [30], [62].

3) **Consortium or Federated Blockchain:** Consortium or federated BC is designed for multiple companies or a group

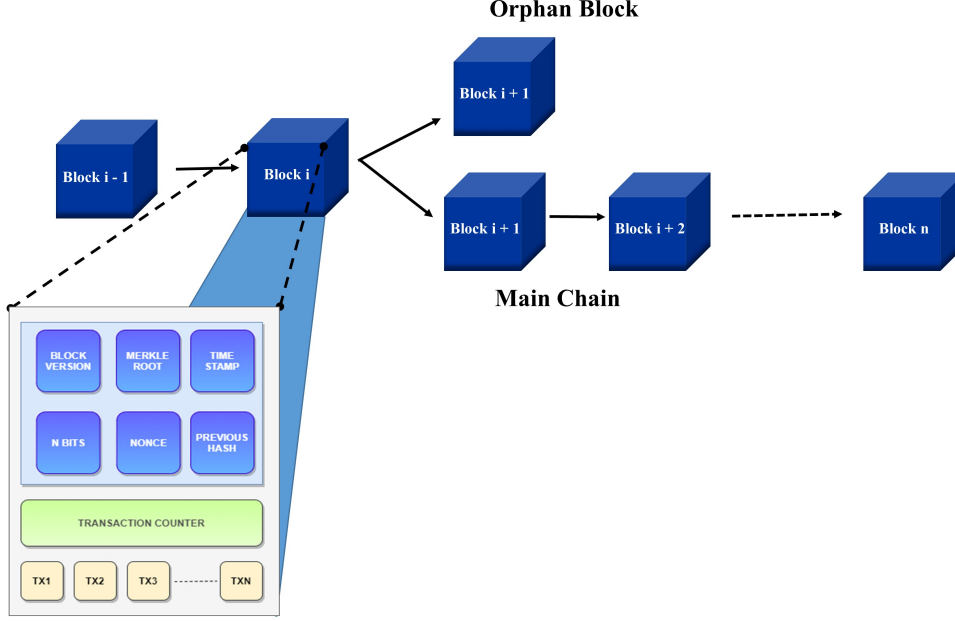


Fig. 5: Structure of the Block

TABLE V: Comparison Among Public, Private & Consortium Blockchains [29] [61]

Property	Public	Private	Consortium
Consensus Algorithm	All nodes	One organization	Only selected nodes
Immutability	Extremely difficult to alter	Modifications are possible	Modifications are possible
Efficiency	Low	High	High
Centralized	No (fully decentralized)	Yes	Partially centralized
Node's Joining Process	Permissionless	Permissioned	Permissioned
Entities' Identity	Pseudonymous	Known entities	Known entities
Confirmation of Transaction	Order of minutes	Order of milliseconds	Order of milliseconds
Write Permission	Write for all	Write for nodes from single organization	Write for only selected nodes from group organizations
Asset	Local Asset	Any Asset	Any Asset

of companies participating in a single BC. It is partially centralized with known set of participating nodes from group organizations [61]. Table V, shows the comparison among the three types of BCs.

D. Smart Contracts

Smart contracts were first proposed in 1994 by Nick Szabo [65]. Smart contracts are equivalent to contracts in the real world, the only difference is that they do not need any administering body for their execution and they are software-based [66]. Smart contract is a set of logic and functions (with the relevant data) that get executed when the pre-defined conditions are satisfied by an external or internal trigger [46]. **Usually, a smart contract is executed when it is invoked by a valid transaction containing the address of the smart contract that occurs in the system and has access rights.** Smart contracts when running on top of a blockchain provide numerous advantages, automation is one of them. Moreover, as the need for intermediaries is

removed, the contract also reduces the expenses required in paper-based traditional contracts [67].

Ethereum was the first BC platform that supported smart contracts [68]. It runs on the Ethereum runtime engine and the byte code is generated since it runs faster on the Ethereum Virtual Machine (EVM) [46]. Since smart contracts are stored on the Ethereum (i.e., on-chain), their byte codes are assigned a unique address after deploying it on EVM [46], [69]. This unique address assigned to the smart contracts in Ethereum is 20 bytes [70]. The transaction associated with smart contracts results in a change in the state of the decentralized ledger [46]. As the smart contracts are stored inside the BC, they inherit some of the properties of BC such as immutability, autonomous execution, transparency, accuracy, and elimination of trusted third parties [69]. **By immutability, we mean once the smart contract is created, it must be verified before the deployment in the nodes as it can not be changed. So no one can tamper with the contract [38].** Autonomous execution means the program written in smart contracts will

run automatically once the BC system reaches the triggering state, which also eliminates any biased operations, not only builds trust but also gives accurate output, and also the need for a trusted third party is not required [69]. Transparency means that the smart contract logic is visible to all the nodes, which ensures trust between the parties [69] and distribution means that the output of the contract is validated by each node in the same way as any other transactions. Bitcoin was the first cryptocurrency to support smart contracts features but it has very limited features. Then world's second-largest cryptocurrency Ethereum was designed specially to support smart contracts [71]. Ethereum platform specially designed for financial and asset trading, its native cryptocurrency is Ether, also supports smart contracts, written in LLL (Low-level lisp-like language), Serpent, Viper, and Solidity [72], [66].

Hyperledger fabric designed especially for enterprise users such as supply chain, trade finance, and stock trading, supports smart contracts written using Java, NodeJs, and GoLang programming language [69]. Corda designed another blockchain-based platform for applications like energy trading, insurance, and retail marketing. Its native cryptocurrency is Corda coin, which supports smart contracts written using languages like Kotlin/Java [69]. NEM is also a blockchain-based cryptocurrency platform specially designed for Banking, gaming, advertising, and marketing and its native cryptocurrency is XEM [69]. Some additional features of NEM such as time stamping documents, identity proof, creation of customized digital assets, and support of smart contracts. Stellar, a blockchain platform designed for financial transactions, and its native cryptocurrency is Lumen, supports smart contracts [69]. Blockchain-based platform Waves, designed for applications like ride-sharing and customized asset trading and its native cryptocurrency Waves uses Scala programming language, and language for smart contracts is non-Turing complete language [69].

E. Salient Features of Blockchain

In this section, we discuss the unique features of BC technology as follows. Fig. 6, illustrates the basic attributes of BC.

1) **Distributed:** Since BC is a type of DLT thus at the core of blockchain lies a ledger which is shared with all the participating nodes such that each node has an exact replica of the ledger [15]. Each node participating in the network can access and view the complete history of transactions without the need for any centralized authority [73].

2) **Decentralization:** In traditional centralized architecture each transaction is regulated and validated by a central party or an intermediary. In contrast, BC uses decentralized network of nodes for validating and confirming transactions. As soon as a transaction is initiated, it is broadcasted to every node in the network. Any node can mine a new block which contains this transaction and thus the transaction gets confirmed in decentralized manner (not by a central authority) [15]. Moreover, decentralization ensure no single point of failure and services are unaffected even if some of the nodes are unavailable.

3) **Immutability:** All the data, i.e., blocks (and transactions within) are cryptographically sealed and chained together. Smallest change in any transaction (in a given block) will lead to drastic change in the value of the Merkle root hash and consequently that block header's hash value will change. As a result, all the subsequent blocks will have to be changed which needs lot of re-computations and consensus among the participating nodes [74]. Thus, once a block is mined and added to blockchain it is said to be immutable (or temper-proof).

4) **Provenance:** Whenever a transaction is recorded in the BC, details of the transaction are recorded across all the nodes because of the decentralized nature of BC. Also, BC uses timestamps to record each transaction which allows each node to keep the order of the transactions [75]. Since each transaction is transparently and permanently recorded across all the nodes, the user can verify and trace transactions at any time [30]. It provides traceability and transparency of the data [76].

5) **Availability:** It is another important feature of BC. It means that the services are always available to the users because of the decentralized nature of the BC network and the system becomes immune to various intentional (e.g., denial of service attack) or accidental failures [77].

6) **Transparency:** Another important key attribute of BC is transparency. All the participating nodes present in the network can view all the transaction details and associated values. Each node present in the network has a copy of the ledger and is authorized to verify and trace the previous records in the distributed network which promotes trusted workflow, sharing of data, immutability, and verifiability [75], [78].

7) **Anonymity:** Anonymity is another key strength of BC technology. Each user in the BC network is assigned a unique BC generated alphanumeric address. Thus users are (pseudo) anonymous, and no central authority is monitoring users' private information. Transactions occur between these BC-generated addresses [73]. This feature provides a certain amount of privacy but at the same time, illegal activities could also happen [76].

8) **Non-Repudiation:** Non-repudiation is again a very important feature of BC. Non-repudiation means users can not deny the activities performed by them, thanks to cryptographic techniques such as digital signature [77], [79].

III. BLOCKCHAIN-BASED IOT APPLICATIONS

This section includes the multiple areas in which blockchain-based IoT can be utilized, the pertinent challenges, and also provides measures to manage these challenges.

A. Healthcare

Healthcare represents an entire ecosystem where health professionals (with the help of advanced medical technologies) diagnose, treat and cure illness or diseases of people. It is estimated that the healthcare market will touch US\$ 372 billion by the year 2022 and the hospital industry will reach up to US\$ 133.44 billion by 2023 [81]. Smart healthcare originated from smart earth proposed by IBM in 2009 [82].

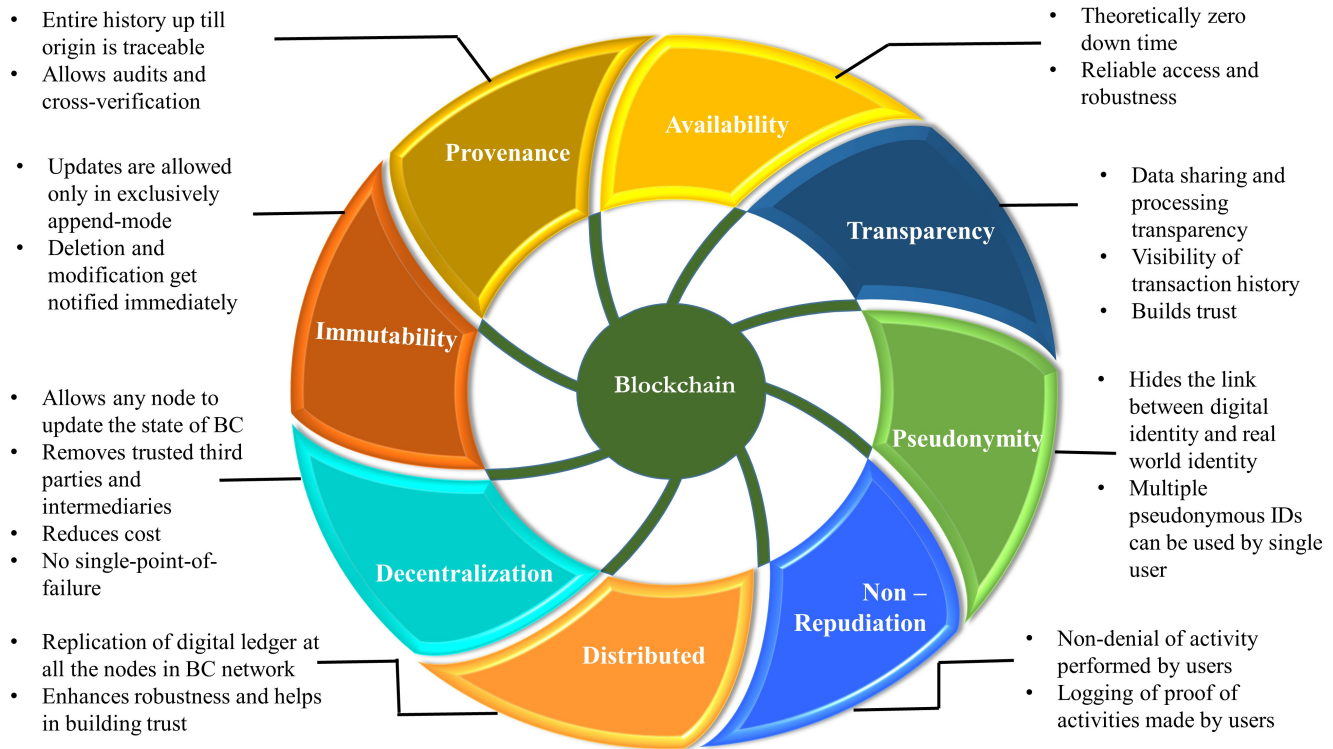


Fig. 6: Characteristics of Blockchain

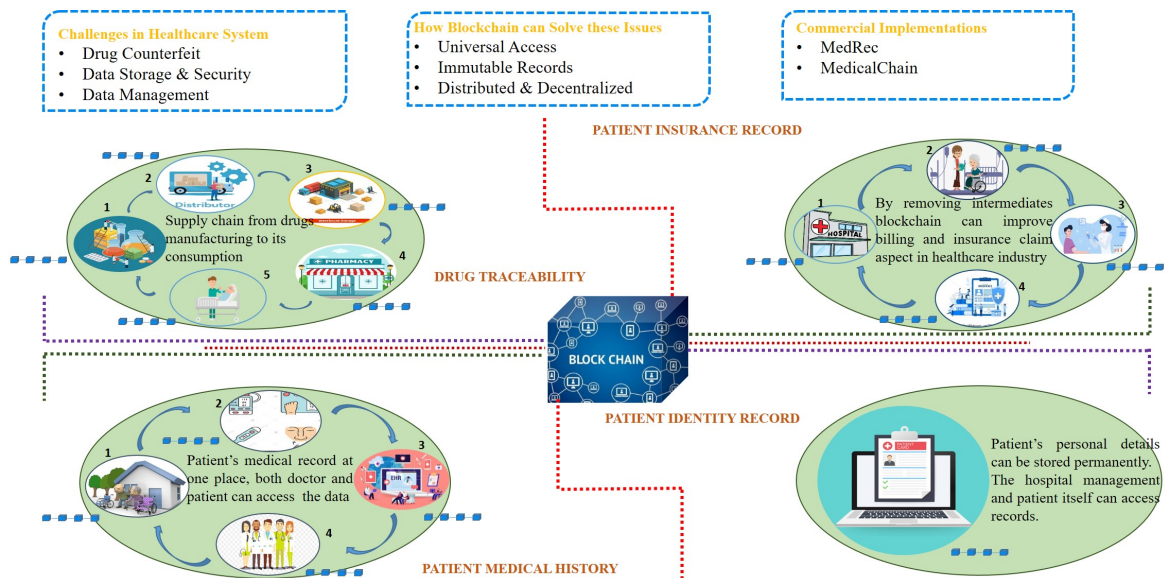


Fig. 7: Application of Blockchain in Healthcare [80]

With the increasing role of the healthcare ecosystem powered by advanced technologies, a tremendous amount of data is generated, which needs to be managed securely [83]. Some of the major issues being faced by the healthcare domain are user and location privacy leakage, counterfeit drugs and medical equipment, loss of ownership and fraudulent access to stored medical (personal) data, fraud in medical claims and bills, and secure platforms required for national and international collaboration of a team of healthcare professionals to deal with

critical cases and pandemic situations like COVID-19.

However, managing such a large massive amount of data is a challenging task but BC technology has the potential to mitigate these issues and provides a better solution than the traditional way of storing data. Blockchain because of its features such as distributed, decentralized, immutability, and availability, becomes the most suited solution to the problems being faced by the healthcare industry. For maintaining the privacy of patients' medical records, BC empowers patients to

have control over their medical data and can decide who can access their medical history [84]. Another issue with medical data (or history) is scattered storage. Usually, part of patients' medical data is stored with hospitals, some of other medical details are with the primary doctor, and some can be with the specialists. In this scenario, BC provides a solution to assemble all these data at one platform [85]. Counterfeit of medical drugs can also be resolved using BC technology, where the details of the drug supply chain from drug manufacturing to its supply to the patient can be updated on blockchain and the concerned authorities can keep an eye on every stage of the pharmaceutical supply chain [86]. Another challenge being faced by the healthcare sector is fraud in medical claims and billing. Sometimes healthcare providers claim charges for non-performed services, overcharging the actual services. Moreover, reimbursement of medical claims is usually a time-consuming process and is prone to fraudulent activities. BC can automate the medical claim's workflow where each person involved in the process can be made accountable for his/her activities and everyone sees the same information stored on BC [86]. Some of the commercial implementations in healthcare are MedRec, used for storing EHR efficiently and Medicalchain is used in the UK to maintain patient data [87]. Fig. 7, shows the application areas of BC in the healthcare domain.

1) Applications of Blockchain in Healthcare:

- **Electronic Health Records** - Storing data (patient's details, health information) digitally is called electronic health record. EHR are beneficial that they can be accessed from anywhere [100]. EHR contains sensitive information about patient's and it is important to maintain the privacy and security [101]. To maintain the medical records or history in unified manner, BC platforms can be instrumental. Along with maintaining the security and privacy of the data, EHRs can be stored and accessed easily [85]. Sharing of information is another important step and BC provides that sharing and trust mechanism [101].
- **Medicine Supply Chain** - Counterfeit of medicine is another major issue, that can adversely effect the lives of patients. BC can resolve this by storing all the details related to the drug supply chain, starting from manufacturing to the final supply of the medicine to the patient, on the BC network. The key steps involved in the supply chain of drugs are manufacturing, transportation, wholesaler, distributor, retailer, and patient [102]. All these entities can be registered on the BC platform and authorities can keep an eye to ensure the quality compliance [86].
- **Medical Claim** - Nowadays, we heard a lot about fraud by hospitals where they charge for non-performed services and overcharge the performed services [103]. As a chain of people involved in verifying the bills. A typical process of claim settlement involves a lot of communication between the concerned authorities which takes a lot of time and sometimes also includes fraud activities. BC can automate the workflow and each person involved in the process will share the same copy of the record, which ensures no changes in the copy of the bill [86]. Gem Health is one of the practical and real-

time systems for health claims [104].

2) *Related work:* The works related to healthcare have been discussed under different categories which are discussed as follows:

Authentication: Authors Saha et al. [92] and Alzubi et al. [94] have worked in the direction of proposing a BC-based approach for authentication and access control in healthcare. Saha et al. [92] highlighted the access control challenges in electronic health records and proposed a private BC technology-based access control approach that enhances features like security, and low computational and communication costs. Rather than using public or consortium BC, authors used private BC as all the data collected in hospitals using IoT-enabled devices is confidential and sensitive. Also authors showed that their proposed approach is resistant to various attacks like impersonation attacks, replay attacks, offline guessing attacks, man-in-the-middle attacks, ephemeral secret leakage attacks, and anonymity and untraceability attack. In their proposed access control scheme, the authors considered two tasks i.e. node authentication (all the newly enrolled users must authenticate themselves with hospital authority for authentic information) and key establishment (after authentication user can establish the shared key with hospital authority for future communications).

Moving forward Alzubi et al. [94] proposed a BC-enabled secured authentication technique for medical IoT devices using Lamport Merkle Digital Signature (LMDS). Their proposed approach is designed for securing the data transmitted between the patient and the hospital. It includes mainly four entities. The first entity records the sensitive medical data of patients obtained from MHEALTH, Second and third entity performs signature generation and verification using LMDSG and LMDSV respectively. The fourth entity is the centralized healthcare controller. Lamport Merkle Digital Signature generation (LMDSG) is used for authenticating i.e., (signature generation and verification) IoT devices. Authentication is done by creating a tree in which leaves represent a hash function of a patient's sensitive and confidential medical data. The root of LMDSG is calculated using Lamport Merkle Digital Signature verification (LMDSV) by a centralized healthcare controller (CHC) to preserve patients' confidential data from intruders. Verification is done when the hash of the public key is equal to the leaf then it becomes the root of the tree and the signature becomes valid. Authors analyzed the performance in terms of communication overhead (decreased by 20%), communication time (decreased by 17%), security (improved by 8%), authentication accuracy (increased by 8%), data confidentiality rate (improved by 9%), authentication time (improved by 11%) and privacy-preserving rate (increased by 7%).

Security:

Chen et al. [91], Tripathi et al. [81], Hemalatha et al. [93] and Zaabar et al. [96] have worked to improve security while storing medical data. Chen et al. [91] discussed the healthcare domain and the challenge it faces in storing health records such as no assurance of integrity and reliability of patient information, privacy leaks, centralized approach, and malicious tampering. Furthermore, the authors showcased the

TABLE VI: Summary of Related Work in BC-Healthcare

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Wang et al. [82]	Proposed a blockchain-powered parallel healthcare framework based on an Artificial system, Computational experiments, and Parallel execution, i.e., the APC approach. The prototypical system is developed for Gout disease and deployed at the hospital of Qingdao University, China.	Consortium blockchain is used to link patients, hospitals, and healthcare communities, a hash of the data is stored on-chain and the DPoS (Delegated Proof of Stake) consensus algorithm is used. Data sharing is done using BC-enabled smart contracts.	✓	✓	-	✓	-
Cyran et al. [88]	Proposed a blockchain-based approach to protecting sensitive health-related information and deploying BC across various hospitals.	Ethereum is used to deploy smart contracts with Docker containers, and various cryptographic techniques like Elliptic Curve Integrated Encryption (ECIS) for enhancing security. Along with this, Inter-Planetary File System (IPFS) is used to store large files to ensure minimum redundancy.	✓	✓	-	-	✓
Griggs et al. [89]	Proposed a BC-based smart contract for secure analysis and management of medical sensors. Their approach integrates WBAN and smart contracts over BC to create an immutable ledger of transactions. All the medical information is stored off the chain in the EHR database.	Private and consortium type blockchain is used to permit the authorized users to read the content on the blockchain and only a few selected nodes can run the smart contract and mine new blocks. Private BC is created using the Ethereum protocols and the PBFT consensus algorithm is used.	✓	✓	-	✓	✓
Carter et al. [90]	Proposed a framework by combining AWS with Ethereum BC for sharing information between the hospitals. BC helps in improving security and inter-operability between hospitals by allowing the complete sharing of data.	Ethereum public BC is used as it supports smart contracts. To overcome the storage scalability issue, off-chain AWS cloud storage is used. Uses AES-GCM with HMAC-based key derivation function HKDF, and 256-bit encryption key.	✓	-	-	-	-
Chen et al. [91]	Proposed a framework for sharing medical records that involve entities like a patient, service provider, and medical institution. Furthermore, a structure for the medical block with the header and body is presented.	Uses both BC and cloud storage. Information like store address, hash value, and permission of medical data are stored on the BC whereas data generated by medical institutions, and patient details are stored using the cloud under the chain. Suggested the use of the DPoS consensus algorithm.	✓	-	-	-	✓
Saha et al. [92]	Proposed an approach for access control to provide better security and requires low computational and communication costs.	Uses private BC and PBFT consensus algorithm for secure access control. Uses ECC for signature and SHA-256 algorithm for the secure collision-resistant hash function.	-	-	✓	-	-
Tripathi et al. [81]	Proposed a BC-based secured and smart healthcare system (S2HS) to provide better security, privacy, and integrity. Data captured using different sensors is encrypted using BC, and stored in a distributed approach and all the entities involved are connected using WSN.	Uses two-level of BC: Private BC is used to record internal entities like healthcare providers, clinicians, and inventory, whereas, public BC is used for external entities like patients, pharmacists, and insurance companies. Access to data is maintained using smart contracts.	-	✓	✓	✓	✓
Hemalatha et al. [93]	Proposed an IoT-based BC e-healthcare framework for storing and managing medical data.	Uses private BC with KSI to verify the data integrity. For comparison with the conventional system uses Apache JMeter and shows proposed approach takes less time.	-	✓	✓	-	✓
Alzubi et al. [94]	Proposed a BC-enabled approach to preserve medical data transmitted between patient and hospital using Lamport Merkle Digital Signature (LMDS). The proposed architecture includes four entities for sensitive data, signature generation, signature verification, and a centralized health controller.	Author evaluated the proposed approach using CloudSim 3.0. The proposed approach is analyzed in terms of computational overhead, computational time, authentication accuracy and time, data confidentiality rate, data integrity, and privacy-preserving rate.	✓	✓	✓	-	✓
Chen et al. [95]	Proposed a BC-driven framework for the detection of diabetes and a privacy server. The proposed framework includes three phases i.e., the registration phase, user authentication phase, and IoT data upload with the BC phase.	BC with IPFS for cloud storage is used for data storage. Uses smart contracts for the exchange of money and property.	✓	✓	-	-	✓
Zaabar et al. [96]	Proposed a BC-driven solution for secure healthcare data management and resolving centralized storage issues.	Uses Hyperledger fabric framework, access control list, and practical byzantine fault tolerance consensus algorithm.	✓	✓	✓	-	✓
Pandya et al. [97]	Discussed the use of FL in various domains and compare it with the traditional ML approach.	Author presented a detailed survey of FL in various domains along with related work done.	-	-	✓	-	✓
Belhadi et al. [98]	proposed an ensemble learning model for medical image segmentation by using a voting mechanism and blockchain technology and evaluated it in four different medical data sets.	Genetic algorithm is used to optimize hyper parameters along with blockchain technology.	✓	-	-	-	✓
Ch et al. [99]	proposed a cyber-physical system and blockchain-based smart healthcare system.	Bayesian grey filter-based convolution neural network (BGF-CNN), PSO, GWO optimization techniques, and blockchain are used.	✓	-	-	-	✓

opportunities offered by BC technology in the healthcare domain like patient control over the data, storage security, privacy, tamper-proof, and interoperability. For this authors have presented a scheme to store medical data using BC and compared it with the traditional approach in terms of tamper-proof, privacy protection, and secure storage.

In line with [91], Tripathi et al. [81] not only discussed the technical challenges such as data security, users' privacy, and lack of skilled manpower, but also highlighted social barriers

such as reluctance to adopt new technology, conventional and irrational mindset, and absence of core infrastructure, in the adoption of the smart healthcare system. To mitigate these issues authors proposed a BC-based framework for smart healthcare to attain the security and integrity of the data. BC allows privacy preserved and secure data exchange of patient data. Entities involved in Smart and secured healthcare system (S2HS) are mainly connected using a wireless sensor network (WSN). Entities involved are IoT-based wearable

TABLE VII: Summary of Related Work in BC-Smart Home

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Dorri et al. [105]	Proposed a lightweight and hierarchical architecture by cost-effectively implementing BC. In particular, smart homes, overlay networks, and cloud storage form the three tiers of architecture.	Smart home tier uses local BC and the overlay network tier uses public BC. The work has been analyzed against various attacks. Also, overhead analysis has been carried out.	✓	-	-	-	✓
Dorri et al. [106]	This work is the extension of [105] and includes three tiers namely smart home, cloud storage, and overlay network. The smart home tier consists of smart devices (centrally managed by miners).	To analyze the energy consumption, packet overhead, and time overhead author uses the Cooja simulator. The results show that these parameters witness an increase but are within manageable limits.	-	✓	✓	-	✓
Aung et al. [107]	Proposed architecture for smart homes to resolve issues related to privacy and security and for handling access control policy, data storage, and data flow management.	Uses Ethereum BC platform, with private BC, smart contract, and mining not required. For data storage, local storage is used.	-	-	-	-	✓
Zhou et al. [108]	Presented an overview of IoT, BC, and smart contracts and proposes BC-IoT and smart contract-based architecture for smart homes.	Uses public BC (for the peer-to-peer blockchain network to connect houses) and private BC (used in each smart home), smart contract. Also uses the Diffie Hellman algorithm for key sharing and the PoW consensus algorithm.	-	-	-	-	✓
Dang et al. [109]	Proposed a BC-IoT-based approach known as SHIB for mitigating security, privacy, and authentication challenges in the smart home.	Uses Ethereum blockchain, three types of smart contracts (ACC, JC, and RC) written in solidity language, Remix IDE software for writing and compiling smart contracts, and Ganache application. Also compared the proposed approach with existing other approaches.	✓	-	-	-	✓
Singh et al. [110]	Discussed the various challenges in IoT-enabled smart homes and proposes an architecture for a smart home known as SH-BlockCC. Proposed algorithms help in achieving network attack detection and response system in smart homes.	Uses cloud computing and blockchain technology, uses encryption and hashing algorithm for achieving confidentiality and integrity, availability is achieved by accepting transactions between devices and miners, authorization is done by policy header and shared key between devices and miner, and MCA detection algorithm is used for identifying the correlation between traffic.	✓	✓	✓	-	-
Arif et al. [111]	Talked about the security challenges being faced by smart homes and proposes a secure smart home framework using BC, to achieve better security.	Proposed framework uses consortium BC with PoW consensus algorithm and SHA-256 algorithm for mining and verifying transactions. Uses RESTfulAPI (Representational state transfer) for user authentication.	✓	✓	✓	-	✓
Ren et al. [112]	Proposed an IBPAS scheme to improve signature verification along with compressing the storage space and reducing the communication bandwidth. The proposed IBPAS scheme aggregates the signatures into one signature.	IBPAS scheme is evaluated using a simulated version of Bitcoin BC. The scheme is shown to perform efficiently in terms of storage space required, size of the blockchain, and energy consumption compared to other schemes.	-	✓	-	-	-
Yang et al. [113]	Proposed a BC-based approach for a trans-active energy management system in IoT-enabled smart homes to mitigate challenges like low efficiency and single point failure.	Uses Elliptic curve digital signature and distributed optimization algorithm, open access consortium BC and smart contracts, and modified form of PBFT consensus algorithm which includes leader selection algorithm and message aggregation scheme. And finally analyzed the performance and the results show that overall cost reduces by 25%. For evaluating BC-IoT, the author uses Quorum.	-	-	-	-	✓
Ammi et al. [114]	Proposed a BC-enabled approach to improve the security, integrity, confidentiality, and availability of the smart home.	Uses permissioned and private BC, hyperledger fabric, and hyperledger composer with cloud storage.	✓	✓	✓	-	✓
Qashlan et al. [115]	Proposed an authentication scheme for preserving the privacy of data collected and shared.	Uses private Ethereum BC with two smart contracts i.e., register and access contract with PoW consensus algorithm. Along with these, uses attribute-based access control, differential privacy, and edge computing.	✓	✓	✓	-	✓
Baucus et al. [116]	Proposed a low-end BC-enabled approach to enhance the security of smart homes.	Uses private blockchain and localization to gain more information about the source of the attack. Also, the Kalman filter is used to increase the accuracy.	-	-	-	-	-
Liao et al. [117]	Proposed a BC-driven approach with different cloud service combinations to achieve a secured and controlled smart home. Furthermore, simulation results show that the proposed approach has better access control.	Uses Hyperledger fabric with Elliptic curve cryptography and attribute-based access control algorithm.	✓	-	-	-	✓

devices, EHR, encryption/decryption and standardization, BC mechanism, and end-users. Their proposed approach uses two-level of BC i.e. private and public BC to provide isolation among the entities involved and helps in achieving consistent and transparent workflow. Taking forward the same issue, in 2021, author Hemalatha et al. [93] highlighted the challenges

in a traditional approach like a single point of failure, mistrust, data manipulation, and tampering, and how BC can resolve these issues. To resolve such issues, the authors proposed a BC-IoT-based approach to protect and save storage of the medical data. Their approach suggested using private BC as it is more stable and provides stronger authentication processing.

BC with KSI (public key infrastructure strategies) is used to verify data integrity and Merkle root hash is used to validate the timestamp. To test the performance of the proposed framework, the authors used Apache JMeter and showed that the proposed approach takes less time than the current system. Along with that, in 2021, Zaabar et al. [96] proposed a Hyperledger fabric BC, based approach for the secured management of healthcare data and resolves the storage issues of a centralized system. For storage of data, the decentralized database OrbitDB with IPFS, as an off-chain database is used. For communication HTTP and CoAP (constrained application protocol) are used. In particular, six layers are there; IoT physical layer, connectivity layer, off-chain database layer, BC network layer, application layer, and users layer. Moreover, analysis was done in terms of data integrity, confidentiality, availability, traceability, and data privacy. Pandya et al. [97] discussed that federated learning is a cost-effective and promising solution to healthcare incorporating privacy, as it utilizes a distributed AI approach to receive local updates from various medical devices, such as the Internet of Medical Things (IoMT) devices so that local data does not have to be accessed directly, which helps in preserving privacy leaks. Ch, Rupa et al. [99] proposed a cyber-physical system and blockchain-based smart healthcare system. Bayesian grey filter-based convolution neural network (BGF-CNN), PSO, and GWO optimization techniques are used. Moreover, Blockchain with CPS is used to enhance security. In particular, accuracy and time complexity are improved.

Real Time Monitoring: In 2018, Wang et al. [82] and Griggs et al. [89] both worked in the same direction and propose approach for real-time monitoring of the patient. Wang et al. [82] used an artificial system, computational experiments, and parallel execution in combination with BC technology to link patients, hospitals, and healthcare communities for sharing of health records. Further, the authors developed a blockchain-based system using consortium type BC to deal with the specific case of Gout disease. For data storage, the hash of the data is stored on the blockchain, and for generating the consensus among the nodes, used Delegated proof of stake (DPoS) consensus algorithm. DPoS allows nodes to elect some number of trustees called delegates, who can collect transactions turn by turn and bundle them in a block. The remaining nodes verify the block and add it to the BC. Data sharing and record review are performed using BC-enabled smart contracts. Here health bureaus serve as the audit nodes to ensure integrity. While Griggs et al. [89] proposed an approach for automated remote patient monitoring, by sending notifications to the patient and medical professionals along with a record of who has initiated the activity. All the sensitive medical information will not be stored on the BC but stored using an EHR storage database instead only the fact that the event occurred is stored on the BC. The logs about measurements and treatments are also stored on the blockchain along with smart contracts. Authors used a smart contract (written using solidity language) for automatic analysis of health data collected and trigger alerts for unusual activity. The authors proposed a DApp to manage the user interface. Furthermore, their work presented a comparison of the proposed approach with the traditional

approach in numerous aspects like confidentiality, availability, immutability, traceability, speed, privacy, and transparency. In line with that in 2021, Chen et al. [95] presented an IPFS and BC-enabled framework for the detection of diabetes in a very secure way. In particular have three phases i.e., registration phase, user authentication phase, and IoT data upload with BC phase. It uses IPFS for storage and smart contract for the exchange of money in a transparent way. Moreover, the authors presented the performance evaluation of their proposed approach in terms of accountability, block capacity, and processing time of transaction.

Data Sharing: Cyran et al. [88] and Carter et al. [90] worked to improve the data sharing between hospitals and patients. Cyran et al. [88] highlighted the challenges in the current centralized system like meeting the scale, accessibility, and security requirements of healthcare organizations, and suggested BC as a promising solution for addressing these challenges. Authors proposed a BC-based solution for protecting sensitive health-related information and deployment of BC across various hospitals at large scale. For the deployment of BC across the hospital authors built a containerized solution. The proposed approach includes the owner for each piece of data and has the right to decide what amount of data can be accessed by whom at varying levels. Moreover, the proposed system enables the data owner to revoke access to the data and ensures that the receiver's private key with data is not sufficient to access data. While in 2019, Carter et al. [90] discussed the interoperability challenge, in sharing data. To resolve this challenge, the authors have suggested an approach using the Amazon web service and Ethereum BC. The proposed approach uses AWS cloud service, information related to patient health identifiers such as Data of Birth (DoB), name, and address are not stored on public BC but stored using AWS cloud storage as AWS is highly customizable and provides security in sharing health data digitally. Belhadi et al. [98] proposed an ensemble learning model for medical image segmentation, for which a voting mechanism is used. To secure the learning process blockchain technology is used. The paper highlights the advantages of blockchain-enabled IoMT. Moreover, the author evaluated the framework IoMT in four different medical datasets.

Table VI, lists out the work done in integrating BC-Health care.

3) **Summary:** Healthcare is a platform where concerned professionals take care of various diseases and cure patients. By introducing smart healthcare systems, society will be benefited in terms of public healthcare management, online access, medical data sharing, availability of data, no central node dependency, and a patient-centric system. Nonetheless, the existing system has a few lacking areas such as lack of trust, scattered data, centralized approach, security, and privacy. By the application of BC, these challenges can be resolved in terms of accuracy, global health data sharing, irreversible transactions, distributed and decentralized storage, transparency, no third-party involvement, and authorized access. All these features will help in improving the overall functioning of the healthcare ecosystem and enable various stakeholders to securely access complete medical history which is generally scattered among

different hospitals and medical institutions. Numerous research works have been carried out to explore the applicability of BC in the healthcare domain. In particular, researchers have made efforts to enhance authentication and access control of medical data using digital signatures, node authenticity, and improved key establishment. To enhance security hierarchical BC, public key infrastructure strategies, and private type BC are used. Furthermore, off-chain (cloud) data storage, consortium type BC, and DPoS consensus algorithm have been suggested for real-time monitoring and data sharing with revocability.

Few points that need attention for widespread adoption of BC in healthcare are better infrastructure and interconnection for easy adoption, secured data sharing among hospitals in a more cost controllable manner, and more implementation options can be explored with hyperledger, a medical BC network connecting as many health organizations, the privacy of patient's can be improvised by adding anonymous identity. Moreover, parallel healthcare systems can be improved and used for other diseases also other than Gout disease. Apart from these, a BC-based interoperable electronic health record-sharing framework can also be implemented using faster-distributed ledger technologies with identity management of patients. Although there are numerous benefits of using BC and smart contracts in the healthcare domain, there exist some challenges such as scalability, immense data management, Interoperability, and a large number of concurrent users. Moreover, some of the operational aspects that need attention for the widespread adoption of BC in healthcare are awareness among the users, standardization, lack of trust among hospitals and patients to share their medical details, and onboarding of various medical organizations over BC-based platforms.

B. Smart Homes

A smart home is an IoT-enabled home that improves the quality of life of the members of the home by providing them automation, security, comfort, and convenience and allowing them to control the gadgets installed in the house using a mobile application [118]. In simple words, smart home enables automation of daily routine tasks with the help of gadgets or devices installed in a house [42]. For a home to be a smart home, it must-have network connectivity, IoT devices, and a mobile application to access and control devices from anywhere [118]. Smart home adoption rate is continuously growing at a rate of 20.8 % from the year 2018 to 2022 [119]. The global market for smart meters and home automation will grow to \$44 billion by 2025 [120]. Some facets of a smart home are smart door locks, smart lighting, smart parking, and video surveillance [118]. The key challenges faced by smart home applications are security (such as authorization, authentication, access control), privacy (data and user), and system configuration security [119] [111]. Another challenge is IoT devices have limited memory and power. Moreover, conventional IoT systems are centralized and a single point of failure can occur. To resolve these challenges BC is the most suitable and promising solution [111]. A private blockchain can be used to manage the communication among devices and these communications can be recorded as transactions on the

BC [84]. Fig. 8, shows the application areas of BC in the smart home.

1) *Applications of Blockchain in Smart Homes:* A smart home consists of IoT-enabled devices (smart devices) and mobile applications for remote access. These IoT-enabled devices need to communicate with each other. For example, when someone enters the home, the light should automatically turn on; for this, the lamp needs to receive signals from the motion sensor [84]. The BC technology enables secure communication among smart devices installed inside the smart home, and each device can request data from other devices instantly [122]. Communication between these devices are considered as transactions and private BC is used to keep the track of these transactions which are immutably stored in the BC ledger. Miners, installed in the smart home, are devices that process all incoming and outgoing transactions to and from the devices in smart home [106].

- **Security and Privacy** - IoT enabled smart homes generate and exchange lot of personal data between the installed devices [106]. Use of heterogeneous IoT devices used in smart home creates security, privacy and authentication challenges. Existing security frameworks to overcome these challenges are mostly centralised along with noisy and incomplete data and thus are not well suited for IoT enabled smart home [109], [111]. BC with its strong security, pseudonymity, distributed and decentralised nature has potential to resolve these challenges in unified manner.
- **Data Storage** - Smart home is a collection of various physical devices, connected to internet, sharing data continuously [108]. Data being generated by IoT enabled smart home can be very large. The data storage by IoT devices does not meet users security requirements because of low capacity, multiple connectivity to the internet and heterogeneity [123]. For which BC can play a vital role in data storage along with maintaining privacy and security [112].

2) *Related work:* The research works related to smart homes have been discussed under different categories which are discussed as follows:

Privacy & Security: Dorri et al. [105], Aung et al. [107], Dorri et al. [106], Dang et al. [109], Singh et al. [110] and Arif et al. [111] worked to improve privacy and security in IoT-enabled smart home. In 2016, Dorri et al. [105] proposed a lightweight architecture using BC technology by removing all the extra overheads of BC but at the same time, it maintains most of the security and privacy benefits of BC. The proposed architecture is hierarchical and includes three tiers; smart home, overlay network, and cloud storage. The first-tier smart home has local BC. Some key attributes of local BC are it is always mined by a device that is always online and high processing, managed by its owner (responsible for adding or removing devices), and the block is mined and added to the chain without solving PoW consensus algorithm which helps in reducing extra overheads of BC. Second-tier uses an overlay network which is the same as a peer-to-peer network that uses public BC. The nodes (home miner, devices, user's smartphone) present in the network use Tor for connecting to

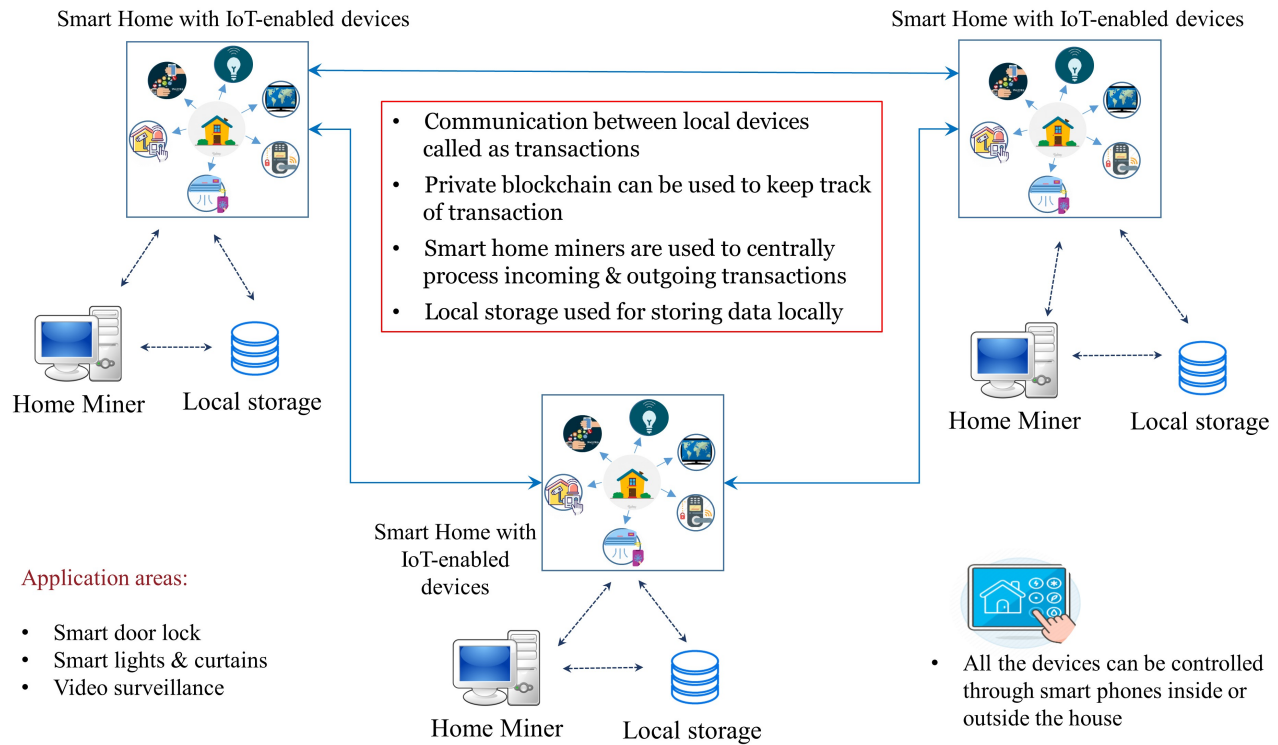


Fig. 8: Application of Blockchain in Smart Home [108] [119] [121]

the overlay network to add extra anonymity to the network. If the user has more than one smart home then they can use shared BC; this can lead to forking in shared BC as each device present in the network can decide whether to keep the block or not. To resolve this, devices maintain a table containing the block number and hash of the data for the last transaction. The proposed architecture is especially for storing and accessing data use cases. At last, the author has evaluated the overhead and performance of the proposed architecture and shown that it has constant performance.

In 2017, Aung et al. [107] discussed about the security and privacy issue in IoT-enabled smart homes and suggested an approach of integrating BC with IoT to resolve these issues. The author suggested using the Ethereum BC platform and proposed an architecture that consists of a smart home miner (device to maintain private BC), private BC (to store the policies set up by the homeowner or for managing transactions), and local storage. Managing transactions means either storing, accessing, or monitoring transactions. But before managing these transactions private BC needs to check the policies set up by the homeowner means which sensors can store data, who can monitor the data and the only homeowner can change smart contract policies. For managing all these activities smart contracts are used and computationally intensive mining is not required, which means no need for modern hardware with high-processing CPUs. In 2017, Dorri et al. [106] proposed an architecture to extend its previous work [105]. The proposed architecture includes three tiers same as in [105]. Smart homes are connected using shared overlays and groups of

these overlays are termed clusters, where each cluster chooses a Cluster Head (CH) which are connected using public BC with two key lists PK requester (list of overlay users' PK) and PK requestee (list of PKs of smart homes connected to the cluster). Authors considered four different components in their proposed BC and IoT enabled smart home: transaction (communication between local devices), local BC (private BC to keep a record of transactions), home miner (device that process incoming and outgoing transactions), and local storage (a backup device used by smart devices to store data locally in FIFO order). Finally, the author evaluated the performance by using the Cooja simulator in terms of packet overhead, time overhead, and energy consumption. The evaluation results show little increase but are manageable and security is analyzed in terms of confidentiality, integrity, and availability against DDOS attacks and linking attacks.

In 2018, Dang et al. [109] proposed a BC-IoT-based architecture for smart homes (termed as SHIB - smart home IoT BC) to resolve the security and privacy issues. Authors designed three smart contracts: ACC (access control contract for registering, updating, or deleting access control method), JC (judge contract for updating the misbehavior judging method), and RC (register contract for updating or deleting policy of ACC). Also, it has the facility of adding or removing IoT devices just by adding or deleting respective smart contracts (only the owner can perform this activity). The proposed SHIB architecture mainly includes a service provider (a device that interacts between IoT devices and storage devices), a storage device (devices for storing the collected data), the user (owner

of a smart home), and a smart home (home where IoT devices are installed). At last, the author presented the comparison between the proposed and existing architecture using terms of smart contract, the privacy of data, usage of tokens, updating policies, and judging the misbehavior. Moving ahead in 2019, Singh et al. [110] present a blockchain and cloud computing-based smart home architecture known as SH-BlockCC. For analyzing network traffic proposed architecture uses MCA (multivariate correlation analysis). Their proposed architecture includes a smart home layer, blockchain layer, cloud computing, and service layer. Authors also discussed the challenges being faced by the smart home such as security and privacy, scalability and access control, availability and reliability, and confidentiality and integrity. Furthermore, authors talked about numerous services provided by the smart home such as remote controlling lights, fuel/smoke leakage, trapped in a bathroom, smart refrigerators, security alarms, and measures of important health signs. Their approach uses ZigBee technology. Finally evaluated the performance across various parameters like confidentiality, integrity, availability, authentication, and privacy using Cooja and Ns-3 simulator and the result shows SH-BlockCC covers all these security aspects.

Next in 2020, Arif et al. [111] described various security issues because of limited storage and processing power and suggested BC as the most promising solution. The authors proposed architecture using consortium BC. As public BC is an open network and scalability is an issue, the author prefers to use consortium BC with PoW consensus algorithm and SHA-256 algorithm for mining and transaction verification. Fundamental building blocks are sensor node (for communicating with supernodes; responsible for transaction verification), supernode (peer-to-peer server as well as storage for BC ledger; responsible for transaction management and blockchain storage), blockchain (uses PoW mechanism), and user (admin user and general user; users are authorized by RESTful API). In line with that, in 2021, Ammi et al. [114] and Qashlan et al. [115] worked to improve the privacy and security of smart homes. Ammi et al. [114] proposed an approach for a secure smart home by using BC and improved some of the features like privacy, integrity, availability, and confidentiality. The proposed approach has four layers; cloud storage, hyperledger fabric, hyperledger composer, and smart home layer. On the other side, Qashlan et al. [115] proposed an approach by combining attribute-based access control with smart contracts and edge computing to resolve the security and privacy-related challenges while data collection and sharing. In particular have four users; end-user, IoT devices, smart home multi-edge servers, and the cloud. Their proposed approach is shown to be resilient against DoS attacks, data mining, modification, and linkage attack. Moreover, authors performed the analysis in terms of block size, gas cost, and time cost to determine the feasibility and efficiency of the proposed approach. In 2022, Liao et al. [117] proposed an approach by combining numerous cloud services for secure access control and a hyperledger fabric alliance chain. In particular, uses an elliptic curve cryptography algorithm. Simulation results show that the proposed approach has a better access control scheme.

Transactive Energy Management: Yang et al. [113]

proposed a BC-based approach for transactive energy management in smart homes to resolve the challenges being faced by conventional methods such as low efficiency, lack of privacy, and single point of failure. It uses open access consortium BC with smart contracts for energy management and payment in a decentralized manner; an elliptic curve digital signature and distributed optimization algorithm for faster processing and small transactions. The authors discussed three reasons to use BC; no need for any central authority, secure data communication at low cost, and easy payment option. The proposed approach is presented in three steps; the first smart home model includes the load and generation, the second transactive energy management system is introduced, and finally, the design of the BC used. The author modified the PBFT consensus algorithm and included a leader selection algorithm and message aggregation scheme which helps in saving the network bandwidth and increases the speed of the consensus process. For leader selection algorithm uses a round-robin leader selection algorithm and secondly, messages collected by the leader elected are aggregated in a single confirmation message to others in prepare and commit phase, which saves the network bandwidth and speeds up the consensus process. The authors also analyzed the performance using a systematic test on a realistic network of IoT devices and numerical simulation with data collected and the results show that overall cost reduces by 25%. For evaluating BC-IoT, uses Quorum as Quorum is a modified form of Ethereum and it modified the PoW algorithm of Ethereum into the PBFT algorithm.

Storage & Computation: Zhou et al. [108] and Ren et al. [112] worked in the same direction to resolve the storage challenge in IoT-enabled smart homes. Zhou et al. [108] proposed a BC-IoT-based architecture with a smart contract. The architecture includes a smart contract (present in each smart home), private BC (local BC in each smart home), and public BC (peer-to-peer BC network to connect the houses). Core components included are: transactions, smart contract, local storage (data is uploaded to the local miner every 10 days due to storage limitations), security (CIA: confidentiality, integrity, and availability), and registration service (IoT devices need to be registered in a distributed ledger). Taking forward, in 2021, Ren et al. [112] discussed the challenges faced by the smart home such as unauthorized access and tampering with data. Security challenges other than these are information disclosure, illegal user invasion, and equipment failure. To mitigate these issues author proposed an identity-based proxy aggregate signature (IBPAS) for improving signature verification, compressing storage space, and reducing communication bandwidth. IBPAS consists of six elements: Setup, Key-Gen, Delegation, Proxy-Sign, Aggregate, and Verify. IBPAS is used to make sure data is viewed by only the home admin and BC storage space is compressed. Their proposed scheme uses an edge network center to manage smart devices. The administrator generates a proxy signature for each block and then aggregates all to obtain the final signature. Then cloud server sends the final signature to the BC. Finally, the author analyzed the IBPAS with existing aggregate signature schemes and shows that IBPAS has better in terms of communication energy consumption and reduces storage space as various

signatures are aggregated into one.

Device Monitoring: Baucas et al. [116] proposed an approach to monitor IoT-enabled devices in smart homes to reinforce security. In particular uses private BC, to find unrecognized devices and localization, to gain more information about the source of an attack, and the Kalman filter is used to increase the accuracy. Furthermore, analysis shows that private BC with WiFi is the most consistent choice.

Table VII summarises the work done for BC and IoT-based smart homes.

3) **Summary:** The smart home aims to provide its residents with convenience, comfort and reduces efforts, and helps in managing, monitoring, controlling, and scheduling tasks with just one click i.e., remote monitoring systems and automation. For home automation, devices must be connected to the internet which leads to IoT-enabled smart homes. The existing IoTized smart home approach faces challenges such as the risk of cyber-attacks, threats to personal data privacy and confidentiality, unauthorized access control, and centralized architecture. The application of BC for IoT-driven smart homes can help in mitigating these issues. BC offers distributed, decentralized, and irreversible transactions, which means as new data arrives, the consensus is established among the nodes to validate it and a copy of the ledger is updated at each node. Several research works have been carried out to explore the capability of BC in IoT-enabled smart homes. Authors worked in numerous directions like privacy and security, energy management, and storage and computation. For privacy and security, both public and private BC along with smart contracts, ZigBee technology, consensus algorithms (such as PoW and PBFT), and elliptic curve digital signature are used. For storage and computation, private BC with cloud storage is preferred and implemented using the cooja simulator. Whereas, for energy management, consortium BC, smart contracts, elliptic curve digital signature, and PBFT consensus is used. Despite the benefits offered by BC-powered IoT-enabled smart homes, there exist many challenges. Some of them are large energy consumption due to inherent computation required in BC, scalability issues in terms of connected devices and a large amount of data generated, and interoperability issues. IoT-enabled smart home involves heterogeneous devices with different operating systems which makes communication and onboarding on the same platform difficult. Hence, there are some areas which need more focus from future prospectus are reduction in computational complexity of decentralized algorithms, increased throughput, and interoperability.

C. Smart Cities

A smart city offers higher quality of life to residents, maximum utilization of resources, and brings transparency in governance. Smart cities are built by connecting and integrating their systems and infrastructures using communication technologies, which work collectively to generate intelligent information [124], [125]. According to a report, 86% of developed countries and 64% of the developing countries will be urbanized by 2050 [126]. According to the United Nations report, 55% of the global population lives in urban

areas presently, which is 30% in 1950 and this will reach up to 68% by 2050 [125]. With the increasing number of people moving from villages to cities, city planners and municipal governments are facing difficulties. As a result, challenges such as traffic congestion, air pollution, greenhouse gas emission, and waste disposal are affecting the quality of life of citizens [84]. Thus, smart cities intends bring many advantages such as effective management of traffic, improved health, education, energy services, transparency in government sectors, and involvement of citizens [84].

Application areas of the smart city where BC can have an impact are education, identity management, land registration, energy and waste management, public utilities, and intelligent government services [124]. Challenges in implementing such systems also exist such as accuracy, uniformity, completeness, and timeliness. Many of the issues can be resolved by using BC technology and its features like immutability, provenance, and availability. Fig. 9, shows some of the application areas of BC in smart cities. Some of the global BC initiatives in the government and public sector as discussed in [124] and are summarized below:

- Government of Estonia has its own BC solution known as KSI to integrate and maintain national e-health records.
- Government of Dubai has partnered with IBM and Consensus, to enable all transactions on BC and termed Smart Dubai.

1) Applications of Blockchain in Smart Cities:

- **Smart Governance** - Government spends some portion of its annual budget on social welfare schemes for poor, sick, elder, and underprivileged citizens. However, due to the lack of proper system such facilities can be misused. Individuals can create multiple copies of their identities and submit them before the authorities, which causes inefficiency and corruption in the system. To avoid such situations, BC can be used to make the system more transparent and traceable [124]. Also, BC can be used to implement voting system for citizens from the comfort of their homes, where citizens' identity can be verified using BC [127]. Thus, BC-enabled smart digital governance approaches can pave the way for improved public administration, improved service deliveries, enhanced transparency and accountability [128].
- **Agriculture** - Price extortion, higher prices, the presence of a middleman, quality of food, and manipulations in expiry dates are some of the open challenges being faced by the agriculture domain. The agricultural food supply chain includes farmers, agents, transportation, wholesaler, shopkeepers, and consumers, all can be connected in a trustless manner using BC. Moreover, BC provides end-to-end visibility and allows tracing the origin of the product and gives a secure, transparent, and efficient supply chain [124]. Thus, for building resilient, secure, transparent, and trustworthy agricultural food supply chain BC has been considered as a vital technology [129].
- **Smart Education** - To implement BC in the education domain, BC can be used where multiple educational institutes, teaches and students can join to manage and

access the records such as student details, migration from one institute to another, course or degree completed along with the transcripts [84], [130]. Moreover, BC can be used to store the learning activities of students across different organizations [131]. In future, with the increasing online mode of education, BC is expected to contribute towards decentralized and secure education ecosystem.

- **Digital Identity** - Blockchain provides a platform where the identities of the citizens can be stored digitally and can be accessed by citizens from anywhere. One example of a practical application of digital identities is the Estonian e-Residency program which enables users to create a Digital Identity [132].

2) *Related work*: The research works related to smart cities have been discussed under different categories which are discussed as follows:

Security & Privacy: Biswas et al. [133], Sharma et al. [126], Rahman et al. [134], Zhang et al. [135] and Kumar et al. [136] all of them worked to achieve better security and privacy in a trustworthy manner in IoT enabled smart cities. Authors Biswas et al. [133] proposed a framework by integrating BC with smart devices installed in smart cities for secure communication. Also identified the major threats to smart cities such as threats to availability, integrity, confidentiality, authenticity, and accountability, and discussed various key attributes provided by BC such as improved reliability and better fault tolerance capability. For achieving security, the proposed framework includes mainly four layers; the physical layer (which includes sensors and actuators), the communication layer (which includes various communication mechanisms such as Bluetooth, WiFi, Ethernet, and 6LoW-PAN), the database layer (which includes distributed ledgers and suggested to use private ledgers to ensure scalability, performance, and security) and interface layer (includes various smart applications).

In 2018, Sharma et al. [126] proposed architecture for a smart city by integrating a software-defined network(SDN) with BC. The proposed architecture includes a core (miner nodes with high computation and storage resources) and edge network (limited storage and computation power), due to which it inherits properties of both centralized and distributed networks. Miner nodes are responsible for block creation and verifying PoW. For maintaining the integrity of the data, digital signatures and hashing (Argon2-based hashing) are used. Includes memory-hardened PoW scheme called "Itsuku PoW" and helps in resolving issues such as a raw re-computation attack, memory saving, pseudo-random array, parallel searches, and hash composability attack. To set up a private BC network it uses Go Ethereum. Finally, the performance is analyzed in terms of hash rate (continuously adjusted according to the difficulty) and block size (number of transactions for variable block size) which shows that the proposed system attains better performance. Also evaluated was the performance overhead of the proposed system in terms of latency and throughput.

Authors Rahman et al. [134] proposed a BC-based infrastructure to provide security and privacy-oriented smart contract service for IoT-enabled economy in smart cities. Smart contracts offer Spatio-temporal service at a global

level without a central authority. For system, implementation authors have taken the example of Hajj as a massive crowded area. In 2020, Zhang et al. [135] worked to achieve higher data accuracy and to reduce the possibility of data being stolen. For this reason, they have proposed an LDC (Lightweight data consensus) algorithm based on BC, to be used in smart cities and presented a comparison with the traditional approach.

After that in 2021, authors Kumar et al. [136] presented a framework for smart cities named trustworthy privacy-preserving secured framework (TP2SF). It includes three modules; trustworthiness, two-level privacy, and intrusion detection module. The trustworthiness module uses an address-based BC reputation system to ensure that recorded data is authentic. In the two-level privacy module, the first level is used for authenticating data processing by using the SHA-512 hashing algorithm and enhanced proof of work consensus algorithm, and the second level is used for data transformation and generation, and original data was transformed into another format by using PCA based privacy preservation (feature mapping, selection, normalization, and transformation). The proposed approach is deployed using IPFS-based off-chain CloudBlock and BC-enabled on-chain FogBlock. The authors analyzed the framework in terms of accuracy, detection rate, F1 score, and precision score using two IoT datasets called BoT-IoT and ToN-IoT. Experiments are performed using R, Python language, and the machine learning algorithm SciKit-learn. The framework is implemented using Ethereum, smart contracts written in solidity language, and IPFS.

Trustworthiness: Khan et al. [137] highlighted the importance of video surveillance in cities to keep an eye on the activities happening in the city and presents a BC-based system to store the recordings of the video to ensure the trustworthiness of the recordings and will help in differentiating between the fake videos and the original video cost-effectively. In particular, it includes six participants; a control room manager (CRM): To ensure the operator operates all devices, control room supervisors (CRS): who manage all devices in line, operators: who perform proactive and reactive surveillance, police officers (POs): manages police radio, police control room operators (PCROs): communicates CCTV command room operatives and local authority staff (LAS): manages police radio to communicate CCTV command room.

Data Sharing: Cha et al. [138] discussed the challenges being faced during public cloud storage and how BC and secret sharing can resolve the personal information sharing issue. The authors also highlighted the advantages provided by the proposed system such as a large amount of data can be stored on an external cloud service provider (CSP), resolving privacy issues that occur in CSP, and data can be restored and verified for integrity. The proposed architecture uses consortium BC and a secret sharing algorithm for managing user data from CSPs. The proposed approach includes mainly five steps; data gathering, processing, data transaction, secret sharing, and data reconstruction. Moreover, compared and analyzed the proposed system in terms of the AES-128 encryption algorithm and the execution speed. Along with this also discussed how it provides security in the smart city use case.

Energy Management: Khattak et al. [139] proposed a BC-

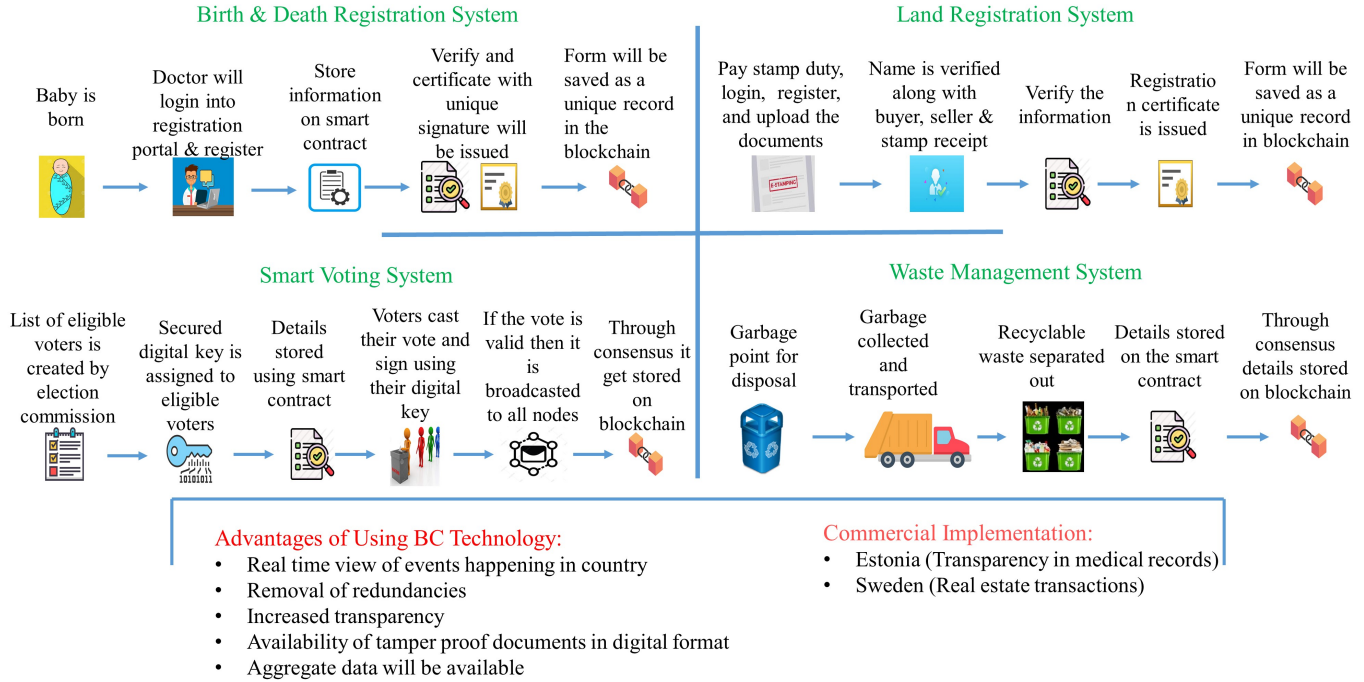


Fig. 9: Application of Blockchain in Smart Cities [84], [124]

based application for the automatic exchange of electricity between residents. The price is calculated by the admin (legal centralized authority). The author has highlighted the application of BC in managing energy in smart cities. Discussed the automatic bidding of supply and demand for energy. In particular, uses a hyper-ledger fabric framework for maintaining privacy and confidentiality as participants are directly affiliated with an exchange of electricity and money, and the ledger is updated and notified.

Authentication & Authorization: Esposito et al. [140] and Ferreira et al. [141] worked in the same direction to enhance the authentication and authorization in smart cities. Esposito et al. [140] highlighted that existing smart city applications are a combination of different existing applications where each application has its own set of privacy policies which leads to the challenges such as consistent and secure data replicas. To resolve this issue author proposes a BC-based approach-integrating it into the FIWARE platform for distributed management of identity and authorization policies with a global view of policies within the system. In the proposed work permissioned BC platform Hyperledger Fabric is used to maintain the consistency between the repositories holding security policies and the Kafka-based consensus algorithm. Smart contract chain code is used for registration, query, and modification of identity information. In addition to this, the proposed approach is evaluated in comparison to the existing approach. On the other side, Ferreira et al. [141] proposed an approach to improve the registration and authentication of IoT devices in smart city applications. In particular, the

authors developed API gateways and network gateways to identify and authorize messages. Authors have proposed HTTP API gateways, edge computing, network gateways, and fog computing. Smart contracts are responsible for registering IoT devices and associating them with their respective owners.

Table VIII, summarises the work done in the BC-smart city use case.

3) **Summary:** Smart city paves the foundation for global urbanization where emerging technologies are used to offer its citizens effortless services such as smart transportation, smart governance, smart healthcare, and smart education. To provide such services the role of IoT is considered to be significant. Despite the numerous advantages of IoT-based smart cities, it faces some challenges like privacy, security, centralization, and denial of service that are preventing faster adaptation of smart cities. These challenges can be resolved by combining BC with IoT-smart homes. BC offers irreversible transactions, distributed and decentralized architecture, and non-repudiation, to its users. Integrating BC with a smart city offers lower administrative costs, reduces corruption, and provides a platform for integrated documents. Authors have worked in numerous directions i.e., security and privacy, data sharing, trustworthiness, energy management, and authorization. For data sharing authors have used external cloud storage, consortium BC with a secret sharing algorithm. While for energy management and authentication & authorization, permissioned BC platform hyper ledger fabric was used. On the other side, authors preferred private BC with a PoW consensus algorithm, digital signatures, hashing, and smart contracts to

TABLE VIII: Summary of Related Work in BC-Smart City

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Biswas et al. [133]	Proposed a security framework for a smart city by integrating BC with smart devices for secure communication.	Uses the Ethereum platform which provides smart contract functionalities, suggested to use of private ledgers to ensure scalability, performance, and security for real-time applications.	-	-	-	✓	✓
Sharma et al. [126]	Presented a new approach for smart city, integrating software-defined networking and BC technologies and offering low latency and real-time processing.	Uses a private Ethereum BC network, memory-hardened PoW scheme called Itsuku PoW, and Argon2 hashing technique. Also, analyze the performance in terms of hash rate and block size.	✓	✓	-	-	✓
Rahman et al. [134]	Put forward a BC-based infrastructure to provide security and privacy-protected smart contracts for IoT-enabled sharing services in smart cities.	Uses permissioned private Ethereum and Hyperledger BC with IPFS as off-chain solutions, MEC, and AI. Along with this uses the Amazon AWS platform and SHA 256 hashing algorithm.	✓	✓	-	-	✓
Khan et al. [137]	Proposed a BC-based approach to ensure that the stored recordings are genuine and help in differentiating between original and fake videos.	Uses Hyperledger Fabric, private BC. No consensus algorithm is used, instead, validation peers are nominated by the admin for validation purposes.	✓	✓	-	-	✓
Khattak et al. [139]	Suggested an intelligent BC-based application for energy management in smart cities.	Uses open source BC i.e. hyperledger fabric framework, cloud for permanent data storage, and smart contract to make sure that transaction is valid.	✓	✓	✓	-	✓
Zhang et al. [135]	Presented a lightweight data consensus algorithm based on BC technology for secure transmission in IoT for smart cities.	Uses proposed lightweight data blocks consensus algorithm.	-	-	-	-	✓
Kumar et al. [136]	Proposed a BC and machine learning-enabled framework for smart cities named as trustworthy privacy preserving secured framework (TP2SF).	Uses Ethereum BC with SHA-512 hashing approach, enhanced proof of work consensus algorithm, solidity language, and IPFS version 0.4.19.	✓	✓	✓	-	✓
Cha et al. [138]	Proposed an approach by integrating BC with the cloud for protecting personal information and secret sharing algorithm.	Uses consortium BC with a secret sharing algorithm. Block data is stored using a chain to maintain data integrity. Finally, the performance is analyzed in terms of the AES-128 encryption algorithm and execution speed, privacy, integrity, efficiency, scalability, and decentralization.	-	✓	✓	-	✓
Esposito et al. [140]	Proposed a BC-enabled approach for authentication and authorization policies in smart cities and integrated it with FIWARE.	Used Hyperledger Fabric BC platform with Kafka-based consensus algorithm. Analyze the proposed approach in terms of latency and throughput.	✓	✓	-	-	✓
Ferreira et al. [141]	Proposed an approach for registration and authentication for applications used for a smart city.	Uses Ethereum BC, a smart contract written using solidity language (responsible for registering IoT devices and associating them). NodeJs is used for IoT device management	✓	-	-	-	✓

attain better privacy and security. Still, there is some future direction that needs further attention. Some of them are electricity distribution among the residents can be improved, in real-time data sharing distributed sharing algorithm need to be more secure, load balancing is another important concern, various emerging technologies can be merged like edge and deep learning with BC enabled smart city. BC-IoT-driven smart city offers innumerable opportunities. Yet some challenges are typically faced such as massive data storage, scalability, a large number of simultaneous users, and chances of centralization.

D. Supply Chain and Logistics

A supply chain means it is a logical chain of all the different stakeholders involved in the different phases of the supply chain. Phases involved in the supply chain of any product are raw material, transportation, manufacturing, shipment, wholesalers, retailers, and consumers [142]. It is estimated that the worldwide supply chain market will expand at a rate of 87% and by the end of the year 2023, it will rise from \$45 million to \$3,314.6 million [143]. A product is a combination of different resources provided by possibly different manufacturers across different geographic locations. Because of the lack of

transparency in the traditional supply chain many times low-quality products are counterfeited with the original product. Some other challenges faced by conventional supply chains are lack of end-to-end visibility, lack of complete trust, ineffective information flow, and lack of advance technologies [144]. According to the report of Microsoft out of 408 organizations in 64 countries, 69% of them lack full visibility in their supply chain and 65% of them have experienced disruption in the supply chain [143]. According to a report by Scarano, 70,000 consumers signed a petition that urged large companies to improvise their supply chain transparency [143].

BC integrated IoT can transform the landscape of supply chain and logistics by instilling complete visibility, traceability, trust, dispute settlement, automation, and auditability [145]. By using BC not only the transparency and the security but also the physical flow of the product also increases as decision-making becomes quick [142]. Traceability is very crucial in the food and agriculture sector because it helps in providing information about the entire food life cycle to ensure the quality of the food [146]. Through e-commerce websites, packed foods were delivered and consumers need to pay for food items without having any food quality information, and packed foods are more sensitive to environmental conditions,

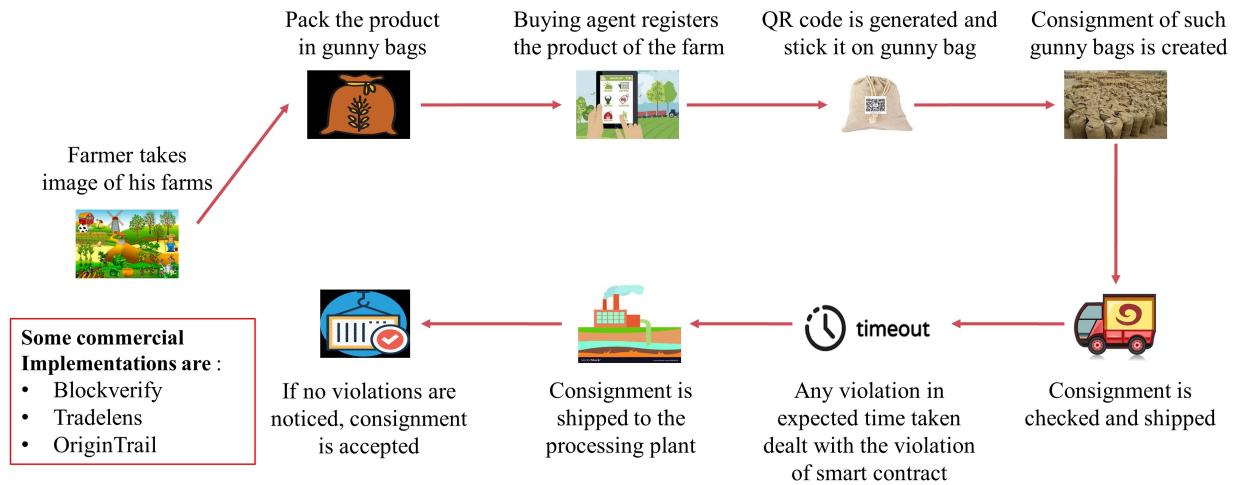


Fig. 10: Application of Blockchain in Supply Chain & Logistics (Food Supply Chain) [124]

and sometimes deterioration of food occurs [146]. The typical supply chain process focuses mainly on the origin of the raw material but today the scope has expanded from origin to end customer. In this context, BC-enabled framework can be build, which can potentially offer access to the required data at every touchpoint [67]. Furthermore, because of the distributed and decentralized nature of BC, all the stakeholders in a supply chain network can immutably view and access the data stored on the distributed ledger. Thus, BC allows users to securely, transparently, and trustlessly build a flexible and resilient supply chain [147]. Walmart and Kroger are the first companies who have implemented BC-based supply chains [148]. Some of the commercial implementations of BC in the supply chain are IBM Blockchain-TradeLens, which mainly focus on logistics, OriginTrail, to bring transparency to the international supply chain from 2013 to let its users know more about their food product and Blockverify, an anti-counterfeit which brings transparency in the supply chain (especially used in diamonds, pharmaceuticals, and electronic industries) [87]. TradeLens is a joint venture of IBM and Maersk (largest container shipping company) [149], where multiple parties can interact with each other and can access real-time shipping data [143]. Fig. 10, shows the application of BC in the supply chain of drugs.

1) *Applications of Blockchain in Supply Chain and Logistics:*

- **Pharmaceutical supply chain** - Drug counterfeiting is a most common problem that not only affects human lives but also economic loss to health sector. According to a report by WHO every year 30% of the drugs sold in the market are counterfeit [150]. Blockchain provides traceability capabilities to verify the drugs, so that the quality is not compromised [67]. By implementing a

better system for drugs traceability, will help in protecting patients from using fake medicines [151].

- **Food supply chain** - Food supply chain is one of the biggest supply chains. It suffers with adulteration of food due to which health and societal issues are on rise. So it is critical to find a way to keep an eye on each phase from food cultivation to consumption. Conventional supply chains face difficulty in ensuring transparency and visibility, and suffers with single point of failure [152]. To maintain the integrity of the product and supply chain, records must be tamper-proof, so that the integrity of the food history is maintained [153]. Also, traceability brings assurance to food quality and safety. To achieve all these discussed features, BC is expected to play a cardinal role.

2) *Related work:* The research works related to supply chain and logistics have been discussed under different categories which are discussed as follows:

Credit Evaluation: Mao et al. [154] proposed a BC-based credit evaluation system for the food supply chain to improve supervision and management. By using BC, traders are accountable for all their actions, which is known as provenance in BC. The proposed approach is a combination of BC technology and a deep learning model to collect and analyze the credit evaluation of traders. The system gathers credit evaluation text from traders by smart contracts on the BC and is analyzed directly by a deep learning network named Long Short Term Memory (LSTM).

Payment: Viriyasitavat et al. [155] put forward an approach for flexibility and smooth flow of cash and payments and improve the efficiency of financial transactions using BC technology and smart contracts. The proposed approach was explained using the proposed cryptocurrency Future Unspent Transactions Output (FUTXO). The proposed approach uses

Blockchain technology, smart contracts, matching algorithms, and off-chain verification with the PBFT consensus algorithm.

Monitoring: Weber et al. [156] presented the use of BC and its smart contracts in collaborative process execution and applies it in three different use cases i.e supply chain, incident management, and insurance claim handling. Moreover, authors highlighted the features of BC like decentralization since using BC so that no central authority is required but trust between the involved parties remains intact. For implementing proof of concept, authors used Ethereum BC platform, smart contracts, and off-chain storage.

Double Chain: Leng et al. [157] proposed a public BC for an agriculture supply chain using double chain architecture. One is the user information chain and the second is the transaction chain. User information is recorded in the user information chain which ensures authenticity, integrity, and privacy, and all the transaction data is stored using the transaction chain which ensures authenticity, integrity, and openness. The key benefits of using a double chain are any node can view the resources without knowing the private information, reduces the redundant information, and business expansion can be easily implemented between platforms and financial institutions. Interestingly, authors proposed their own consensus algorithm which they claim to work efficiently for agriculture BC.

Real time tracking: Helo et al. [158] proposed a project known as real-time supply chain architecture (RTSC) for real-time tracking and tracing of the supply chain using RFID, IoT, and BC. RFID and IoT are used for user interface and to provide real-time information and BC is used to verify the authenticity of transactions and provide a chain of immutable transactions. The proposed approach uses the Ethereum BC platform and PoW consensus algorithm. DApps are used to develop the front end using HTML and the back end using solidity smart contract and interaction between the front end and back end was done using web3.js. Stakeholders involved in the supply chain can track and trace data about the shipped items. The proposed system provides a connection between transport companies and tracking devices. Along with this, presented the benefits of the proposed system.

Traceability: Tian et al. [159], Tian et al. [160], Caro et al. [153], Rovzman et al. [161], Tsang et al. [146], Humayun et al. [162], Agrawal et al. [163] and Lou et al. [164], worked in the same direction i.e., to track and trace the products in supply chain, which offers openness, transparency, reliability and trusted environment. Authors Tian et al. [159] proposed a food supply chain traceability system using RFID and BC technology to improve food safety and quality. RFID technology is used for data acquisition, circulation, and sharing, and BC technology is used to ensure that the information shared and published is reliable and authentic. The benefits of using BC technology are information is transparent and open, no requirement for centralized organization, and irreversible transactions. In 2017, Tian et al. [160] put forward a new decentralized traceability system which is an extension of [159], based on HACCP (Hazard analysis and critical control points), IoT, and BC technology. It includes mainly five links; production, processing, warehousing, distribution, and retail.

It uses IoT (RFID, WSN, GPS) to collect and transfer, and BigchainDB for storing and managing data.

Caro et al. [153] proposed a decentralized traceability approach for the agriculture food supply chain by integrating BC with IoT, known as AgriBlockIoT. As it directly provides critical information on production and consumption, it ensures transparency and auditable assets. The main modules included are API, controller, and Blockchain. Also deployed the proposed system for the use case 'from farm to fork using two different BC platforms Ethereum and Hyperledger Sawtooth. Both of these provide a different level of customization as Ethereum works with a single transaction while Hyperledger allows custom transactions. A comparison of the performance of both the BC platforms is shown in terms of latency, CPU, and network usage and results show Hyperledger has better performance as compared to Ethereum.

In 2019, Rovzman et al. [161] proposed a concept to integrate BC and IoT and implemented it for supply chains. One of the crucial features provided by this approach is modularity which means any number of different types of nodes can be linked. Some of the core nodes are the genesis node, service node, user node, interface node, agreement node, and mapping node. For validation smart contracts are implemented using the Rinkeby test network. Tsang et al. [146] discussed the issues in the conventional supply chain like reliability, scalability, and information accuracy, and suggested how BC can mitigate these challenges. Proposes a BC -IoT-based food traceability system (BIFTS) for traceability in the supply chain. IoT is used for monitoring applications, collected data is stored using a cloud database and the food life cycle is managed by using BC. It is a lightweight and vaporized hybrid approach of BC and cloud. For consensus, it uses proof of supply chain share (PoSCS) to mint or forges the blocks and SHA-256 for hashing. The benefits of using the proposed approach are secure and reliable food traceability, lightweight and vaporized design, and intelligent food quality evaluation. Authors also highlighted the challenges in implementing BIFTS in the supply chain like human errors, honesty, integrity, and open-mindedness for all stakeholders to adopt the system.

In 2020, Humayun et al. [162] proposed a framework by integrating BC with IoT, named BCTLF for logistics and transportation systems to make the system more convenient and transparent. Authors highlighted the benefits of integrating BC-IoT such as freight tracking, temperature control, carrier authentication, and fast delivery through continuous monitoring. In particular, the authors discussed the two case studies to highlight the role of BC and IoT in the supply chain. Agrawal et al. [163] in 2021 proposed a BC-driven supply chain traceability system that uses distributed ledger for storage and authentication, in the textile and clothing industry, and explained the proposed approach at an organizational and operational level. In particular, the authors presented a use case of the organic cotton supply chain through a mass balancing validation mechanism. The proposed approach uses private BC, proof of work consensus algorithm, and public and private key pairs generated using the RSA algorithm. Lou et al. [164] proposed a BC-based framework named SESCOF to resolve the challenges being faced by the supply chain such as information

TABLE IX: Summary of Related Work in BC-Supply Chain & Logistics

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Weber et al. [156]	Proposed a BC-based technique to address the lack of trust challenge in the collaborative business process.	Uses Ethereum blockchain, smart contracts written in solidity language, Proof of concept consensus, and off-chain data storage.	-	✓	✓	-	-
Tian et al. [159]	Proposed a supply chain traceability system that covers the whole process of data gathering to information management of every link involved in the agricultural supply chain.	Proposed system uses RFID and BC technology. Also analyzed were the advantages (like the benefit of tracking and traceability, enhanced credibility, and fight against fake products) and disadvantages (like high cost, and immaturity of BC), of using RFID and BC technology.	✓	✓	-	-	-
Tian et al. [160]	Proposed a traceability system based on HACCP that uses BC and IoT to improve the efficiency, openness, neutrality, reliability, and transparency in the food supply chain.	Uses RFID for labeling the products, digitally signed the smart contract for the exchange of information stored on BigchainDB.	✓	-	-	-	-
Caro et al. [153]	Proposed an approach by integrating BC with IoT for traceability of the agriculture food supply chain known as AgriBlockIoT.	Deployed the use case using two BC platforms i.e. Hyperledger sawtooth and Ethereum and evaluated the performance in terms of latency, CPU, and network usage. Concluded that Hyperledger sawtooth shows comparatively better performance.	-	-	-	✓	-
Leng et al. [157]	Proposed an approach for an agriculture supply chain based on double chain architecture.	Uses public BC double chain architecture i.e. user information chain and the transaction chain with its proposed consensus algorithm.	✓	✓	-	-	✓
Mao et al. [154]	Proposed a credit evaluation system for different stakeholders in the food supply chain, to strengthen the effectiveness of supervision and management.	Uses IoT and BC with smart contracts known as chain code. The system adopts Hyperledger fabric 1.0 consortium BC.	✓	✓	-	✓	✓
Rovzman et al. [161]	Presented an approach for integrating BC and IoT technologies that supports modularity which means any number of different types of nodes can join.	Uses IoT as a communicating means for nodes and BC is used for listing the services and information and for validation uses the Rinkeby test network.	✓	-	-	-	✓
Tsang et al. [146]	Presented an overview of the food supply chain, challenges in existing food traceability systems, and benefits of integrating BC and IoT. Proposes a BC-IoT-based food traceability system for managing perishable food.	Uses IoT technology for environmental monitoring, collected data is stored using a cloud database and associated keys, and the life cycle is maintained using BC with hash algorithm SHA-256, to store the fingerprints of the block. POSCS (Proof of Supply Chain Share) consensus algorithm is used.	✓	✓	-	-	✓
Humayun et al. [162]	Proposed a framework named BCTLF, for smart logistics and transportation.	Uses BC and IoT for intelligent logistics and transportation systems. Data is collected using sensors and stored in the distributed blockchain ledger.	-	✓	-	-	✓
Helo et al. [158]	Proposed an approach by integrating BC, IoT, and RFID for real-time tracking and tracing of the supply chain.	Uses the Ethereum BC platform and PoW consensus algorithm. DApp is used to develop the front end using HTML and the back end using solidity smart contracts and interaction between the front end and back end was done using web3.js	✓	-	-	-	-
Agrawal et al. [163]	Proposed a BC-driven supply chain traceability system that uses distributed ledger for storage and authentication, in the textile and clothing industry.	Proposed approach uses private BC, proof of work consensus algorithm, public, and private key pair generated using RSA algorithm.	✓	-	✓	✓	✓
Viriyasitavat et al. [155]	Proposed an architecture based on BC and smart contracts for a smooth flow of payments, to improve the efficiency of the financial transactions.	Uses Blockchain technology, smart contracts, matching algorithm, and off-chain verification with PBFT consensus algorithm.	✓	-	-	-	-
Lou et al. [164]	Proposed a BC-based framework named SESCOF to resolve the challenges being faced by the supply chain.	Proposed approach uses Ethereum consortium BC, solidity language for smart contracts, RFID, and payment channels.	✓	-	-	-	-
Song et al. [165]	Proposed a framework to form a supply chain effectively using IoT and BC.	Uses access control list, double chain structured consortium BC with two different BC techniques; hyperledger fabric and ethereum.	✓	-	-	-	✓
Bamakan et al. [166]	Proposed a framework to evaluate the performance of the supply chain.	Uses fuzzy logic, AI, IoT, BC, and big data.	✓	✓	✓	-	✓
Al et al. [167]	Proposed a BC-driven trust model which simplifies data sharing and reduces computational, latency, and storage requirements.	Uses IoT, BC, and compared it with the PoW consensus algorithm.	✓	-	-	-	-

flow, logistics, and capital flow. The proposed approach uses BC, smart contracts, RFID, and payment channels. BC and smart contract ensures information symmetry, RFID ensures the unique identity of goods and the payment channel solves the issue of a payment default. The proposed approach helps in improving the efficiency of the supply chain by putting goods transactions on the chain and capital transactions off the chain. The proposed approach follows a layered architecture;

user layer, transaction layer, and BC layer.

Performance Evaluation: Bamakan et al. [166] proposed an approach to evaluate the performance of the supply chain, save computing time, and speed up information flow. The proposed framework includes six layers; data layer (system's data input sources), connection layer (necessary infrastructure to receive real-time information), blockchain layer (exploit data in conjunction with ANFIS model), smart layer (smart

contracts), ANFIS (adaptive network-based fuzzy interface system) layer (evaluates SSC performance) and application layer (performance management). With the help of IoT, BC, and ANFIS, a performance management system is created.

Security: Song et al. [165] proposed an approach using IoT and BC technology to form supply chains effectively. In particular, includes an access control framework, an access control policy determined by all members jointly, and BC technology to ensure all processing is trusted and valid. The access control list has two modules; the registration module (for information registration) and the inspection module (for judging misbehavior). Moreover, the authors have used a backup peer mechanism, internal data isolation, and transmission method to ensure availability.

Trust Model: Al et al. [167] proposed a BC-driven trust model which simplifies data sharing and reduces computational, latency, and storage requirements. It resolves trust challenges between supply chain parties and maintains data integrity. In particular, includes three modules; data (data produced by sensors within the supply chain and trade events in between its nodes), IoT network (authenticates and supervises the messages and node), and BC and supply chain (communicates with each other through series of queries).

Table IX, summarizes the work done in the BC-supply chain use case.

3) **Summary:** The supply chain is the chain of stakeholders involved from initial production stage to final consumption of any product. It aims to provide quality compliance, eliminate of communication gaps, optimize shipping, and customer satisfaction. However, there are some challenges with the existing system such as the availability of resources, limited transparency, traceability, trust issues, and stakeholder management. BC has been leveraged to overcome these challenges, such as decentralized collective maintenance, matching between supply and demand of resources, verifiability, and identifying counterfeit products. To explore the applicability of BC in supply chain and management various research has been done. In particular, researchers have made efforts to monitor, track and trace the supply chain and ensure smooth flow of payment. Especially for real-time tracking and monitoring, various researchers have used Ethereum BC platform with smart contracts, double chain, RFID, IoT, and Hyperledger BC. For hashing, SHA-256 and consensus PoW is preferred. Nonetheless there are many aspects which still need dedicated research efforts, for instance, analyzing scalability and interoperability for real-time use cases, speed, and efficiency of the consensus algorithm. Quality management, risk management, and e-commerce are other significant areas to be considered in the supply chain. Apart from information flow, BC and IoT enabled supply chain can be built that manages material flow, capital flow, value flow, and risk flow [146]. Lastly, interoperability, massive data handling, throughput enhancement are few more areas which need to be worked upon when considering BC and IoT enabled supply chain and logistics.

E. Autonomous Vehicle

Vehicles are becoming smarter as they can not only gather information with the help of the sensors installed in them

but can also communicate that information over the Internet and can act according to the received response [168]. An autonomous vehicle refers to a connected, smart, and driverless vehicle that can communicate or exchange data with other vehicles, city infrastructure, and online services or applications and is traveling without humans controlling the vehicle [169]. City infrastructure includes traffic lights, road work, route planning, etc. Autonomous vehicles are a network of a vehicle to vehicles (V2V), vehicles to infrastructure (V2I), vehicles to the roadside unit (v2R), and vehicles to pedestrians (v2P) [145].

The concept of driverless vehicles was first introduced in 1920 [170]. The level of automation varies from zero to full automation, according to NHTSA, which has classified automation into five levels, (i) no automation, (ii) function-specific automation, (iii) combined function automation, (iv) limited self-driving automation, and (v) fully autonomous vehicle [170]. According to a report, the smart vehicles market will be worth US\$87 billion and by the end of the year 2040, every four out of ten vehicles could be autonomous [169]. Because of human errors, thousands of deaths happened each year which can be reduced to zero by using AVs [169]. smart insurance, and self-owning car, are the application of autonomous vehicles. Some practical implementations of self-driving vehicles are La'Zooz, a ride-sharing application, a blockchain version of Uber [171], and also Uber has ordered 50,000 SUVs to deploy fully self-driving vehicles over the street.

Implementing autonomous vehicles will help in reducing accidents, reducing traffic congestion, increasing lane capacity, and efficient parking. However, realising these benefits from autonomous vehicles requires large exchange of small data and real-time processing. Moreover, the data exchanged by these smart vehicles leads to new privacy challenges [172]. BC and IoT enabled autonomous vehicles will be able to handle these challenges.

1) Applications of Blockchain in Autonomous Vehicles:

- **Electric Vehicle Charging** - The increase in electric vehicles (EVs) has resulted in high demand for fast charging stations. In this context, smart vehicles connected to the owner's smartphone can provide pro-active services. If the travel pattern is securely stored on BC then charging can be done automatically at regular intervals. Moreover, based on the secure data stored on BC, EVs can be provided with the most efficient charging cycle [172] and the unavailability of charging stations can be minimized. In addition to energy management, identity management of autonomous EVs is yet another area where BC can be leveraged [173]. Share and charge are the BC-based platforms that allow P2P energy trading among EVs and private charging stations [56].
- **Smart Insurance** - Today insurance companies offer flexible insurance which is based on various data collected from the vehicles and evaluation of driving behavior like speed, and breaking pattern [172]. In this context, BC enabled vehicles can provide secure, distributed, privacy protected exchange of data. Moreover, data is shared on the basis of demand not continuously [172]. Since the

TABLE X: Summary of Related Work in BC-Autonomous Vehicle

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Yuan et al. [171]	Proposes a BC-based seven-layer ITS framework (B2ITS) for the establishment of a secured, trusted, and decentralized autonomous ecosystem.	Uses BC technology, SHA-256 for hashing, Merkle tree, time stamping, and PoS consensus algorithm.	-	✓	-	-	✓
Dorri et al. [172]	Proposes a BC-based architecture to enhance the privacy of users and security of the vehicular ecosystem.	Uses public BC, each vehicle is equipped with WVI (wireless vehicle interface) and local storage to store sensitive data.	✓	✓	✓	-	✓
Singh et al. [176]	Briefly introduces intelligent vehicles and propose a reward-based approach for communication between intelligent vehicles using blockchain.	Uses three basic technologies i.e. communication network, vehicular cloud computing, and blockchain technology. Also uses the PoD (proof of driving) consensus algorithm.	✓	-	-	-	✓
Oham et al. [177]	Brief overview of a liability attribution model and proposes a blockchain-based framework for providing untampered pieces of evidence for liability attribution and adjudication.	Uses permissioned BC, public key infrastructure to issue digital identities for authenticated and authorized communication, digital signatures, and data stored in the blockchain.	✓	✓	-	-	✓
Cebe et al. [168]	Proposed a blockchain-based framework for vehicular forensics which manages the collected vehicle-related data for trustless, and privacy-aware post-accident analysis with minimal storage and processing overhead.	Uses permissioned blockchain, PBFT consensus algorithm, and cloud for data storage while their hash is stored on BC.	✓	✓	-	-	✓
Singh et al. [178]	Proposed a BC-enabled intelligent vehicle communication approach for trusted and secured communication.	Uses two blockchain mechanisms, one is LDB and the other is MB. When LDB is filled then it is overwritten in a FIFO manner and MB is implemented using Merkle Tree, PoW consensus algorithm.	-	-	-	-	✓
Rathee et al. [179]	Proposed a BC-based framework to address security challenges in smart sensors of connected vehicles.	Uses blockchain technology to record each activity, and analysed the performance using an NS2 simulator.	✓	-	-	-	✓
Yin et al. [180]	Proposed a BC-based incremental update system for data storage.	Uses BC, data and index storage, incremental data update adaptive PoW algorithm, elliptic curve digital signature algorithm (ECDSA), and SHA256 for hashing.	✓	-	✓	-	-
Jamil et al. [181]	Proposed a BC-based privacy-preserving approach for automatic payment of fueling of smart cars without human intervention.	Uses Hyperledger fabric, Hyperledger composer, docker composer, docker engine, CLI tool, off-chain storage, smart contract, elliptic curve to generate public and private keys, and Diffie Hellman key exchange.	✓	✓	✓	✓	✓
Oham et al. [182]	Proposed a BC-based security framework known as B-FERL for securing smart vehicles.	Uses double-tier blockchain-based architecture, SHA-256 for hashing, asymmetric encryption and digital signatures, and appendable block concept.	✓	✓	-	-	✓
Tyagi et al. [183]	Proposed an approach to secure smart vehicles (preserve user's personal information) using BC technology.	Uses BC technology and Inter planetary file system (IPFS) for storage.	✓	-	-	-	✓

data stored on BC is tamper-proof and distributed, users are not able to alter it, neither for insurance claim fraud nor for inflating insurance premium [174]. Smart contracts running on top of BC can enforce automatic claim settlement in transparent and trustless manner [175].

2) *Related work*: The research works related to autonomous vehicles have been discussed under different categories as follows:

Payment: Jamil et al. [181] proposed a BC-based privacy-preserving approach for automatic payment for fueling of smart cars without human intervention, ensuring privacy, transparency, and trust. In particular, authors used Hyperledger fabric permissioned BC (to provide modular, scalable, and secure foundation), off-chain storage, a smart contracts written using solidity language, an elliptic curve to generate public and private keys, Diffie Hellman key exchange. Their proposed approach includes services like data sharing, smart pump management, secure payment transaction, smart car management, and user identity management. Finally, the authors analyzed the performance in terms of latency, resource consumption, and transactions per second using the Hyperledger caliper.

Data Storage: Yin et al. [180] proposed a BC-based

incremental update system for data storage, improving data records and update efficiency. Their proposed system includes only the data storage stage and update stage. Copies of the data are stored on different independent sources and their index is stored on-chain, which enhances data reliability. Along with that, a PoW algorithm is designed to improve transaction efficiency and reduces system security risk. For calculating the secret key authors used the elliptic curve digital signature algorithm (ECDSA) and SHA 256 for hashing.

Communication: Singh et al. [176] highlighted the issues in intelligent vehicle communication using a traditional approach such as trust, data accuracy, and reliability. To overcome these challenges, the authors proposed a reward-based approach known as Intelligent Vehicle-Trust Point (IV-TP) for communication using BC technology. The proposed approach stores all IV-TP details of every vehicle and is accessed by IVs. IV-TP provides fast and secure communication between IVs. It includes three basic technologies; connected devices, vehicular cloud computing, and BC.

Forensic Application: Oham et al. [177] and Cebe et al. [168], both worked toward forensic aspects of autonomous vehicles. Oham et al. [177] proposed a distributed forensic

framework using permissioned BC for the auto insurance liability model for autonomous vehicles. Their framework provides untampered evidence for automatic processing of insurance claims and settling disputes. Thus, the framework puts an end to the chances of a single point of trust and allows multiple participants to simultaneously agree on the evidence needed to process claims. Authors also presented a security analysis of the proposed framework. While Cebe et al. [168] proposed a framework to manage the collected data, identify faulty parts, and solve the disputes in case of an accident with the help of integrating vehicular public key infrastructure (VPKI) with permissioned BC. Their work includes three types of data; event data, diagnosis data, and maintenance data which is stored using the cloud, and respective hashes are stored in BC. The proposed system connects all the stakeholders involved from vehicle manufacturers to customers and offers traceable, privacy-aware post-accident analysis with minimum processing overhead. Moreover, the proposed approach includes a fragmented ledger that stores data such as maintenance information, history, and car diagnosis report.

Security & Privacy: Yuan et al. [171], Dorri et al. [172], Singh et al. [178], Rathee et al. [179], Oham et al. [182] and Tyagi et al. [183], worked towards improving security and privacy in Autonomous vehicle using BC. In 2016, Yuan et al. [171] provided an overview of BC technology and its potential in a transportation system. To resolve security and privacy-related challenges, the authors proposed a seven-layer BC-enabled intelligent transportation system (B2ITS) and explained it using a case study of a ride-sharing service. Seven layers are the physical layer (which includes physical entities such as devices, and vehicles), the data layer (which includes chained data blocks using techniques such as asymmetric encryption, time stamping, hashing, and Merkle tree), the network layer (includes distributed networking, data forwarding, and verification), consensus layer (includes all possible consensus algorithm), incentive layer (includes incentives and rewards), contract layer (includes scripts, algorithm, and smart contracts) and application layer (includes various application scenarios).

In 2017, Dorri et al. [172] discussed the conventional methods used in smart vehicles and highlighted the challenges namely centralization, lack of privacy, and safety threats, and suggested BC as a potential solution to all these challenges. Authors proposed a solution based on BC for automotive security and privacy. Stakeholders involved in the chain such as smart vehicles, equipment manufacturers, and service providers form an overlay network to communicate with each other. Communications are encrypted using asymmetric encryption. Discussed some of the applications of the proposed architecture like remote software updates, insurance, electric vehicle, smart charging services, and car-sharing service. Furthermore, compared it with the conventional method in terms of security and privacy. In 2018, Singh et al. [178] provided a brief overview of BC technology, its advantages like security, transparency, reliability, and its application for an intelligent vehicle. Moreover, the authors proposed a BC-driven approach for Intelligent Vehicle communication, which ensures trustworthiness among vehicles and evaluated the

performance using real-time traffic scenarios.

Rathee et al. [179] in 2019 highlighted the security-related challenges in smart sensors of connected vehicles. They proposed a security mechanism for connected autonomous vehicles services framework using the BC technique to ensure transparency and security. Initially, data is stored using an ordinary database and then stored permanently on BC to track each activity. The authors analyzed the proposed approach using NS2 simulator against the existing approaches and the results showed a 79% success rate. In 2021, Oham et al. [182] proposed a framework for decentralized security known as B-FERL for securing smart vehicles using BC. Their framework is based on a double-tier architecture which includes initialization operation (for creating a record of vehicles for authentication) and challenge-response mechanism (to query the integrity of the vehicle's network). The proposed framework includes entities like verifiers (legal authorities) and proposers (vehicle manufacturers, service technicians). Transactions are secured using SHA-256, off-chain storage, asymmetric encryption, and digital signatures. No consensus algorithm is used, instead an appendable block concept is used where transactions are added by the verified block owner. The authors analyzed the performance of their proposed framework in terms of overhead, the time required, and storage space required. The results showed that their proposed approach is resilient against various security attacks such as Sybil attacks, fake data, and masquerade attacks. Authors also discussed the applicability of the proposed approach in various use cases such as vehicular forensic, trust management, and secure vehicular communication. In 2022, Tyagi et al. [183] proposed an approach to secure users' personal information in smart vehicles using BC and IPFS. Table X, summarizes the work done in the BC-autonomous vehicle use case.

3) **Summary:** Autonomous vehicles are connected, smart, and diverless vehicles that can sense, communicate and exchange data with other vehicles or infrastructure. Autonomous vehicles are anticipated to enhance road safety, reduce the number of road accidents, minimize driving errors, reduce traffic congestion, and enable stress-free parking. For providing such services, IoT is an integral part of an autonomous vehicle. The existing approach faces some challenges such as centralization, trust issues, privacy and security and the user's control over exchanged data is less. Combining BC with IoT-enabled autonomous vehicles brings opportunities such as data integrity, data sharing, proof of delivery, unaltered records, transparency, and reliability. To explore the applications of BC in an autonomous vehicle, numerous research works have been done in different directions like payments, data storage, communication, forensic application, and security and privacy. To achieve security and privacy, BC, SHA-256, off-chain storage, asymmetric encryption, and digital signatures are used. Hyperledger Fabric, off-chain storage, smart contracts, elliptic curve, and Diffie Hellman key exchange are used for executing payments. Apart from the features offered by BC, there are some challenges in integrating BC with Autonomous Vehicles, such as high infrastructural cost, massive data storage, scalability, integration into the existing system, and avoiding chances of centralization. Some of the research

directions for BC-IoT enabled autonomous vehicles are how to achieve high throughput without compromising security and privacy, how BC-IoT autonomous vehicles can be used for accident reconstruction, multiple vehicle communication scenarios, and privacy of smart vehicle when moving from one roadside to another. System intelligence can be increased by adopting deep and reinforcement learning.

F. Smart Grid

A smart grid is also known as a smart power grid, intelligent grid, or future grid. A conventional power grid has to simply carry power from central generators and supply it to users/consumers [184]. In contrast, a smart grid involves use of state of the art sensing methods, communication technologies, interconnected power systems, advanced control and optimization techniques, smart metering, and integration of microgrids and other decentralized sources of renewable energy [185], [186]. Nowadays, solar panel installation has seen significant growth which has resulted in individual homeowners installing solar panels and contributing excess energy generated from solar panels to the larger electric grids [187]. Due to variable energy consumption pattern, some users' energy generation can be more than required and at the same time other users may be facing insufficient energy supplies. Thus, the former can trade their excess energy to latter [188].

Smart homes, smart buildings, and smart infrastructure, all of these collectively form a smart community [189]. All of these must be supported by a smart power supply. The challenges being faced by conventional power supply can be reduced by Smart grid [189]. Along with this, these smart sensor-based metering systems will require less manpower as compared to the conventional approach [56]. Some of the general challenges faced by the smart grid are the availability of trusted parties for data aggregation, hiding the link between the user's real identity, and pseudonym and authentication speed [189]. Implementing BC-based smart contracts in smart grids is an opportunity to increase the speed and security of the smart grid [190]. BC makes the grid network decentralized which means the supply and distribution of energy need not be channeled through a centralized system [56]. For instance, users who own some form of renewable energy generation facility such as solar panels can become producers by selling their surplus energy to the grid [56]. However, the challenge is to ensure secure and trusted energy trading between two trading parties. BC has potential to build decentralized and secure P2P energy trading platform [145]. Some existing commercial implementations are PowerLedger, Bankymoon, and Brooklyn [56], [87]. PowerLedger is an Australia-based startup that enables owners of renewable energy sources to sell their surplus energy [191]. Bankymoon is a South Africa-based startup, that provides smart prepaid energy meters and supplies energy to schools and communities who need affordable power supply [192] and Brooklyn, launched by US energy firm is the most significant implementation of BC in P2P decentralized energy trading [56]. WePower is another Lithuania based company for energy data accounting and storage using smart contracts [193].

1) Applications of Blockchain in Smart Grids:

- **Decentralized P2P Energy Trading-** In a traditional grid network, the major concern is lack of security in a transaction of energy and high operational costs. However, the BC-based grid trading infrastructure is a decentralized platform that enables peer-to-peer transactions of energy [56], [201], [205]. Power Ledger platform provides numerous energy trading applications [193].
- **Power Distribution and Management-** BC with its strong security features can prevent many attacks that have been made on the traditional power grids to manipulate the data and to have control of the system [56]. Moreover, BC and smart contracts can enable secure, efficient and reliable management of IoT-enabled distribution network in smart grids [205].
- **Secure Metering -** Meters are installed in every house to maintain the record of electricity consumed. Intruders can record and analyze the electricity consumption pattern and can reveal users' details. BC with advanced cryptography methods can be used to ensure the privacy of the information [195], [206].

2) *Related work:* The research works related to the smart grid have been discussed under different categories which are discussed as follows:

Grid Monitoring: Mengelkamp et al. [194] discussed smart grids and local energy markets and propose an approach based on BC, which underlines the decentralized nature of local energy markets with an auction mechanism at a small level. The proposed approach consists of a closed double-sided auction market, implemented using a smart contract. It uses private permissioned Ethereum BC, smart contracts written using solidity language, and a PoW consensus algorithm. In 2018, Gao et al. [195] proposed a BC-based solution for creating a system to protect consumer data that is recorded and transferred through the smart grids in a tamper-proof manner. Cryptographic keys are used for specific tasks such as system and data security. The proposed approach includes various layers; user layer, data processing and monitoring layer, registration and authentication layer, smart contract layer, smart contract database layer, energy center layer, and data center layer. SHA-256 is used for hashing the blocks. Along with that, compared the proposed solution with the existing solution in terms of information sharing, efficient data manageability, data immutability, data confidentiality, and data provenance. In line with that, in 2021, Naseer et al. [199] proposed a BC-enabled lightweight scheme for access control to ensure temper proof, trusted communication between entities of the smart grid and provide a secure channel to submit transactions in the network. In particular, uses the Ethereum BC platform, SHA-256 for key generation, elliptic curve cryptography for secure communication, and BC. Furthermore, the authors analyzed the scheme in terms of security and performance and the results show it is effective in terms of computational and storage costs.

Device Identification & Management: Wang et al. [200] put forward an approach for the connection of IoT devices by using BC and 5G MEC technologies. Their approach uses public and private BC deployed using MEC server. Authors

TABLE XI: Summary of Related Work in BC-Smart Grid

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Guan et al. [189]	Proposed an approach to preserve user's identity and efficient data aggregation in a smart grid.	Uses blockchain, bloom filter, RSA algorithm, and zero-knowledge proof.	✓	✓	-	-	✓
Mengelkamp et al. [194]	Proposed an approach for trading local energy generation.	Uses distributed information and communication technology i.e. private permissioned blockchain, Ethereum blockchain, PoW consensus algorithm, and on-chain simulation.	✓	-	-	-	-
Gao et al. [195]	Proposed an approach to monitor electricity consumption, that allows no manipulation and protects consumer data recorded and transferred.	Uses smart contracts, blockchain, and SHA-256 and analyzes the performance in terms of information sharing, efficient data manageability, and data immutability.	✓	✓	✓	✓	-
Gai et al. [188]	Proposed a privacy-preserving blockchain-enabled trading model.	Uses Hyperledger fabric consortium blockchain for secure energy trading system, smart contract for preventing privacy leakage.	-	-	-	-	✓
Baza et al. [196]	Proposed a blockchain-based approach to enable a decentralized charging coordination mechanism.	Uses Ethereum BC platform, smart contracts written in solidity language to implement charging coordination algorithm.	-	✓	-	✓	✓
Sestrem et al. [197]	Proposed an approach for the implementation of blockchain in a smart grid.	Uses three blockchains named BlockPRI, BlockSEC, and BlockTST, smart contracts, Loom network, side chains, and DPOS consensus algorithm.	✓	✓	✓	-	✓
Bera et al. [198]	Proposed a BC-based access control protocol named DBACP-IoTSG, for IoT-enabled smart grids.	Uses Dolev-Yao (DY) threat model, private BC, SHA-256/512, PBFT consensus algorithm, random numbers, and current timestamp and analyzed the approach in terms of computation and communication cost.	✓	✓	✓	-	✓
Naseer et al. [199]	Proposed a BC-enabled scheme for access control to ensure tamper-proof, trusted communication between entities of smart grid.	Uses Ethereum BC platform, SHA-256, elliptic curve cryptography, and BC and analyzed the scheme in terms of security and performance.	✓	✓	✓	-	-
Wang et al. [200]	Proposed a mechanism by integrating BC and 5G MEC technologies for the connection of massive power IoT devices.	Uses public and private BC both and deployed on MEC server. Also analyzed was the performance of different consensus algorithms in terms of average computing time and average time to an agreement.	✓	✓	-	-	✓
Guan et al. [201]	Proposed an approach named privacy-preserving blockchain energy trading scheme (PP-BCETS) based on ciphertext policy attribute, which exponentially improves operation efficiency.	Uses credibility-based equity proof consensus algorithm, elliptic curve digital signature algorithm, SHA-256, and Ethereum BC platform. Finally, a security analysis and performance evaluation are presented.	-	✓	-	-	✓
Wang et al. [202]	Proposed an approach for mutual authentication in smart grids.	Uses Ethereum BC, smart contracts, elliptic curve cryptography, join and exit mechanism, and batch verification.	✓	-	-	-	-
Mazumdar et al. [203]	Proposed an approach to detect energy theft with privacy preservation of energy consumption data for smart grid neighborhood area network.	Uses consortium BC hyperledger best with Proof of Authority consensus, AES256 for encrypting private transactions. User and data authentication is achieved using ZK-STARK and RS256 digital signature. SHA256 is used to hash energy consumption data.	-	-	-	-	✓
Wang et al. [204]	Proposed a solution to mitigate latency and bandwidth-related challenges	Uses Fog Nodes with ElGamal cryptosystem, computational Diffie hellman algorithm.	✓	✓	✓	-	-

also discussed numerous consensus algorithms and their usefulness in hybrid BC. The authors analyzed the performance of different consensus algorithms in terms of average computing time and average time to agreement.

Privacy Preserving: Guan et al. [189] proposed a BC-based privacy-preserving and efficient data aggregation scheme, in which users are divided into different groups. Each group consists of a private BC to record its members' data. The proposed approach is specially designed to tackle challenges like privacy, pseudonym, and speed. Their scheme allows a user to create multiple pseudonyms to hide user identity and bloom filter for fast authentication, to judge the validity of pseudonyms and check the existence of pseudonyms based on zero-knowledge proof. Authors showed that their proposed scheme outperforms and meets security requirements as compared to other popular methods. In 2019, Gai et al. [188] presented a BC-based approach to solve the problem of privacy leakage in trading functions and user privacy in a smart grid, known as the privacy-preserving blockchain-driven trading model (PBT). For preserving privacy it uses a noise-based

approach to hide the trading distribution. Moreover, their approach use consortium BC to establish a secure energy trading system and smart contracts for preventing privacy leakage. It includes mainly three phases; energy seller initialization, B-Box operation, and buyer purchase. Evaluated the performance in terms of privacy-preserving. In line with that, in 2021, Guan et al. [201] proposed another approach named privacy-preserving blockchain energy trading scheme (PP-BCETS) based on ciphertext policy attribute, exponentially improving operation efficiency. It enables direct transactions between electricity users and producers and helps in improving the privacy, security, and reliability of the energy trading process by implementing smart contracts. Along with that, proposed a credibility-based equity proof consensus algorithm to resolve low efficiency and high delay in BC. The design goals of PP-BCET are privacy protection, efficiency, and anti-attack. It includes mainly five phases; system initialization, user registration, transaction process, building consensus, application for arbitration, and generating accounting node. In particular, uses an elliptic curve digital signature algorithm for generating

public and private keys, SHA-256, and the Ethereum BC platform. Finally, security analysis and performance evaluation are presented. In 2022, Mazumdar et al. [203] proposed a BC-driven approach to detect energy theft in smart grid neighborhood area networks along with preserving the privacy of energy consumption data. In particular, authors have used consortium BC hyperledger best with Proof of Authority consensus, AES256, ZK-STARK, RS256 digital signature, and SHA256. Furthermore, results show that the proposed approach achieves more than 98% accuracy in energy theft detection. [204] proposed a solution along with dynamic billing and arbitration, named PPDB to reduce latency and bandwidth-related issues and to improve efficiency. In particular, the author has designed a four-layer data aggregation framework that uses fog nodes (FNs) to collect and aggregate electricity consumption data using the ElGamal cryptosystem and employ distributed decryption to achieve fine-grained access and bill generation based on real-time prices. Along with a trusted third party to arbitrate disputed bills. Further, the comparison shows that the communication overhead is reduced by 38 percent, and the computational efficiency is improved by 40 times.

Control Access: Bera et al. [198] proposed a BC-based access control protocol named DBACP-IoTSG, for IoT-driven smart grids without the involvement of a trusted third party, while preserving the anonymity and untraceable properties. In particular, uses Dolev-Yao (DY) threat model, private BC, PBFT consensus algorithm, random numbers, and current timestamp is used to protect against the replay attack. Phases involved are system setup (either SHA-256/512), registration of smart meters and service providers, access control, key management among service providers, block formation and addition in the blockchain, and new smart meters addition after initial deployment in the smart grid. Furthermore, the analysis shows that the proposed approach provides better security and requires less communication and computation cost.

Charging Coordination: Baza et al. [196] proposed a BC-based charging coordination mechanism for energy storage units (ESUs). For defining the rules for coordination between different ESUs, smart contracts written in solidity language are used, and the Ethereum BC platform. For scheduling the charging of ESUs, a greedy algorithm is used. The approach includes three phases; acquiring anonymous credentials, charging request submission, and charging schedule computation. Finally author evaluated the proposed approach for charging coordination using first come first serve (FCFS) and analyzed it in terms of security and privacy.

Cost Analysis: Sestrem et al. [197] proposed an architecture using BC and side chains for smart grids to make them more scalable and adaptable. It includes three BCs named BlockPRI, BlockSEC, and BlockTST for user privacy, to store user data, and to manage and validate information regarding the energy trade between consumers and prosumers respectively. A Loom network, based on the side chain, is used to develop these BC. Loom network uses the DPOS consensus algorithm. The proposed architecture includes three layers namely the user layer (registers users in the blockchain), the protocol layer (uses OSGP protocol to model data package), and the blockchain layer (ensures privacy

security, and trust). Moreover, evaluation was done in terms of several transactions per second, and smart contract cost and results show it is feasible for use.

Authentication: In 2021, Wang et al. [202] proposed a secure, reliable, and efficient mutual authentication protocol for smart meters. The proposed approach resolves identity authentication issues by combining BC, elliptic curve cryptography, dynamic join and exit mechanism, and batch verification. Furthermore, the authors have analyzed the performance in terms of security and functionality, and computation overhead and the results show the proposed approach is more secure and efficient.

Table XI, summarizes the work done in the BC-smart grid use case.

3) **Summary:** A smart grid is the transmission of power from producer to consumer without the involvement of any centralized system. It allows monitoring of power flow from power generation to power consumption, advanced metering infrastructure, better consumer services, fraud detection, technical losses, and reduces electricity theft. These services are provided as IoT is a significant part of the smart grid. The existing grid system faces challenges like data getting stolen and a centralized system which leads to a single point of failure and alterations. BC technology helps in mitigating these issues and provides transparency and provenance, ensuring the reliability and accuracy of smart grid IoT devices. Along with that, it offers decentralized, immutable, trusted access control and a highly reliable system. Implementing BC to the smart grid has attracted widespread attention. Researchers have worked in different directions to explore the applications of BC in smart grids and make it a more efficient solution. Several authors worked on grid monitoring, device identification, privacy preservation, control access, charging coordination, and cost analysis. In their particular work, authors have used private Ethereum BC, smart contracts, PoW consensus algorithm, and SHA-256 for hashing. For control access, private BC with PBFT consensus algorithm while for cost analysis DPOS consensus algorithm is preferred. Apart from the work done, there are some areas, to be considered in the future. Transaction processing time and data storage can be improved, while computational overheads caused by authentication, during system initialization, can be reduced. Yet some challenges are being faced by BC such as high infrastructural and development costs, scalability, chances of centralization, and an enormous amount of data generated.

G. Industrial IoT

Industrial IoT or industry 4.0, is a revolution in industries. Industrial IoT is a switch from traditional industries to smart industries [87]. IIoT is a combination of a wireless sensor network, communication protocol, and internet infrastructure for monitoring, analysis, and management [87]. IIoT can also be defined as the automation of the conventional manufacturing industry. IIoT is an integration of many technologies like the Internet, IIoT, blockchain, big data, edge, and cloud computing, robotics, human-machine interaction, artificial intelligence, and open-source software [87], [218].

TABLE XII: Summary of Related Work in BC-IIoT

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Tesla et al. [207]	An architecture was developed by combining the smart M3 platform and BC to process and store information related to the interaction between smart components.	Uses tiger tree hashing algorithm to calculate transaction hashes.	-	-	-	-	-
Liu et al. [208]	Proposed a BC-enabled data collection and secure sharing scheme by integrating BC with deep reinforcement learning (DRL) for IIoT.	Uses Ethereum as private BC, deep reinforcement learning (DRL), and PBFT consensus algorithm. Analyzed the proposed scheme against attacks such as eclipse attacks, majority attacks, and terminal device failure.	✓	-	-	-	-
Huang et al. [209]	Proposed a credit-based system that ensures system security and protects the confidentiality of data. Also, a data authority management method was designed to protect sensitive data.	Uses public blockchain network, directed acyclic graph (DAG) structured BC, implemented the system using Raspberry Pi, symmetric key encryption, SHA-256, AES block cipher algorithm.	-	✓	✓	-	✓
Xu et al. [210]	Proposed a BC-based fair non-repudiation service provisioning scheme for IIoT applications. Also designed a service verification method based on homomorphic hash techniques to validate services based on lightweight on-chain evidence.	Uses smart contracts, homomorphic and homomorphism hash function, consortium BC with PoA consensus mechanism, and analysis of the security and efficiency of the proposed scheme.	-	-	-	-	-
Rathee et al. [211]	Proposed a secure hybrid industrial IoT framework for tracing workers' location, product shipment, and product documentation.	Uses blockchain technology, with PoW consensus algorithm and performance is analyzed using NS2 simulator over request time, falsification attack, black hole attack, and probabilistic authentication scenario.	✓	-	-	-	✓
Kumar et al. [212]	Proposed a framework named as BlockEdge, to address some of the issues faced by current IIoT like latency, power consumption, and network usage.	Uses edge computing and lightweight private blockchain technology and analyzed the performance in terms of latency, power consumption, and network usage.	✓	✓	✓	-	✓
Liu et al. [213]	Proposed a BC-enabled PLM (product life cycle management) framework for data exchange and service sharing among the products, factories, business network, and customers.	Uses smart contracts, SHA-256, Hyperledger fabric Java SDK with redundant Byzantine Fault Tolerance consensus algorithm.	-	-	-	-	✓
Rathee et al. [214]	Proposed an approach using BC for secured wireless to maintain transparency and secure activities of smart sensors.	Uses distributed cloud framework using BC, RFID. The analysis is performed in terms of the success rate of the attack, ease of attack detection, falsification attack, and authentication delay.	✓	-	-	-	✓
Manogaran et al. [215]	Introduced a BC-based secured data sharing model named BSDS for inbound and outbound security in data acquisition and dissemination.	Uses BC technology with IoT. Analysis performed in terms of response rate and failure rate.	✓	✓	-	-	✓
Sarier et al. [216]	Proposed a BC-based identity management system. Combining it with off-chain storage ensures GDPR compliance, required to protect user data.	Uses accumulators, BC with off-chain storage.	✓	-	-	-	-
Latif et al. [217]	Proposed a private BC-enabled architecture for secured and trustworthy industrial operations.	Uses sensors, actuators, private BC, ARM cortex lightweight nodes, elliptic curve digital signature algorithm, proof of authentication consensus algorithm and analyzed the performance in terms of execution time, power consumption, and memory utilization	✓	✓	-	-	✓

IIoT architecture involves three layers, the physical layer, the communication layer, and the application layer. The physical layer consists of physical devices like sensors, the communication layer uses network technologies like a wireless sensor network, and the application layer contains different applications using IIoT [87]. Industry 4.0 will bring the revolution by making machines smarter, factories more efficient, processes less wasteful, and higher productivity [219]. IIoT is facing several challenges which need to be addressed. Some of the general challenges being faced by IIoT are interoperability issues, security vulnerability, lack of data analysis, improved resilience, fast adaptability, improved trust, and lower maintenance costs [212], [218]. As the devices are interconnected, they share information directly and are subject to security threats [218]. Because of the tamper-proof and distributed nature of BC technology, it can be proved as a game-changer in the IIoT domain. Some of the practical implementations are, for example in the agriculture industry, iGrow, which asso-

ciates landowners, farmers, investors, and harvest purchasers to make a supply chain for organic food, and Avenues-GT, which supports the commercial trade of agriculture products from farmers securely and transparently [87].

1) Applications of Blockchain in IIoT:

- **MIoT** - BC can be proved as a revolution in the health-care industry, in particular for Medical IoT (MIoT). It can be used to manage security, privacy, trusted ownership, authenticity, interoperability, and autonomous cooperation between MIoT devices [74], [220].
- **Automatic and Secure Micro Payment** - As we are moving towards digitization and IoTized systems where automatic and micro payments are the need of time. BC provides a solution to secure, privacy protected, trustless, and automatic micro payments for IoT devices [220] such as smart meters [37].
- **Supply Chain Logistics** - BC can help in maintaining the authenticity and tracing the products to ensure quality

of the products from raw material to final finished goods and efficient supply of the product [221].

- **Power Industry** - Integrating BC and the power industry has many applications such as the trade of energy, power demand, and power generation schemes that can be stored on the BC network. BC reduces that extra transition cost and makes the transition of power in a more efficient way [87].

2) *Related work*: The research works related to IIoT have been discussed under different categories which are discussed as follows:

Data Collection and Sharing: Manogaran et al. [215] introduce a BC-based secured data sharing model named BSDS for inbound and outbound security in data acquisition and dissemination, as BC controls data gathering and dissemination. Its design goal is to maximize the response rate of the industrial process by reducing false alarm progression (FAP) in IIoT. Analysis shows that the proposed model gains a 5.67% high response rate, and reduces the failure rate by 2.14%.

Network Computing Service: Xu et al. [210] proposed a BC-based non-repudiation service provisioning scheme for IIoT applications where BC is used to record evidence and a service publication proxy and each service is delivered separately using on-chain and off-chain. Moreover, designed a service verification method based on homomorphic hash techniques to validate services based on lightweight on-chain evidence. Uses smart contracts to efficiently settle disputes between service providers and IIoT clients, homomorphic and homomorphism hash function, consortium BC with PoA consensus mechanism. The proposed architecture includes three entities; the service provider, the IIoT client, and the arbitration node. Also analyzed was the security and efficiency of the proposed scheme.

Product Life cycle Management: Liu et al. [208] proposed a BC-enabled data collection and secure sharing scheme. Uses the private BC Ethereum platform to ensure the security and reliability of data shared and deep reinforcement learning (DRL) to achieve the maximum amount of collected data. The proposed scheme is simulated using the python language and Ethereum platform with the PBFT consensus algorithm. Authors have analyzed the proposed scheme and the results show that it provides better security against attacks such as eclipse attacks, majority attacks, and terminal device failure. In line with that, Liu et al. [213] proposed a BC-enabled framework for data exchange and service sharing among the products, factories, business networks, and customers in the product life cycle. First, it proposed the idea of integrating BC with IoT, M2M, and consensus algorithm, and secondly developed a BC information service to maintain the connection between a single node with the BC network. Smart contracts written using GO language are used to automate the alert service in the product life cycle and SHA-256 for encryption with Hyperledger fabric Java SDK with redundant Byzantine Fault Tolerance consensus algorithm. The proposed framework includes mainly five layers; the perception layer (used to collect data using IoT devices like QR codes, RFID tags, and GPS sensors), the off-chain layer (collected data will be processed in BC information service), the BC layer

(which contains smart contracts, consensus protocol, DApps, and cryptography), application layer (includes services and software) and service layer (services like product creation, tracking and tracing, product maintenance, and recycling). Finally, the analysis was presented in terms of latency and throughput and the results show that the proposed framework is scalable, efficient, and feasible for industries.

Secure and Trustworthy Operations: Huang et al. [209] presented a BC-based system with a credit-based consensus mechanism for IoT devices to decrease the power usage in the consensus mechanism, and to ensure system security and efficiency. A data authority management method was designed to protect sensitive data and regulate access to sensor data. In particular, uses directed acyclic graph (DAG) structured BC, implemented the system using Raspberry Pi, symmetric key encryption, SHA-256 to distribute secret keys, AES block cipher algorithm, and a case study of the smart factory was presented. The proposed system is resilient against various attacks such as DDoS, Sybil attacks, and double-spending attacks. In 2019, Rathee et al. [211] proposed a secure hybrid IIoT framework using BC technology for tracing workers' location, product shipment, and product documentation and maintaining transparency among users located at different locations. Recording of information is done using BC technology. Finally, the performance is analyzed using the NS2 simulator and the results show the proposed approach offers 89% success over user request time, falsification attack, black hole attack, and probabilistic authentication scenario. In 2021, Rathee et al. [214] proposed a BC-enabled secured wireless mechanism to preserve transparency and secure each activity of smart sensors. The proposed approach uses distributed cloud framework using BC, and RFID. Mainly it includes registration of sensors on BC and consensus among users and industry providers for the product shipment. Finally, the approach is simulated using the NS2 simulator in terms of probability of attack success, ease of attack detection, falsification attack, and authentication delay.

In the line above work, in 2021, Latif et al. [217] proposed a private and lightweight BC-based architecture for secured and trustworthy industrial operations and implemented it for a food processing plant use case. It uses a low-power ARM Cortex M4 processor, energy-efficient consensus mechanism proof of authority (PoAh). The proposed architecture is used to perform industrial operations such as user and device registration, sensor and actuator data storage, and client service task. It has three layers; the physical layer (sensors, actuators, and microcomputers), the BC service layer (ARM cortex-based lightweight nodes, private BC), and the application layer (which provides services like administration, user management, and task management). Uses sensors, actuators, private BC, ARM cortex lightweight nodes, elliptic curve digital signature algorithm to generate public and private keys, and proof of authentication consensus algorithm. Moreover, the performance analysis in terms of execution time, power consumption, and memory utilization has shown the effectiveness of the proposed architecture.

Identity Management: Sarier et al. [216] proposed a BC-based identity management system. Combining it with off-

chain storage ensures GDPR compliance, required to protect user data. Moreover, it includes a blinded DLRep scheme to provide multi-show unlinkability. For bigger organizations, it replaces the Merkle tree with an accumulator to improve scalability. Major participating entities are credential generators, credential issuers and verifiers, and service enablers. User privacy is achieved by implementing an efficient authentication scheme.

BC-IIoT: Teslya et al. [207] presented the possible ways to integrate BC technology with IoT. The architecture was developed by combining the smart M3 platform and BC along with smart contracts to process and store information related to the interaction between smart components. A core component is a semantic information broker (SIB) to store information and service requests of participants. In particular, uses a tiger tree hashing algorithm to calculate transaction hashes. In 2020, Kumar et al. [212] proposed a framework named as BlockEdge by integrating edge computing and BC, to resolve the challenges such as data integrity, trust, and security. Edge computing helps in achieving low latency and lightweight private permissioned BC ensuring secure and trusted data sharing, accessing, tracking, tracing, and monitoring. The proposed framework includes mainly three parts; IoT-Edge networks, Fog networks, and cloud networks. Along with this authors have analyzed the performance using the simulator iFogSim in terms of latency, power consumption, and network usage.

Table XII, summarizes the work done in the BC-IIoT use case.

3) **Summary:** IIoT is an application of IoT in different industry domains which helps in achieving automation and an efficient industry approach. It offers the ability to interconnect numerous devices, process various data, and reduce human intervention. Still, IIoT is facing various issues, like privacy-related concerns while collecting and sharing data, high costs, high rate of failures, massive data management, and untrusted third parties. Here, BC can be used to mitigate these challenges because of the features offered by BC such as ease of record-keeping, avoiding fraudulent cases, improved transparency, and a decentralized approach. Researchers are exploring different areas for the adoption of BC-IIoT on a large scale. Numerous research works have been done in various application areas like data collection and sharing, product life cycle management, network computing services, secure and trustworthy operations, identity management, and BC-IIoT. For secure and trustworthy operations authors have used DAG, Raspberry Pi, SHA-256, RFID, PoA consensus algorithm, and elliptic curve digital signature algorithm. Whereas for identity management off-chain storage is preferred to ensure GDPR compliance. Ethereum BC platform with PBFT consensus algorithm, smart contracts are written using GO language, SHA-256 with hyperledger with PBFT is used for product life cycle management. While the PoA consensus algorithm with smart contracts was preferred for network computing services. Still, some areas need to be focused on in the future such as the time required to validate a block can be improved, real network computing enabled IIoT platform to add more features, a non-repudiation dispute resolution mechanism for a massive

amount of data generated, integration of various technologies such as edge computing, 3D printing, SDN, NFV to address different requirements like adaptive security, privacy, and trust mechanism. Integrating BC-IIoT offers various opportunities but along with that, some challenges are being faced such as scalability, high infrastructural costs, throughput, and a large number of simultaneous users.

H. Unmanned Aerial Vehicles (UAVs)

UAVs, also known as drones, are self-programmed devices that do not require any human pilot but are managed through mobile applications [222]. These are equipped with sensors and processors. It was first introduced in 1920 for military operations and later on also deployed for civil applications such as traffic management, photography, and shooting, product delivery [223] and it is simply an aerial device without pilot [224]. UAVs are designed in different sizes, large size UAVs are more suitable for defense applications while small-size UAVs are best for civilian applications [224]. Based on altitude, UAVs are categorized as high altitude (used in wide geographical areas with extended battery) and low altitude UAVs (used in normal day-to-day tasks with fast deployment, cost-effective and limited battery) [223]. According to the report of SIPRI (Stockholm International Peace Research Institute), India is one of the top countries for importing drones which is 22.5% of the world's UAVs [224]. According to the report by the Federation of Indian Chambers of Commerce and Industry (FICCI), the adoption rate of UAVs in India and globally is expected to be 885.7 million USD and 21.47 billion USD respectively [223]. Some of the applications of UAVs are product delivery, Military surveillance, aerial photography, traffic control, and management and cinematography [225]. Some of the general challenges faced by UAVs are security and privacy, and latency. Some of the application areas of UAVs are defense, agriculture, transportation, delivering goods, and surveying. Integrating BC with UAV has great potential. For example, military information is highly sensitive and confidential thus it must be safe and secured and BC can be a good choice for this [224]. Some of the practical implementations of UAVs are companies like Matternet and Flirtey, which uses UAVs for the delivery of medicines in rural areas [224].

1) Applications of Blockchain in UAV:

- **Data Storage and Verification using UAV** - The data collected with the help of UAVs can be directly transmitted to a cyber-physical system connected through BC. Each block will contain details that are scanned through the UAVs and the time of the creation of the block. With the integration of BC with UAV, information can be stored and monitored efficiently [226].
- **BC-based UAV Surveillance** - Video surveillance is very important whether it is at the border, at traffic lights, DAM's or in our homes. All these tasks can be performed by using UAVs. But because of the dynamic nature of the UAVs, they also face some challenges like trust and data authentication, finding the optimal path, security, reliability, unauthorized access to the UAVs ID, and DoS attack. BC can mitigate these challenges, BC ensures the

security of information by sharing and verifying the data in a distributed manner.

- **Blockchain-based UAV system for automation of supply chain** - Supply chain and logistics require manpower from the production of any product to its distribution and sales. Automating all of these tasks leads to reduced manpower, on-time deliveries, and increased profits. UAVs can help in surveying the stocks, collecting data, and dispatching products. But at the same time automating these tasks will also lead to security threats. BC technology can be used to maintain trust and security and store data. The supply chain requires the collection of data which is generally performed by humans and is prone to errors. This is where UAVs can be used to collect the data.

2) *Related work*: The research works related to UAVs have been discussed under different categories which are discussed as follows:

Communication: Kumari et al. [223] presented a survey on BC-based softwarization for UAV networks. Provides a brief introduction about BC and UAV. Highlighted the challenges faced by the conventional UAVs approach such as security is a major concern. To resolve the challenges, the authors have proposed a BC-based UAV softwarization architecture for secure UAV networks to provide dynamic, flexible, and on-the-fly decision capabilities. The proposed approach includes four layers; the infrastructure layer, the BC middleware layer, the control layer, and the application layer. Uses public BC Ethereum client to store UAV communications and SDN controller information as a transaction with IPFS to store data. Moreover, discussed the challenges in integrating BC-UAV such as interoperability, data processing latency, data security, real-time deployment, and BC standardization.

Privacy & Security: Rana et al. [227] and Abualsauod et al. [228] both worked to choose the same direction i.e., security and privacy in UAV. In 2019, Rana et al. [227] proposed an approach to improve the security of UAVs using BC. Integrating BC with UAV helps in achieving additional security in transmitting signals as BC uses private key cryptography and peer-to-peer network. In particular, uses BC, image gathering and sensing of UAV, SHA-256, timestamp (to keep a log of a transaction between the server and drone with its GPS location), and GPS location (will be added by UAV in the block). In line with that, in 2022, Abualsauod et al. [228] proposed a solution to resolve security and privacy-related issues in UAV-assisted IoT applications using BC. In particular, the authors choose to use Ethereum BC, SHA, and elliptic curve cryptography with numerous machine learning algorithms like K Nearest Neighbour and Naive Bayes. Furthermore, the authors analyzed the proposed solution in terms of system utility, latency, and processing time with overall attack detection accuracy. Results show that with the implementation of BC, latency and processing time are increased which increases the overall time consumption and reduction in attack rates.

Data Collection: Islam et al. [229] and Xu et al. [230] worked in the same direction i.e., data collection using BC through UAVs. Islam et al. [229] proposed a BC-enabled secure scheme for data acquisition through UAVs and IoT de-

vices. It includes two-way validation using the pie hash bloom filter and digital signature algorithm. Using the consortium BC Ethereum platform, Geth was used as an Ethereum client and proof of authority (PoA) consensus algorithm. Furthermore, presented a performance analysis in terms of connectivity, energy consumption, and security analysis against various threats such as man in the middle, key spoof resistance, data tampering resistance, and resistance against intrusion and reply attacks. A simulation was performed using MATLAB and python. In 2020, Xu et al. [230] proposed a BC-based UAV-assisted IoT, a data collection secured and energy efficient scheme. An adaptive linear prediction algorithm was designed to reduce energy consumption and based on this algorithm, a data transmission scheme for BC-based UAV-assisted IoT is also proposed. BC-enabled UAVs consist of three main entities; IoT devices, the UAV swarm, and the charging station and management swarm. Uses BC in the UAV swarm (to record forwarding), private chain, edge computing, and asymmetric encryption for acquiring data security. The proposed approach has three special attributes which make it suitable for UAV-assisted IoT namely; every forwarding is defined as a transaction and each transaction is initiated by the management server, difficulty of mining, and charging strategy. Moreover, performance was evaluated using MATLAB in terms of security, accuracy, energy efficiency, training overhead, and training delay. Simulation results show proposed scheme offers better security and is energy-efficient.

Health Monitoring: In 2019, Islam et al. [231] proposed a BC-based scheme for secure monitoring using UAVs outside the homes in smart cities. The main components involved are the user (citizens), UAV (provides extended connectivity and low power transmission), and MEC (works as a validator in BC). It accumulates health data using wearable sensors and transmits it to the nearest MEC server using UAV. Uses the private Ethereum BC platform. Furthermore, performance was evaluated in terms of processing time, expected transmission of data, validation time, and energy consumption using MATLAB and python. In line with that, in 2020, Islam et al. [232] proposed a BC-based secure healthcare scheme called BHEALTH in which health data is collected using UAVs. Uses consortium BC Ethereum BC platform with proof of authority (PoA) consensus algorithm, and time division multiple access (TDMA) protocols for communication. Core entities involved in the proposed scheme are the body sensor hive (BSH) and server. HEALTH does not have any reward for validators. Moreover, the author presented a security and performance analysis in terms of throughput, energy consumption, and processing time. BHEALTH is resilient against numerous threats such as man in the middle, unauthorized access, illegal data tampering, and reply attack.

In 2021, Raj et al. [233] proposed an approach based on BC, for health monitoring using UAVs. In particular, healthcare data is collected using sensors and delivered using UAV to servers, and then saved using BC. Authors have highlighted the threats that are faced by UAVs during transmissions such as reply attacks, unauthorized access, and man-in-the-middle-attack. Furthermore, the authors have used the threat model to analyze security aspects, performance is analyzed

in terms of energy consumption, individual processing time, and data transmission. Authors Aggarwal et al. [234] proposed an effective and efficient, three-layered architecture for the collection, processing, and transmission of medical data using UAVs, ensuring security and privacy during the transfer of medical data. Three layers are patient-generated data and clinical data, BC network of UAV, and data analytics and visualization. In particular, authors have used Ethereum BC with the PoW consensus algorithm. For analysis, the authors have focused on three major attacks; confidentiality attack, integrity attack, and availability attack.

Spectrum Trading: Qiu et al. [235] proposed a BC-based privacy-preserving scheme for trading and sharing of the spectrum to resolve issues related to privacy and security. Uses consortium BC technology, edge computing, and a proof of work consensus algorithm. Major entities involved are trusted authorities, spectrum providers and requestors, edge computing nodes, and smart counters. Also for efficient pricing of spectrum, a non-uniform pricing algorithm and a distributed uniform pricing bargaining algorithm are designed. Analysis shows that the proposed scheme offers better security and privacy.

UAV Visualization: Pathak et al. [236] proposed BC-enabled UAV virtualization for IIoT called AerialBlocks to provide secure and persistent UAV services to the end-users with the help of BC to ensure security, privacy, service quality, and transparency. It includes three actors; the UAV owner (takes care of the maintenance of the UAV), end-users (registers to the platform to access UAV service), and the virtual UAV service provider (the link between the UAV owner and end-users). The proposed architecture includes three layers; the application layer (web-based applications for end-users), the virtualization layer (the connecting layer between the physical and application layer), and the physical layer (Physical UAVs available on the ground for various UAV missions). Uses permissioned BC (to ensure that only registered end users and UAV owners can access), smart contracts (used to store transactions and business regulation), and a combination of proof of authentication and practical byzantine fault tolerance consensus algorithm to ensure lightweight validation for fault tolerance.

Authentication: Tan et al. [237] proposed a BC-enabled authentication approach for industrial UAVs. In particular, uses hyperledger fabric and smart contracts with the Kafka consensus algorithm. During designing the particular approach, the authors considered some goals; confidentiality, mutual authentication, conditional anonymity, perfect forward secrecy, backward secrecy, resistance to cyber-attack, and lightweight. Moreover, a security analysis was performed based on two problems i.e., elliptic curve discrete logarithmic and computational Diffie Hellman problem, to ensure the security provided by the proposed approach.

Table XIII, summarizes the work done in a BC-UAV use case.

3) **Summary:** UAVs are flying drones equipped with sensors, deployed for traffic applications, photography, and surveillance. To achieve such services IoT is an important requirement. Security and privacy issues because of an untrusted

broadcast, and a single point of failure due to a centralized system are some of the challenges being faced by the existing approach. Combining BC with UAV brings numerous opportunities such as more secure, autonomous, flexible, improved service quality, and user experience. Various research works have been carried out to explore the applications of BC with UAVs. In particular, the authors explored the applications of BC using UAVs for communication, data collection, health monitoring, spectrum trading, UAV visualization, and improved privacy and security. Authors preferred consortium BC, Ethereum BC, IPFS, and SHA-256 with PoA consensus algorithm. For spectrum trading authors used BC with edge technology, PoW consensus algorithm, and smart contracts as authors preferred Proof of authentication with the PBFT consensus algorithm. Some of the future aspects that need to be considered for widespread adoption of BC-enabled UAVs are integrating AI and ML-based algorithms, and satellite-based networks for UAV visualization, implementing UAVs for different use cases like UAV-driven healthcare use cases, consumer-friendly drones where mobile phones can act as servers. Along with the benefits offered by integrating BC-UAV, there are some challenges such as interoperability, data processing latency, data security, real-time deployment, and BC standardization.

IV. TECHNICAL ASPECTS AND CHALLENGES

The integration of BC-IoT has been broadly used in different fields because of its key attributes like decentralization, data immutability, and trustworthiness. This segment presents the most difficult issues identified with the execution of BC for IoT, specifically, Security, Privacy, Scalability, Access Control, Processing Power, Data Storage (On Chain versus Off-Chain), and Consensus algorithms. Besides, the effect of these issues and the work done on these aspects are talked about in this part.

A. Scalability

Scalability is defined as the ability of a system to handle the increase or decrease in terms of size, volume, performance, and cost [239]. **When the number of active users increases in blockchain, a scalability issue arises that affects blockchain performance [240].** For instance, in the bitcoin blockchain, the number of transactions that arrives can vary, maybe 10 or maybe 100 but irrespective of the number of arriving transactions, the blockchain process only some fixed number of transactions relying upon the size of the block (such as the size of bitcoin block is 1 MB and can process only seven transactions per seconds) [29]. The number of transactions processed per second in blockchain relies upon a wide range of factors like network latency, consensus protocol, and CPU processing power. This restricted block size cannot process a large number of transactions at once which causes delays in transactions [63]. The system must be scalable so that it must be able to handle the sudden increase and decrease in the transaction load. Because of the decentralized structure of blockchain, each node must process each transaction which leads to low capacity and low speed of transaction

TABLE XIII: Summary of Related Work in BC-UAV

Reference	Main Contribution	Relevance to BC	Targeted Characteristics				
			Authenticity	Integrity	Confidentiality	Provenance	Privacy
Islam et al. [231]	Proposed a BC-based scheme for outdoor health monitoring called BHMUS using UAVs.	Uses Ethereum BC, UAV, MEC, and python language. Also, evaluation of performance is done in terms of processing time, expected transmission of data, validation time, and energy consumption.	-	-	-	-	-
Qiu et al. [235]	Proposed a scheme for preserving privacy, secure trading, and sharing of the spectrum along with a Stackelberg game to obtain maximum spectrum pricing. A non-uniform pricing algorithm with low complexity and a distributed uniform pricing bargaining algorithm is also designed.	Uses consortium BC technology, edge computing as a network enabler to offload the computation-intensive proof of work puzzle. Also, an analysis of performance is done in terms of transaction security and privacy.	-	✓	✓	-	✓
Islam et al. [229]	Proposed a BC-enabled secure scheme for data acquisition through UAVs and IoT devices.	Uses consortium BC Ethereum platform, Geth was used as Ethereum client and proof of authority (PoA) consensus algorithm and performance is analyzed in terms of connectivity and energy consumption.	✓	✓	-	-	✓
Rana et al. [227]	Proposed an approach for maintaining the privacy, and security of UAVs by using BC.	Uses cloud for data storage with blockchain, SHA256, image gathering, and sensing of the UAV. time stamp and GPS location.	✓	-	-	-	✓
Kumari et al. [223]	Proposed a BC-based UAV softwarization architecture for secure UAV networks.	Uses public BC Ethereum client to store UAV communications and SDN controller information as a transaction with IPFS to store data.	✓	✓	✓	-	✓
Islam et al. [232]	Proposed a UAV-assisted healthcare scheme that collects health data from users through UAV.	Uses consortium BC Ethereum BC platform with proof of authority (PoA) consensus algorithm, time division multiple access (TDMA) protocols for communication. Also analyzed were the security and performance.	✓	✓	-	-	-
Xu et al. [230]	Proposed a BC-based data collection scheme. An adaptive linear prediction algorithm was also designed to reduce energy consumption.	Uses BC private chain, edge computing, asymmetric encryption, and MATLAB to analyze the performance in terms of security, accuracy, energy efficiency, training overhead, and training delay.	-	-	-	-	✓
Pathak et al. [236]	Proposed BC-driven UAV virtualization for IIoT called AerialBlocks to provide secure and persistent UAV services to the end-users with the help of BC to ensure security, privacy, service quality, and transparency.	Uses permissioned BC, smart contracts, and a combination of proof of authentication and practical byzantine fault tolerance consensus algorithm.	-	-	✓	-	✓
Raj et al. [233]	Proposed an approach for health monitoring using UAV. A threat model is used to analyze security aspects. Results are analyzed in terms of latency, block size, and throughput.	Uses Ethereum BC, smart contracts, mobile edge computing, and smart sensor devices.	-	✓	-	-	-
Aggarwal et al. [234]	Proposed a three-layered architecture for the collection, processing, and transmission of medical data using UAVs.	Uses Ethereum BC with PoW consensus algorithm to verify medical data.	✓	✓	✓	-	✓
Abualsaud et al. [228]	Proposed a solution to resolve security and privacy challenges in UAV-assisted IoT applications. Analyzed the proposed solution in terms of system utility, latency, and processing time with overall attack detection accuracy.	Uses Ethereum BC, cloud platform, elliptic curve cryptography, SHA algorithm (to protect data privacy), multiple ML algorithms, K Nearest Neighbours, and Naive Bayes.	✓	✓	-	-	✓
Tan et al. [237]	proposed a BC-enabled authentication approach for industrial UAVs.	Uses hyperledger fabric and smart contracts with the Kafka consensus algorithm.	✓	✓	✓	-	✓

processing [241]. The Sharding process partition the network into numerous small subsets known as shards to avoid the duplication of resources such as communication, data storage, and computation overhead and improves the blockchain's performance [242]. Each shard includes a different set of transactions instead of the whole network processing the same transaction. This helps in improving the throughput of the network [243]. As IoT is a collection of connected devices and IoT is becoming the Internet of Everything (IoE), that means a lot of connected devices are involved or each and everything is connected, which means a lot of transactions occur and enormous data will be generated [3], [24]. Therefore, it is important to maintain the scalability in BC-IoT. Table XV encapsulates the technical aspect of the scalability of BC.

1) **Challenges related to the Scalability::** In this segment, we are reviewing and discussing the scalability challenges

faced by blockchain for IoT.

- **Throughput:** In general, throughput is defined as the rate at which something is processed. In the context of blockchain for IoT, throughput implies the **number of transactions processed per second**. If we take bitcoin as an example then in bitcoin only seven transactions per second can be processed while existing payment systems like VISA can process 4000 transactions per second [29], [240]. Here, processing seven transactions per second means, irrespective of the input transactions coming at any rate, that the system is not scaling up with the inputs and giving a flat response, which naturally relies upon the underlying available hardware, the number of peers connected, and its available computational power [63].
- **Storage:** Whenever a new transaction comes, all the new transactions get accumulated in the pool of unconfirmed

TABLE XIV: Role of Blockchain in IoT Applications for Various Use Cases

Application	Use cases	Advantages of using blockchain										Blockchain related Challenges	Deployment
		Decentralization	Provenance	Non-Repudiation	Anonymity	Immutability	Availability	Auditability	Automation	Lower Cost	Confidentiality		
Healthcare	Electronic Health Record	L	H	M	M	H	H	L	H	L	H	Scalability, Chances of centralization	
	Drug Supply Chain	H	H	M	M	H	L	H	L	L	L	Compliance to privacy laws, Throughput, Scalability, and Immense data management	
	Health Insurance Claim	H	H	M	L	H	L	L	H	L	H	Throughput, Data storage, Number of concurrent users	
Smart Home	Automated Home Appliances	L	M	H	L	H	H	H	H	M	M	Scalability, Interoperability	
Smart Cities	Digital Identity	M	H	H	L	H	H	H	M	L	H	Massive data storage, Scalability, Chances of centralization	
	Smart Governance	H	M	H	M	H	H	H	M	L	H	Legal issues, Updating smart contracts, Defining protocols for being decentralized systems, Enormous data storage	
	Online Education	H	M	H	L	H	H	M	M	M	M	Operational cost of transaction, Throughput, Data storage, Large number of simultaneous users, and Revoke a certification before its expiration	
	Smart Transportation	H	H	H	M	M	H	H	H	M	L	Interoperability	
Supply Chains & Logistics	Food Supply Chain	H	H	H	L	H	M	H	L	L	L	Data management, Interoperability, and Scalability	
	Pharmaceutical Supply Chain	H	H	M	M	H	L	H	L	L	L	Legal issues, Interoperability, Binding the physical and digital	
	Automotive Supply Chain	H	H	M	M	H	H	H	H	L	L	Legal issues, Interoperability, Binding the physical and digital	
Autonomous Vehicle	Electric Vehicle Charging	H	H	H	M	H	H	H	H	L	L	High infrastructural costs	
	Smart Insurance	M	H	H	M	H	H	H	M	L	M	Massive data storage	
	Self Driving Vehicle	M	H	H	L	H	H	H	H	L	L	Scalability, Chances of centralization	
	Digital Service Record	H	H	H	M	H	H	H	L	L	H	Scalability	
Smart Grid	Peer-to-Peer Trading	H	H	H	L	H	H	H	H	L	L	Scalability, Chances of centralization, High infrastructural costs	
	Energy Trading in Electric Vehicle	H	H	H	M	H	H	H	H	L	L	High infrastructural costs	
	Power Generation and Power Distribution	H	H	H	L	H	H	H	M	L	L	High infrastructural costs	
	Secure Equipment Maintenance	H	H	H	L	H	H	H	M	L	M	Scalability	
IIoT	Healthcare Industry	H	H	H	M	H	H	M	L	L	M	Scalability, Chances of centralization	
	Power Industry	H	M	H	L	H	H	H	H	L	H	High infrastructural costs	
	Manufacturing Industry	H	M	H	L	H	H	H	H	L	L	Throughput, Data storage, Large number of simultaneous users	
UAVs	Surveillance	L	H	H	L	H	M	H	H	L	H	Physical and security attacks, Breach of privacy, Legal issues, Light-weight consensus algorithms for resource-constrained robots	

H High Relevance

M Medium Relevance

L Low Relevance

transactions, and miners pick a transaction to validate and verify the transaction. As the size of the block is limited, so the number of transactions that can be stored in the block is also restricted. Miners pick the transactions with a higher processing rate and transactions with less processing rate get delayed [29]. For example, in the food supply chain, a large number of IoT-enabled devices are used which leads to a huge amount of transaction

data (may be audio, video, images) to be stored on the blockchain which leads to large storage and higher costs and directly affects the scalability [152].

B. Security and Privacy

In general, Security is defined as the protection of the system against malicious attacks, unauthorized access, modifications, and deletion. In the context of the blockchain, security

TABLE XV: Summary of Technical Aspect - Scalability

Reference	Technical Aspect	Proposed Solution
Atlam et al. [3]	All the transactions are stored in a ledger that is shared among all the nodes and the size of the blockchain increases continuously, which has a direct effect on the speed.	No solution is proposed.
Gao et al. [238] & Zheng et al. [29]	Discussed the continuous increase in the size of the BC which results in increased cost of storage, BC becomes bulky and also leads to a reduction in distribution speed in the network.	Both have discussed two solutions to resolve this issue: storage optimization of data and redesigning blockchain.
Reyna et al. [24]	Talked about the size of the BC, as the size grows nodes required more resources, which also has an effect on performance, synchronization time increases.	Suggested off-chain storage and inter-planetary file system.
Mahmoud et al. [40] & Xie et al. [84]	Discussed the ever-growing and continuously increasing size of the BC.	Highlighted the solutions like BC pruning and Lightning network and storing data off-chain using DHT (Distributed Hash Table) respectively.
Monrat et al. [63]	As BC is distributed in nature, copies of the ledger are stored at each node which has a direct effect on throughput and latency. In the PoW algorithm resources are wasted in solving the puzzle which also results in low throughput and high latency. Also, the PoW algorithm is CPU intensive leading to high electricity consumption.	Suggested using DCS (Decentralized, Consistent, and Scalable) theorem.
Rupasena et al. [152]	Discussed FSC, transaction data generated is extremely large, leading to the blockchain ledger growing continuously.	Also discussed that data about the product in FSC is not required after a certain period but as BC is an immutable ledger. In contrast to this fact, suggested an off-chain storage scheme and a technique to reduce the growth of off-chain storage.

means the protection of transaction information and data in a block, detection of threat, and prevention of threat [244]. As blockchain is distributed and decentralized in nature it allows nodes to join the network and can view all the details of the transactions occurring in the network. It is crucial to maintain the integrity of the transactions, and availability of data, and to prevent double-spending, the system must be secured [245]. According to a report titled "State of IoT security", cyber-attacks on IoT have increased by 22% [246]. As BC-IoT implies a huge number of connected devices in a distributed and decentralized manner, without security, these connected devices can be hacked, and once the hacker gains control, they can tamper with the data. So all the connected devices must be secured [24]. Privacy means protecting stored, transmitted, and processed private information such as data, identity, and location [247]. Especially in permissionless blockchain anyone can join the network and sometimes the nodes present in the network are the malicious ones whose aim is to collect the information from the network [247]. In the context of the blockchain, maintaining privacy means performing a transaction without leaking the user's identification information [244]. The privacy and security of data can essentially be achieved by fulfilling five basic criteria such as confidentiality, availability, integrity, authentication, access control, and privacy requirements [247]. As blockchain is distributed and decentralized in nature, transaction privacy is not guaranteed. The issue with blockchain is that users cannot stay anonymous [84]. Especially, this is a challenge in public blockchain as anyone can join the network and all the previous and current transactions are visible [29]. If somehow all these transactions can be linked then the identity of the person who is behind the transactions gets revealed. So it is important to achieve privacy in blockchain [245].

IoT-driven devices collect a lot of data and personal information from the surrounding environment and they communicate with each other. When such data is managed by some central authority then the user's privacy is at risk. Here

blockchain technology can help maintain IoT privacy [248]. As BC supports distributed and decentralized features but with this also some challenges arise. Table XVI, encapsulates the technical aspects of the security of BC.

1) **Challenges related to the Security & Privacy::** This section highlights the challenges related to the privacy and security of the BC for IoT.

- **Transaction Privacy Leakage:** Blockchain uses asymmetric key cryptography as it uses public key and private key pairs for transactions. The real identity of the user does not get revealed as a blockchain-generated address was provided to the user and all the transactions occur between these addresses to hide the original identity of the user. But still, the privacy of the transactions is not guaranteed since all the transactions that occur in the network are visible to all the nodes present in the network and still, some detectable hints can divulge the identity of the users. These transactions can be linked or the transaction history can be linked to disclose the user's identity [29], [249]. Various researchers propose methods against privacy to link pseudonyms with IP addresses [63].
- **Security of Private Key:** BC uses asymmetric key cryptography, which means it uses public and private key pairs. If the private key of the user is compromised then all the transactions will be leaked. Maintaining the security of the private key is of utmost importance [40], [249].
- **Non-Compliance to Privacy Laws:** As blockchain is a distributed ledger, participating nodes are from across the world, which raises privacy issues. A key point is that the miners are spread across different countries and thus it is not clear which privacy law(s) will be applied [250]. For instance, this may be decided based on the location of the miner who mined the new block or the location where the transaction occurs [250].
- **Selfish Mining:** Selfish mining was first reported by Eyal

TABLE XVI: Summary of Technical Aspect - Security and Privacy

Reference	Technical Aspect	Proposed Solution
Islam et al. [253]	Highlighted the security, trust, and privacy concerns in IoT-enabled smart homes.	Proposed a blockchain-based smart contract approach to resolve security and privacy issues in IoT devices.
Zhao et al. [254]	Highlighted the remote data integrity checking and involvement of third parties.	Proposed a blockchain-driven privacy-preserving scheme for IoT using EC-EIGamal cryptosystem, bilinear pairing, and aggregated signature.
Rahman et al. [255]	Discussed the security and privacy issues with IoT devices and how distributed ledger and blockchain technology had resolved these issues.	Proposed architecture for smart buildings called DistBlockBuilding (disseminated block building) for safe and secure data transfer.
Agrawal et al. [26]	Discussed the open issues in IoT i.e. lack of trust and single point of failure.	To resolve this issue, the author proposed a blockchain-based IoT security solution.
Al et al. [256]	Highlighted the smart healthcare system and the issues such as security and privacy of data.	Proposed a blockchain-based privacy-preserving architecture for healthcare data to attain accountability, integrity, and security.
Azbeq et al. [257]	Highlighted the IoT-enabled devices such as wearables and medical sensors for diabetes self-management.	Proposed a blockchain-based architecture for self-managed follow-ups. The proposed architecture includes connected devices, blockchain networks, smart contracts, and medical teams.
Dorri et al. [172]	Highlighted the core components and functions of IoT-enabled smart home.	Also proposed a blockchain-based architecture to improve security in terms of confidentiality, integrity, availability, and performance evaluation in terms of packet overhead, time overhead, and energy consumption.
Dwivedi et al. [258]	Talked about IoT and remote patient monitoring and also the concerns related to privacy and security such as the transfer of medical data.	Highlighted the security concerns and proposed a blockchain-based architecture for IoT devices.
Mohanty et al. [259]	Highlighted the concerns related to the IoT such as resource constraints, centralization, and lack of privacy, and the advantages provided by blockchain technology.	Proposed an efficient lightweight integrated blockchain architecture and deployed in the smart home environment.
Ouaddah et al. [260]	Highlighted the access control challenges in IoT and how blockchain can be useful to resolve this challenge.	Proposed a decentralized, pseudonymous, and privacy-preserving framework based on blockchain to manage access control.
Qian et al. [261]	Presented the opportunities IoT provides and also the challenges it carries like privacy and security issues.	Highlighted the three layers of IoT and the security issues at each layer. Proposed a decentralized scheme for enhancing security based on blockchain for different IoT devices.
Si et al. [262]	Highlighted the issues related to conventional IoT information-sharing approaches such as positioning security problems.	Proposed blockchain-enabled information sharing IoT security framework by using a double chain model and improved practical byzantine fault-tolerant consensus algorithm.

and Sirer [251]. When any malicious node mines the block but does not reveal that block and starts maintaining his/her private blockchain and still the other blocks are busy mining that block and the malicious node starts mining the next block without any competition and when this malicious node's chain becomes longer than the original chain then he reveals that chain. At this point, honest miners think that as the selfish miner's chain is longer, has a large number of blocks mined, done more proof of work, this is the original chain and starts mining and adding the block to the selfish miners' chain. Before the private branch is revealed the honest miners are wasting their resources [252] on a useless branch [29], [238].

- **51% Attack:** It is one of the most well-known security attacks and is also known as a majority attack. In this attack, if the hashing power of an individual miner or a pool of miners becomes more than 50% of the complete blockchain then the attacker or the malicious node can roll back the transaction, cause a double-spending problem, and modify the order of transaction [63], [238], [249].

C. IoT Data Storage

Data storage refers to storing or recording data or information using some storage medium so that when required it allows easy retrieval of stored data. In IoT, the collection of devices leads to the generation of a huge amount of data that needs to be efficiently stored for easy access and fast processing. Since IoT devices are characterized by less computational and storage resources thus the generated data is to be stored at some other location. In conventional methods, data is stored in

a centralized infrastructure that suffers from security, privacy, and single-point-of-failure. Using blockchain, IoT data can be stored in a distributed manner (i.e, replicated at all the nodes in the blockchain network). However, it is a major concern how blockchains can cater to such data storage demands from IoT systems. On the one hand, the distributed ledger helps in improving the security and availability of the stored data and makes a blockchain-based IoT system decentralized. On the other hand, the distributed nature of the database results in a storage challenge because with time IoT devices will exponentially increase in number and blockchain does not allow delete operations since is designed to be an append-only database.

Table XVII encapsulates the data storage aspect of BC.

1) Challenges related to the IoT Data Storage: This section aims to bring the focus of the readers toward the challenges related to data storage. The continuous increase in the size of the blockchain will increase the difficulty for the full nodes to continue their participation in blockchain-based IoT systems. As a result, there will be less number of full nodes driving the blockchain at a given point in time making the system less decentralized. Variable block sizes are not the optimum solution to solve this issue. If we try to store a large number of transactions in a single block this will put an additional strain on full nodes. The speed to process a transaction depends on block size and block interval. Increasing the block size will improve the throughput but take more time to propagate the block to other nodes and reducing the block interval reduces latency but leads to instability [263].

D. Consensus Algorithm

Blockchain is distributed and decentralized in nature, which means the nodes are geographically spread. Whenever a new

TABLE XVII: Summary of Technical Aspect - Data Storage

Reference	Technical Aspect	Proposed Solution
wang et al. [34]	Discussed the potential blockchain design in IoT applications and also discussed possible solutions to reduce storage costs.	Discussed the off-chain storage in which data can be stored separately at another place and for indexing using a pointer.
Hepp et al. [264]	Discussed the storing data in the chain itself, i.e. on-chain, which leads to the question of how much data we can store in the main chain. Also discussed off-chain storage and the challenges in maintaining the link between the hash stored in the main chain and the physical storage location.	For on-chain storage, the size of the block can be variable to store data while for off-chain storage, suggested solutions like smart contracts and Distributed hash tables to maintain the link between hash in the chain and physical storage.
Eyal et al. [263]	Discussed the alternatives to improve the latency and bandwidth of the blockchain.	To improve the performance of the blockchain, the author talked about federated chains, also known as side chains.
Back et al. [265]	Discussed the performance issues of blockchain and their solutions.	Discussed the Pegged chain and its features.
Lu et al. [266]	Present the comparison between on-chain and off-chain regarding what data should be stored on-chain and off-chain.	Suggested not to store private data on-chain and raw data can be stored off-chain while its hash is stored on-chain.

TABLE XVIII: Summary of Technical Aspect - Consensus Algorithm

Reference	Technical Aspect	Proposed Solution
Fernandez et al. [64]	Discussed the power consumed by the PoW consensus algorithm. PoW has a certain level of difficulty but at the same time also consumes a lot of energy.	Highlighted the solutions like PoS (Proof of Space) also known as Proof of Capacity (PoC). Some other consensus mechanisms which consumes less energy are PoS.
Reyna et al. [24]	Highlighted the disadvantages of the PoW consensus algorithm like high latency, low transaction rate, and high energy consumption.	Suggested using another alternative algorithm like PoS, DPoS, LPoS, PoB. Also suggested using private BC where the number of participants is limited.
Mahmoud al. [40]	Discussed the PoW algorithm in which miners solve difficult puzzles which consume a lot of electricity.	Suggested using the Proof of Stake (PoS) algorithm, one who has more stake value will get the chance to append the block.
Alsunaidi et al. [268]	Discussed the technical aspects such as node identity management, power consumption, throughput, and block creation speed.	No solution is proposed.
Mingxiao al. [267]	Discussed that the nodes that have high hashing power (computation power) will get the right to mine the block and get the reward for mining the block, which forces people to upgrade their hardware and these systems consume a lot of energy.	No solution is proposed.

transaction arrives it must be validated by every node present in the network and only after validation, each node updates its copy of the ledger. This validation is performed by creating a general agreement between the nodes by using some algorithms known as consensus algorithms. As Blockchain is a distributed and decentralized approach, there is no centralized authority to validate and verify the transaction but with the help of the consensus algorithm, they ensure that each block added to the network is valid and verified, and agreed upon by all the nodes otherwise the challenges like double-spending attack can occur. Consensus algorithms help in maintaining the integrity of the system and work against double-spending attacks [24]. Consensus Algorithms help in maintaining the sanctity of the data recorded on the blockchain [244].

As IoT involves a lot of connected devices and a large number of transactions occur. To involve each node and each node having equal rights, consensus algorithms are useful. Consensus algorithms help in creating consensus among the untrusted parties involved in the public blockchain. Table XVIII, encapsulates the technical aspect consensus algorithm of BC.

1) **Challenges related to the Consensus Algorithm:** Some of the challenges related to the consensus algorithm are presented in this section. The most commonly used consensus algorithm is PoW but it also has some limitations such as waste of resources meaning the nodes with high hashing power get more chance to mine the block and for this purpose, nodes spend a lot of money on upgrading hardware. These machines consume a lot of energy in solving puzzles [267]. But if the hashing power of the mining pool is more than 50% then it will be a concern for the network as they have control of the network and they can reverse the transactions [267]. Other than this, PoW is also not suitable for real-time payments because of the creation speed of a block [60]. Also, pool mining is

possible in PoS (proof-of-stake) and difficult to prevent [60].

E. Processing Power

Whenever a new technology comes into the market, one of the things that need to be considered before its adoption is that it must be energy efficient. In the case of BC technology, the mining process requires very high computational power and modern hardware resources. BC is a distributed and decentralized approach, whenever a new transaction occurs it is validated by generating the consensus between the participating nodes [3]. Every time a new transaction occurs it is broadcast to all the other users in the network and miners start mining the block for this, they are using a considerable amount of computer power. It is also a waste of resources when each node repeats the same process [84].

Let us take bitcoin as an example, for validating the transactions PoW consensus algorithms are used which requires a high amount of energy with modern hardware [63]. Depending upon the resources available the transaction processing speed in bitcoin is very less compared to other existing systems such as VISA payment systems. So it is very important to increase the processing speed in the blockchain. IoT includes several divergent types of devices with various computing capabilities and all of them will not be able to run the same encryption algorithm at the required speed [14].

Table XIX encapsulates the processing power aspect of BC.

1) **Challenges related to the Processing Power:** Each miner present in the network starts mining the block and the one who mines the block first will get the chance to append the block to the blockchain with some corresponding reward. To receive the reward for mining the block, each participating node starts mining the block which requires a huge amount of energy. As each node is repeating the same process, this

leads to a waste of resources. The energy consumption rate of the Bitcoin network has set a new benchmark. According to a report by the bitcoin energy consumption index, VISA has consumed a total of 740,000 Gigajoules of energy for all its operations which is less than the energy consumed in the bitcoin mining process [271]. Also according to the same report carbon footprint of a single mined bitcoin is equal to the worth of mining gold [271].

V. LESSON LEARNED AND FUTURE WORK

BC for IoT is a profoundly dynamic research topic. There are many research areas with significant degrees of challenges that should be handled in a modern way. Furnishing new arrangements should be limited to specific prerequisites and limitations like low complexity and reliability. This segment momentarily talks about lessons learned from related works and conceivable future directions in incorporating BC and IoT.

A. Healthcare

1) *Lessons Learned:* Despite the hype around smart healthcare system, it faces many challenges, such as data sharing, data integrity, privacy, and access control. Here BC technology has proved the potential to resolve these challenges such as patient details, doctor's records, patient's medical history, and pharmaceutical supply chain can be stored on BC. Moreover, Integrating BC with healthcare will reduce the counterfeit medicines and instruments supplied to hospitals and can inform the authorities about discrepancies because of the transparency in the network. But at the same storing a large amount of data directly on the main chain is a challenge. To resolve this, researchers suggested use of either side chains and cloud storage as off-chain solution. BC also helps in maintaining privacy among the users and provides a single platform where all previous and present data can be accessed. Some of the authors suggested using private BC to exercise tight control access and maintain features like privacy and security and confidentiality of the information. Use of both private and public BCs have been suggested by various researchers. **Many works suggest use of cloud storage or IPFS to store a large amount of data since the storage capacity is limited and BC add data in append-mode only. For storing data on the cloud or other chain, a hash of the data is stored on the main chain.**

2) *Future Work:* A lot of data is generated on daily basis in healthcare systems like patients' personal records, medical history, and medical reports like MRI, CT Scan, Ultrasounds, and many more. As BC supports immutability but according to EU regulations, patients will have the right to get their data erased whenever they want.

- **Data storage:** In the healthcare system lots of data are generated like medical scanning/imaging, reports, and other such large-size data. Storing such a big amount of data is a challenge as BC supports only a limited amount of data to be stored on-chain as bigger data leads to latency and less throughput [87].
- **Security and privacy:** Healthcare data contain sensitive and personal information about the patient which must remain secure. The intruder can attack and can steal a patient's details or else can make it difficult to share details between hospitals which can lead to the wrong diagnosis and come to know everything about your medical history. Achieving privacy and the ability to access sensitive information are the major challenges.
- **Interoperability:** In the healthcare domain there is a huge number of interconnected devices and all these devices must communicate with each other. All the users (different stakeholders such as patients and health personnel) have multiple types of devices communicating with each other, which requires coordination between multiple users.
- **Standardization:** BC technology is in its beginning stage and whenever a new technology emerges, it requires some widely-applicable standards from Standard Development Organizations (SDOs) such as ISO [272]. [273] list out the basic standardization organizations and their efforts to standardize blockchain. [274] calls attention to various standardization organizations and their publications about blockchain. **But still, there are no globally accepted standards and protocols for the applicability of blockchain.**

B. Smart Homes

1) *Lessons Learned:* A smart home is defined as a home where all the appliances installed in the house are connected through the Internet and can communicate and share data. This process involves significant amount of data generation. BC technology enables IoT devices to communicate and share data. The primary focus is to maintain security and privacy in IoT-enabled homes. Moreover, use of access control list

TABLE XIX: Summary of Technical Aspect - Processing Power

Reference	Technical Aspect	Proposed Solution
Atlam et al. [3]	The mining process requires very high computation power.	Discussed an approach to speed up the mining process by simultaneously using CPU & GPU in single machines (originally proposed by [269]).
Xie et al. [84]	PoW algorithm requires high computational power to mine the block.	Suggested using another consensus algorithm like PoS, DPoS.
Monrat et al. [63]	In the PoW consensus algorithm, the miner needs to solve a difficult puzzle to compute the hash, which requires high computational power and modern hardware resources. Energy consumption in comparison to other payment systems is too high.	Suggested solution either to redesign the BC infrastructure or use another consensus algorithm like PoS, which consumes less energy.
Golosova et al. [270]	Discussed the high energy consumption. To validate a transaction each node starts computing solutions for which they are using an enormous amount of computer power. Each node is repeating the same process which is a waste of resources.	No solution is proposed.

and Lamport Merkle Digital Signature algorithm has been suggested by researcher for authorization. The most preferred consensus algorithm is PoW by researchers. But PoW adds an extra cost which can be removed and can be mined by the homeowner. The secondary focus while leveraging BC for smart homes is energy management. For this consortium BC with PBFT consensus algorithm has been suggested. Some researchers have suggested tier architecture for efficient integration of BC and IoT-enabled smart homes. Use of smart contracts running on top of BC have been also found efficient for ensuring tight access control and authentication in smart homes. Moreover, proxy signature, Kalman filters, and private BCs have also been used by researchers for achieving authentication and monitoring of IoT devices in smart homes.

2) Future Work:

- **Access control attack:** If the intruder gets access to the device controlling the activities in a smart home then the intruder can do malicious activities [119]. It is important to design an access control system to permit the third person or guests in the house. This permission will be given based on access records generated by IoT devices and stored permanently using blockchain [119].
- **Inter-operability:** A smart home consists of different appliances and it is difficult to communicate with each other. It is important to work in the direction to achieve interoperability among the devices.
- **Privacy and security:** Although blockchain provides robust security and privacy, many other malicious attacks are possible. So, It is important to research more to improve privacy of user data.

C. Smart City

1) *Lessons Learned:* Smart cities can be defined as cities equipped with modern, smart, and connected amenities that make the lives of citizens easier. Due to rapid urbanization and the increase in population, cities are facing many challenges. Here BC can serve as a possible solution because of the features it offers like improved reliability, better fault tolerance capability, and faster and more efficient operations. The idea of combining BC with a smart city provides a platform for communication, supports data integrity, motivates organizations like schools, hospitals, and government entities to share data transparently, and saves individuals time. For maintaining privacy and security, SDN with BC is used with PoW consensus algorithms with private BC. Different frameworks include mainly four layers physical, database, communication, and interface layer. Numerous researchers suggested off-chain storage like IPFS, cloud storage, and private BC along with BC-enabled on-chain for data storage. This will help in the personal data sharing challenge. While some of the authors suggested using Hyperledger fabric to maintain authentication and authorization. For data integrity, digital signatures and hashing are preferred. For energy management in smart cities, hyperledger fabric is used to maintain confidentiality and Kafka algorithm for authentication.

2) Future Work:

- **Security and privacy:** As blockchain is a distributed ledger it does not guarantee the privacy of the user's data,

as all the data is shared among all the nodes present in the network. Another issue in BC is that each node has blockchain generated address and its real identity is not revealed.

- **Throughput:** Throughput of the blockchain depends upon the number of transactions inside a block which is restricted by block size. The number of transaction rates must be improved for faster services.
- **Storage:** Applying blockchain technology in smart cities will generate a huge amount of data which leads to data storage issues. To manage such large amount of data is another primary focus.
- **Energy efficiency:** For any transaction to occur, nodes present in the network need to create consensus among themselves for which they need to solve hard computations which consume a large amount of electricity. So, the proposed system must be energy efficient.

D. Supply Chain Management

1) *Lessons Learned:* The major application of BC in supply chain management is to trace and keep the track of the products. Also, BC helps in secure sharing information among all the entities involved in the supply chain. Tracing and sharing information about the product not only prevents counterfeiting of products but also provides transparent information about the product. Ethereum BC with PoC, BigChainDB, off-chain storage, and double chains are some of the solutions proposed by researchers. For monitoring or real-time tracking Ethereum and Hyperledger sawtooth with IoT and RFID have been used to ensure unique identification of items. While some other researchers discussed hyperledger fabric BC as it has better performance. For credit evaluation, BC with deep learning has been used. Smart contracts are also used for payments and smooth transactions.

2) *Future Work:* Here are some challenges that need to be resolved while integrating BC with supply chain management.

- **Adoption of technology:** The major hurdle in adopting Blockchain technology is making people aware of the adaptability of blockchain technology due to lack of knowledge and lack of skills to use the technology [67].
- **Throughput performance:** As blockchain is decentralized in nature, each transaction needs approval from all the other nodes present in the network, which brings consensus among the nodes. This validation process and size of the block limits the throughput of the blockchain [147].
- **Security:** In the supply chain the privacy of the manufacturer and supplier is the most important issue. Any one of the participating entities in the blockchain network can be a competitor and can misuse the information flowing in the supply chain [67].
- **Inter-operability:** A supply chain consists of different nodes, all of which need to communicate and share information between different nodes [67].

E. Autonomous Vehicle

1) *Lessons Learned:* Autonomous vehicles connected, smart, and driverless vehicle that can communicate or ex-

change data with other vehicles or infrastructure. Use of autonomous vehicles help in reducing accidents, reducing traffic congestion, increasing lane capacity, and efficient parking. However, security, privacy, trustless sharing, provenance are some of the required features which can be achieved with the use of BC in IoT-enabled autonomous vehicles. Some of the important use of BC for autonomous vehicles are energy trading between electric vehicles and charging stations, information sharing, vehicle-to-vehicle communication, and road-related messages such as road conditions and traffic congestion [84]. Use of Hyperledger Fabric, off-chain storage, and the Diffie hellman key exchange algorithm have been proposed for payments in AV. To ensure scalability, off-chain storage and separate chains have been proposed. Data is stored on independent sources and their indexes are stored on the main chain.

2) *Future Work*: Integrating BC with autonomous vehicles brings many challenges along with it like motivating vehicles to share road-related messages also it is important to design a trust management system.

- **Scalability**: In autonomous vehicles, lots of data are generated in the case of connecting vehicles the data is to be shared as road information, traffic jam, traffic lights, etc. All this requires memory to store. Data growing rate is 40% as compared to IT which is 5% [275].

F. Smart Grid

1) *Lessons Learned*: Smart grid are build to offer optimized and uninterrupted power supplies to user, however, it faces issues like non-trusted data collection, privacy leakage, centralized generation and distribution, insecure power system, and energy thefts. BC supports features like immutability, non-repudiation, and decentralization, which makes it the intriguing solution for achieving security, privacy, and trust in smart grid systems. For storing meter readings and electricity consumption, BC can be used. Also in the future, IoT-enabled device-to-device electricity trading and payments can be done through BC [84]. BC-enabled P2P energy trading platform allows decentralized selling of excess energy by one consumer to other consumer who are in need. While SHA-256/512 are the most preferred hashing algorithms, researcher have used RSA with zero knowledge proof and an elliptic curve algorithm to enhance access control and authorization. Another important focus is charging coordination among the users for which BC and smart contract enabled smart grid have been advocated.

2) *Future Work*: According to a bitcoin energy consumption report, for carrying out thirty million transactions thirty billion kWh of electricity was consumed [87]. If we integrate BC with a smart grid, it will require a lot of energy as the number of transactions is a direct multiple of 1000.

- **Scalability**: In the energy sector, the number of transactions is very high and energy consumption for such BC-based transactions will be very high. Thus, scalability is a challenge.
- **Centralization**: The chances of centralization are because all the miners form a mining pool to solve the

PoW consensus algorithm and which can further lead to a 51% attack.

- **Implementation Cost**: Integrating blockchain with smart grids requires high infrastructure cost because of restructuring the current grid network. So, implementing BC in existing smart grid is a challenge.

G. Unmanned Aerial Vehicle

1) *Lessons Learned*: Unmanned Aerial Vehicles (UAVs), also known as drones or Flying Robots [224], are self-regulating devices accessed through remotes or sometimes self-controlled and do not require a human pilot. BC has huge potential for encouraging the benefits of UAV-based applications. By implementing BC technology, governments across different geographical locations can keep an eye on the UAVs flying in their domains. With the expanding prominence of UAVs, their utilization in metropolitan territories has additionally expanded. BC enables UAVs to be outfitted with features like immutability, distribution, and decentralization which makes UAVs a prominent approach for applications that carry critical information such as defense, healthcare, surveillance, and financial applications. For communication among the UAV's, Ethereum BC with IPFS storage is mostly used by different researchers. Although the use of BC for UAVs results in increase in overall processing time but it results in reduction in attack rates. For data collection, PoA consensus is used with Geth Ethereum BC. A few of the researchers, for health monitoring using UAV, also used the PoA consensus algorithm in data collection. Whereas few other researchers have also preferred the Kafka consensus algorithm with hyperledger fabric and smart contracts.

2) *Future Work*: Integrating BC with UAV is a complex task as it requires thorough testing before it is launched in the market. Also, UAVs have limited battery capacity with fly-time concerns whereas BC consumes more power. Thus, if we integrate BC with UAVs then power consumption is one of the major concerns to be resolved [226]

- **Privacy**: UAVs have cameras, temperature sensors, and GPS to collect data which can cause unintentional invasion of privacy [224].
- **Scalability**: In small groups of UAVs, communication is easily possible but in large groups, communication is not efficient. The number of transactions in Bitcoin and Ethereum is 12 transactions per second [224] which are quite less as compared to traditional approaches.
- **Lack of Standards and Regulations**: Many organizations are currently working to release the BC standards so that the integration of BC with existing technologies will be possible. But the proper guidelines, rules, and regulations are yet to be released [224].
- **Resource limitations**: UAVs are lightweight flying machines but BC requires high computational power to run consensus algorithm [224].

VI. CONCLUSION

BC is represented as a highly scalable technology that can be applied in many areas. Also, the IoT network is growing

tremendously which leads to many challenges that need to be resolved soon. Here blockchain comes as a most promising solution because of its key attributes such as decentralization, immutability, distribution, transparency, non-repudiation, and pseudonymity. The future of integrating BC and IoT is undeniably bright. In this paper, we briefly introduce blockchain, related terminology, its types, and the technology behind blockchain i.e., DLT along with a quick overview of IoT. Further, this paper has surveyed the available literature on BC for IoT to provide an in-depth understanding of the integration of BC and IoT, related technical aspects, and their challenges. In particular, we focus attention on the opportunities and challenges that exist with the use of blockchain for IoT use cases. The key attributes of BC can support the implementation of various use cases such as healthcare, supply chain, and logistic management, smart city, smart grid, and autonomous vehicles. Our survey covered an aggregate treatment of challenges in integrating BC for IoT including scalability, security, and power consumption. We also discussed the lessons we learned from our literature survey. Finally, a broad list of future directions and open challenges were presented to motivate future research on BC for IoT.

REFERENCES

- [1] A. Kalla, P. Prombage, and M. Liyanage, "Introduction to IoT," *IoT Security: Advances in Authentication*, pp. 1–25, 2020.
- [2] H. D. Kotha and V. M. Gupta, "IoT application: a survey," *International Journal of Engineering & Technology*, vol. 7, no. 2.7, pp. 891–896, 2018.
- [3] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and iot," in *Advances in computers*. Elsevier, 2019, vol. 115, pp. 1–39.
- [4] Cisco, "At-a Glance," 2016, accessed on 16.04.2021. [Online]. Available: <https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf?dtd=ossdc000283...>
- [5] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *2014 International conference on science engineering and management research (ICSEMR)*. IEEE, 2014, pp. 1–8.
- [6] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 414–454, 2013.
- [7] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.
- [8] J. Li and M. Kassem, "Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction," *Automation in construction*, vol. 132, p. 103955, 2021.
- [9] U. Zaman, F. Mehmood, N. Iqbal, J. Kim, and M. Ibrahim, "Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications," *Electronics*, vol. 11, no. 12, p. 1893, 2022.
- [10] R. S. Bhadoria, Y. Arora, and K. Gautam, "Blockchain hands on for developing genesis block," *Advanced applications of blockchain technology*, pp. 269–278, 2020.
- [11] T. M. Hewa, A. Kalla, A. Nag, M. E. Ylianttila, and M. Liyanage, "Blockchain for 5g and iot: Opportunities and challenges," in *2020 IEEE Eighth International Conference on Communications and Networking (ComNet)*. IEEE, 2020, pp. 1–8.
- [12] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trust-worthy blockchain oracles: review, comparison, and open research challenges," *IEEE Access*, vol. 8, pp. 85 675–85 685, 2020.
- [13] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.
- [14] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, 2018.
- [15] A. Singh, A. Smirti, R. Gupta, C. de Alwis, and A. Kalla, "Introduction to blockchain and smart contract—principles, applications, and security," in *Blockchain Technology in Healthcare Applications*. CRC Press, 2022, pp. 175–197.
- [16] T. Alam, "Blockchain and its Role in the Internet of Things (IoT)," *arXiv preprint arXiv:1902.09779*, 2019.
- [17] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications*, vol. 79, no. 15-16, pp. 9711–9733, 2020.
- [18] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8599–8622, 2022.
- [19] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the internet of things," in *Proceedings of the 23rd ACM on symposium on access control models and technologies*, 2018, pp. 77–83.
- [20] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*. Springer, 2010, pp. 389–395.
- [21] H. Wang, Y. Wang, T. Taleb, and X. Jiang, "Special issue on security and privacy in network computing," *World Wide Web*, vol. 23, pp. 951–957, 2020.
- [22] S. G. H. Soumyalatha, "Study of IoT: understanding IoT architecture, applications, issues and challenges," in *1st International Conference on Innovations in Computing & Net-working (ICICN16)*, CSE, RRCE. *International Journal of Advanced Networking & Applications*, no. 478, 2016.
- [23] G. S. Ramachandran and B. Krishnamachari, "Blockchain for the iot: Opportunities and challenges," *arXiv preprint arXiv:1805.02818*, 2018.
- [24] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT Challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.
- [25] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the internet of things (IoT): A security taxonomy for IoT," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 163–168.
- [26] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, "Continuous security in IoT using blockchain," in *2018 IEEE international conference on acoustics, speech and signal processing (ICASSP)*. IEEE, 2018, pp. 6423–6427.
- [27] T. Choudhary, C. Virmani, and D. Juneja, "Convergence of Blockchain and IoT: An Edge Over Technologies," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*. Springer, 2020, pp. 299–316.
- [28] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.
- [29] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017, pp. 557–564.
- [30] A. Priyanka and A. Nagaratnam, "Blockchain Evolution-A Survey Paper," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 4, no. 8, 2018.
- [31] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.
- [32] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.
- [33] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for managing heterogeneous internet of things: A perspective architecture," *IEEE Network*, vol. 34, no. 1, pp. 16–23, 2020.
- [34] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Computer Communications*, vol. 136, pp. 10–29, 2019.
- [35] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI," *Big Data and Cognitive Computing*, vol. 4, no. 4, p. 28, 2020.
- [36] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT)*. IEEE, 2017, pp. 464–467.

- [37] F. Chen, Z. Xiao, L. Cui, Q. Lin, J. Li, and S. Yu, "Blockchain for Internet of things applications: A review and open issues," *Journal of Network and Computer Applications*, vol. 172, p. 102839, 2020.
- [38] F. Restuccia, S. D. Kanhere, T. Melodia, and S. K. Das, "Blockchain for the Internet of Things: Present and Future," *arXiv preprint arXiv:1903.07448*, 2019.
- [39] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *2018 International Conference on Information Networking (ICOIN)*. IEEE, 2018, pp. 473–475.
- [40] Q. H. Mahmoud, M. Lescisin, and M. AlTaei, "Research challenges and opportunities in blockchain and cryptocurrencies," *Internet Technology Letters*, vol. 2, no. 2, p. e93, 2019.
- [41] N. J. Van Eck and L. Waltman, "Vosviewer manual," *Manual for VOSviewer version*, vol. 1, no. 0, 2011.
- [42] T. Choudhary, C. Virmani, and D. Juneja, "Convergence of Blockchain and IoT: An Edge Over Technologies," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*. Springer, 2020, pp. 299–316.
- [43] M. Salimiti, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained IoT networks," *Internet of Things*, vol. 11, p. 100212, 2020.
- [44] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.
- [45] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions," *Wireless Networks*, pp. 1–36, 2020.
- [46] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions," *Blockchain: Research and Applications*, p. 100006, 2021.
- [47] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: a survey," *IEEE Internet of Things Journal*, 2021.
- [48] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain," *Cluster Computing*, vol. 24, no. 1, pp. 37–55, 2021.
- [49] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks," *Computers in Industry*, vol. 144, p. 103801, 2023.
- [50] J. Li, D. Greenwood, and M. Kassem, "Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases," *Automation in Construction*, vol. 102, pp. 288–307, 2019.
- [51] H. F. Atlam and G. B. Wills, "Intersections between IoT and distributed ledger," in *Advances in Computers*. Elsevier, 2019, vol. 115, pp. 73–113.
- [52] U. S. Aditya, R. Singh, P. K. Singh, and A. Kalla, "A Survey on Blockchain in Robotics: Issues, Opportunities, Challenges and Future Directions," *Journal of Network and Computer Applications*, vol. 196, p. 103245, 2021.
- [53] A. Sultan, M. S. A. Malik, and A. Mushtaq, "Internet of Things Security Issues and their Solutions with Blockchain Technology Characteristics: A Systematic Literature Review," *Am J Compt Sci Inform Technol*, vol. 6, no. 3, p. 27, 2018.
- [54] D. B. Rawat, V. Chaudhary, and R. Doku, "Blockchain: Emerging Applications and Use Cases," *arXiv preprint arXiv:1904.12247*, 2019.
- [55] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, "Blockchain for smart cities: A review of architectures, integration trends and future research directions," *Sustainable Cities and Society*, vol. 61, p. 102360, 2020.
- [56] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019.
- [57] I. Ahmed and M. A. Shilpi, "Blockchain Technology A Literature Survey," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 10, pp. 2395–0056, 2018.
- [58] M. Niranjanamurthy, B. Nithya, and S. Jagannatha, "Analysis of Blockchain technology: pros, cons and SWOT," *Cluster Computing*, vol. 22, no. 6, pp. 14743–14757, 2019.
- [59] P. Szalachowski, "(Short Paper) Towards More Reliable Bitcoin Timestamps," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 101–104.
- [60] G.-T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," *Journal of Information processing systems*, vol. 14, no. 1, 2018.
- [61] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.
- [62] S. T. Aras and V. Kulkarni, "Blockchain and its applications—a detailed survey," *International Journal of Computer Applications*, vol. 180, no. 3, pp. 29–35, 2017.
- [63] 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. 117 134–117 151, 2019.
- [64] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.
- [65] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.
- [66] M. Alharby and A. Van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," *arXiv preprint arXiv:1710.06372*, 2017.
- [67] Y. Chang, E. Iakovou, and W. Shi, "Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities," *International Journal of Production Research*, vol. 58, no. 7, pp. 2082–2099, 2020.
- [68] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, and Y. Liu, "Transaction-based classification and detection approach for ethereum smart contract," *Information Processing & Management*, vol. 58, no. 2, p. 102462, 2021.
- [69] T. Hewa, M. Yliantila, and M. Liyanage, "Survey on blockchain based smart contracts: applications, opportunities and challenges," *Journal of Network and Computer Applications*, p. 102857, 2020.
- [70] M. Di Angelo and G. Salzer, "Characterizing types of smart contracts in the ethereum landscape," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 389–404.
- [71] Alyssa Hertig, "Ethereum 101," accessed on 10.01.2021. [Online]. Available: <https://www.coindesk.com/learn/ethereum-101/ethereum-smart-contracts-work>
- [72] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 2018, pp. 2–8.
- [73] I. Marco and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.
- [74] A. Kalla, C. De Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6g: Technical aspects, use cases, challenges and research directions," *Journal of Industrial Information Integration*, p. 100404, 2022.
- [75] Y. Lu, "The blockchain: State-of-the-art and research challenges," *Journal of Industrial Information Integration*, vol. 15, pp. 80–90, 2019.
- [76] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
- [77] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.
- [78] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digital Communications and Networks*, 2020.
- [79] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, pp. 1–15, 2020.
- [80] A. Siyal, A. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," *Cryptography*, vol. 3, no. 1, p. 3, 2019.
- [81] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS-A blockchain based approach for smart healthcare system," in *Healthcare*, vol. 8, no. 1. Elsevier, 2020, p. 100391.
- [82] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942–950, 2018.
- [83] E. J. De Aguiar, B. S. Façal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–27, 2020.
- [84] 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 Communications Surveys & Tutorials*, 2019.

- [85] M. N. Sadiku, K. G. Eze, and S. M. Musa, "Block chain Technology in Healthcare," *International Journal of Advances in Scientific Research and Engineering*, vol. 4, 2018.
- [86] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," *IEEE Systems Journal*, 2020.
- [87] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.
- [88] M. A. Cyran, "Blockchain as a foundation for sharing healthcare data," *Blockchain in Healthcare Today*, 2018.
- [89] 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," *Journal of medical systems*, vol. 42, no. 7, p. 130, 2018.
- [90] G. Carter, H. Shahriar, and S. Sneha, "Blockchain-Based Interoperable Electronic Health Record Sharing Framework," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2. IEEE, 2019, pp. 452–457.
- [91] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of medical systems*, vol. 43, no. 1, p. 5, 2019.
- [92] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, and J. J. Rodrigues, "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.
- [93] P. Hemalatha *et al.*, "Monitoring and securing the healthcare data harnessing iot and blockchain technology," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2554–2561, 2021.
- [94] J. A. Alzubi, "Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare," *Computer Communications*, vol. 170, pp. 200–208, 2021.
- [95] M. Chen, T. Malook, A. U. Rehman, Y. Muhammad, M. D. Alshehri, A. Akbar, M. Bilal, and M. A. Khan, "Blockchain-enabled healthcare system for detection of diabetes," *Journal of Information Security and Applications*, vol. 58, p. 102771, 2021.
- [96] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021.
- [97] S. Pandya, G. Srivastava, R. Jhaveri, M. R. Babu, S. Bhattacharya, P. K. R. Maddikunta, S. Mastorakis, M. J. Piran, and T. R. Gadekallu, "Federated learning for smart cities: A comprehensive survey," *Sustainable Energy Technologies and Assessments*, vol. 55, p. 102987, 2023.
- [98] A. Belhadi, J.-O. Holland, A. Yazidi, G. Srivastava, J. C.-W. Lin, and Y. Djenouri, "BloMT-iSeg: Blockchain internet of medical things for intelligent segmentation," *Frontiers in Physiology*, vol. 13, p. 2744, 2023.
- [99] R. Ch, G. Srivastava, Y. L. V. Nagasree, A. Ponugumati, and S. Ramachandran, "Robust Cyber-Physical System Enabled Smart Healthcare Unit Using Blockchain Technology," *Electronics*, vol. 11, no. 19, p. 3070, 2022.
- [100] Y. Sharma and B. Balamurugan, "Preserving the privacy of electronic health records using blockchain," *Procedia Computer Science*, vol. 173, pp. 171–180, 2020.
- [101] A. H. Mayer, C. A. da Costa, and R. d. R. Righi, "Electronic health records in a Blockchain: A systematic review," *Health informatics journal*, vol. 26, no. 2, pp. 1273–1288, 2020.
- [102] M. Sahoo, S. S. Singhar, and S. S. Sahoo, "A blockchain based model to eliminate drug counterfeiting," in *Machine Learning and Information Processing: Proceedings of ICMLIP 2019*. Springer, 2020, pp. 213–222.
- [103] A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, p. e4333, 2021.
- [104] M. M. H. Onik, S. Aich, J. Yang, C.-S. Kim, and H.-C. Kim, "Blockchain in healthcare: challenges and solutions," in *Big Data Analytics for Intelligent Healthcare Management*. Elsevier, 2019, pp. 197–226.
- [105] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.
- [106] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.
- [107] Y. N. Aung and T. Tantidham, "Review of Ethereum: Smart home case study," in *2017 2nd International Conference on Information Technology (INCIT)*. IEEE, 2017, pp. 1–4.
- [108] Y. Zhou, M. Han, L. Liu, Y. Wang, Y. Liang, and L. Tian, "Improving iot services in smart-home using blockchain smart contract," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 81–87.
- [109] T. L. N. Dang and M. S. Nguyen, "An approach to data privacy in smart home using blockchain technology," in *2018 International Conference on Advanced Computing and Applications (ACOMP)*. IEEE, 2018, pp. 58–64.
- [110] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, p. 1550147719844159, 2019.
- [111] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating smart home security: Is blockchain the answer?" *IEEE Access*, vol. 8, pp. 117 802–117 816, 2020.
- [112] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, J. Wang, Z. Almakhdme, and A. Tolba, "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Generation Computer Systems*, vol. 115, pp. 304–313, 2021.
- [113] Q. Yang and H. Wang, "Privacy-Preserving Transactive Energy Management for IoT-aided Smart Homes via Blockchain," *arXiv preprint arXiv:2101.03840*, 2021.
- [114] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Information Processing & Management*, vol. 58, no. 3, p. 102482, 2021.
- [115] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," *IEEE Access*, vol. 9, pp. 103 651–103 669, 2021.
- [116] M. J. Baucas, S. A. Gadsden, and P. Spachos, "IoT-based smart home device monitor using private blockchain technology and localization," *IEEE Networking Letters*, vol. 3, no. 2, pp. 52–55, 2021.
- [117] K. Liao, "Design of the Secure Smart Home System Based on the Blockchain and Cloud Service," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.
- [118] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, p. 106382, 2020.
- [119] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Computers & Electrical Engineering*, vol. 83, p. 106585, 2020.
- [120] C. Lazaroui and M. Roscia, "Smart district through iot and blockchain," in *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)*. IEEE, 2017, pp. 454–461.
- [121] M. AbuNaser and A. A. Alkhatib, "Advanced survey of blockchain for the Internet of Things smart home," in *2019 IEEE Jordan international joint conference on electrical engineering and information technology (JEEIT)*. IEEE, 2019, pp. 58–62.
- [122] 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 Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.
- [123] J. M. Batalla, A. Vasilakos, and M. Gajewski, "Secure smart homes: Opportunities and challenges," *ACM Computing Surveys (CSUR)*, vol. 50, no. 5, pp. 1–32, 2017.
- [124] S. Baru, "Blockchain: The next innovation to make our cities smarter," *en. In: (Jan. 2018)*, p. 48, 2018.
- [125] H. Treiblmaier, A. Rejeb, and A. Strebing, "Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda," *Smart Cities*, vol. 3, no. 3, pp. 853–872, 2020.
- [126] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.
- [127] C. Năulea and S.-M. Mic, "Using blockchain as a platform for smart cities," *Journal of E-Technology*, vol. 9, no. 2, p. 37, 2018.
- [128] S. Theodorou and N. Sklavos, "Blockchain-Based Security and Privacy in Smart Cities," in *Smart Cities Cybersecurity and Privacy*. Elsevier, 2019, pp. 21–37.

- [129] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *Computers in Industry*, vol. 109, pp. 83–99, 2019.
- [130] R. A. Mishra, A. Kalla, A. Braeken, and M. Liyanage, "Privacy protected blockchain based architecture and implementation for sharing of students' credentials," *Information Processing & Management*, vol. 58, no. 3, p. 102512, 2021.
- [131] C. Shen and F. Pena-Mora, "Blockchain for cities: a systematic literature review," *Ieee Access*, vol. 6, pp. 76787–76819, 2018.
- [132] C. Näsulea and S.-M. Mic, "Using Blockchain as a Platform for Smart Cities," *Journal of E-Technology Volume*, vol. 9, no. 2, p. 37, 2018.
- [133] K. Biswas and V. Muthukumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE, 2016, pp. 1392–1393.
- [134] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.
- [135] W. Zhang, Z. Wu, G. Han, Y. Feng, and L. Shu, "Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications," *Future Generation Computer Systems*, vol. 108, pp. 574–582, 2020.
- [136] 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," *Journal of Systems Architecture*, vol. 115, p. 101954, 2021.
- [137] P. W. Khan, Y.-C. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, p. 484, 2020.
- [138] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *Journal of Information Security and Applications*, vol. 57, p. 102686, 2021.
- [139] H. A. Khattak, K. Tehreem, A. Almogren, Z. Ameer, I. U. Din, and M. Adnan, "Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities," *Journal of Information Security and Applications*, vol. 55, p. 102615, 2020.
- [140] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021.
- [141] C. M. S. Ferreira, C. T. B. Garrocho, R. A. R. Oliveira, J. S. Silva, and C. F. M. d. C. Cavalcanti, "IoT registration and authentication in smart city applications with blockchain," *Sensors*, vol. 21, no. 4, p. 1323, 2021.
- [142] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardaš, "Blockchain Technology Implementation in Logistics," *Sustainability*, vol. 11, no. 4, p. 1185, 2019.
- [143] Y. Chang, E. Iakovou, and W. Shi, "Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities," *International Journal of Production Research*, pp. 1–18, 2019.
- [144] S. Aich, S. Chakraborty, M. Sain, H.-i. Lee, and H.-C. Kim, "A review on benefits of iot integrated blockchain based supply chain management implementations across different sectors with case study," in *2019 21st international conference on advanced communication technology (ICACT)*. IEEE, 2019, pp. 138–141.
- [145] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.
- [146] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.
- [147] J. Zhang, "Deploying blockchain technology in the supply chain," in *Blockchain and Distributed Ledger Technology (DLT)*. IntechOpen, 2019.
- [148] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldó, "The rise of blockchain technology in agriculture and food supply chains," *Trends in Food Science & Technology*, vol. 91, pp. 640–652, 2019.
- [149] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, p. 102067, 2020.
- [150] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE access*, vol. 9, pp. 9728–9743, 2021.
- [151] X. Liu, A. V. Barenji, Z. Li, B. Montreuil, and G. Q. Huang, "Blockchain-based smart tracking and tracing platform for drug supply chain," *Computers & Industrial Engineering*, vol. 161, p. 107669, 2021.
- [152] J. Rupasena, T. Hewa, K. T. Hemachandra, and M. Liyanage, "Scalable Storage Scheme for Blockchain-Enabled IoT Equipped Food Supply Chains,"
- [153] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," in *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IoT Tuscany)*. IEEE, 2018, pp. 1–4.
- [154] D. Mao, F. Wang, Z. Hao, and H. Li, "Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain," *International journal of environmental research and public health*, vol. 15, no. 8, p. 1627, 2018.
- [155] W. Viriyasitavat, D. Hoonsopon, and Z. Bi, "Augmenting cryptocurrency in smart supply chain," *Journal of Industrial Information Integration*, vol. 21, p. 100188, 2021.
- [156] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in *International Conference on Business Process Management*. Springer, 2016, pp. 329–347.
- [157] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuysse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Generation Computer Systems*, vol. 86, pp. 641–649, 2018.
- [158] P. Helo and A. Shamsuzzoha, "Real-time supply chain—A blockchain architecture for project deliveries," *Robotics and Computer-Integrated Manufacturing*, vol. 63, p. 101909, 2020.
- [159] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *2016 13th international conference on service systems and service management (ICSSSM)*. IEEE, 2016, pp. 1–6.
- [160] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in *2017 International conference on service systems and service management*. IEEE, 2017, pp. 1–6.
- [161] N. Rožman, M. Corn, T. Požrl, J. Diaci *et al.*, "Distributed logistics platform based on Blockchain and IoT," *Procedia CIRP*, vol. 81, pp. 826–831, 2019.
- [162] M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 58–62, 2020.
- [163] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Computers & industrial engineering*, vol. 154, p. 107130, 2021.
- [164] M. Lou, X. Dong, Z. Cao, and J. Shen, "SESCF: A Secure and Efficient Supply Chain Framework via Blockchain-Based Smart Contracts," *Security and Communication Networks*, vol. 2021, 2021.
- [165] Q. Song, Y. Chen, Y. Zhong, K. Lan, S. Fong, and R. Tang, "A supply-chain system framework based on internet of things using blockchain technology," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 1, pp. 1–24, 2021.
- [166] S. M. H. Bamakan, N. Faregh, and A. ZareRavasan, "Di-ANFIS: an integrated blockchain-IoT-big data-enabled framework for evaluating service supply chain performance," *Journal of Computational Design and Engineering*, vol. 8, no. 2, pp. 676–690, 2021.
- [167] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the internet of things supply chain management," *Sensors*, vol. 21, no. 5, p. 1759, 2021.
- [168] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50–57, 2018.
- [169] Dave Maunsell, Praveen Tanguturi, James Hogarth, "Realising the benefits of autonomous vehicles in Australia," accessed on 27.01.2021. [Online]. Available: https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/en-gb/PDF_3/Accenture-Realising-Benefits-Autonomous-Vehicles-Australia.pdf
- [170] P. G. Saranti, D. Chondrogianni, and S. Karatzas, "Autonomous vehicles and blockchain technology are shaping the future of transportation," in *The 4th conference on sustainable urban mobility*. Springer, 2018, pp. 797–803.

- [171] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th international conference on intelligent transportation systems (ITSC)*. IEEE, 2016, pp. 2663–2668.
- [172] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.
- [173] J. C. Ferreira, C. Ferreira da Silva, and J. P. Martins, "Roaming service for electric vehicle charging using blockchain-based digital identity," *Energies*, vol. 14, no. 6, p. 1686, 2021.
- [174] R. Roriz and J. L. Pereira, "Avoiding insurance fraud: a blockchain-based solution for the vehicle sector," *Procedia Computer Science*, vol. 164, pp. 211–218, 2019.
- [175] A. Kumar, A. Prasad, and R. Murthy, "Application of blockchain in usage based insurance," *International Journal of Advance Research, Ideas and Innovations in Technology, IJARIT*, vol. 5, no. 2, pp. 1574–1577, 2019.
- [176] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," *arXiv preprint arXiv:1707.07442*, 2017.
- [177] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," *arXiv preprint arXiv:1802.05050*, 2018.
- [178] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Computer Networks*, vol. 145, pp. 219–231, 2018.
- [179] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, 2019.
- [180] Y. Yin, Y. Li, B. Ye, T. Liang, and Y. Li, "A blockchain-based incremental update supported data storage system for intelligent vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4880–4893, 2021.
- [181] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "Petroblock: A blockchain-based payment mechanism for fueling smart vehicles," *Applied Sciences*, vol. 11, no. 7, p. 3055, 2021.
- [182] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," *Information Processing & Management*, vol. 58, no. 1, p. 102426, 2021.
- [183] A. K. Tyagi, D. Agarwal, and N. Sreenath, "SecVT: Securing the Vehicles of Tomorrow using Blockchain Technology," in *2022 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2022, pp. 1–6.
- [184] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.
- [185] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2020.
- [186] D. L. Dinesha and P. Balachandra, "Conceptualization of blockchain enabled interconnected smart microgrids," *Renewable and Sustainable Energy Reviews*, vol. 168, p. 112848, 2022.
- [187] A. R. Rao and D. Clarke, "Perspectives on emerging directions in using IoT devices in blockchain applications," *Internet of Things*, vol. 10, p. 100079, 2020.
- [188] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.
- [189] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.
- [190] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *2017 Resilience Week (RWS)*. IEEE, 2017, pp. 18–23.
- [191] "Powerledger," accessed on 25.02.2023. [Online]. Available: <https://www.powerledger.io/>
- [192] "Bankymoon," accessed on 25.02.2023. [Online]. Available: <http://bankymoon.co.za/>
- [193] M. Kuzlu, S. Sarp, M. Pipattanasomporn, and U. Cali, "Realizing the potential of blockchain technology in smart grid applications," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2020, pp. 1–5.
- [194] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 207–214, 2018.
- [195] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.
- [196] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *2019 IEEE wireless communications and networking conference (WCNC)*. IEEE, 2019, pp. 1–7.
- [197] I. Sestrem Ochôa, L. Augusto Silva, G. de Mello, N. M. Garcia, J. F. de Paz Santana, and V. R. Quietinho Leithardt, "A cost analysis of implementing a blockchain architecture in a smart grid scenario using sidechains," *Sensors*, vol. 20, no. 3, p. 843, 2020.
- [198] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, 2021.
- [199] O. Naseer, S. Ullah, and L. Anjum, "Blockchain-Based Decentralized Lightweight Control Access Scheme for Smart Grids," *Arabian Journal for Science and Engineering*, pp. 1–11, 2021.
- [200] D. Wang, H. Wang, and Y. Fu, "Blockchain-based IoT device identification and management in 5G smart grid," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–19, 2021.
- [201] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 34–45, 2021.
- [202] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2681–2693, 2021.
- [203] A. Muzumdar, C. Modi, and C. Vyjayanthi, "Designing a blockchain-enabled privacy-preserving energy theft detection system for smart grid neighborhood area network," *Electric Power Systems Research*, vol. 207, p. 107884, 2022.
- [204] H. Wang, Y. Gong, Y. Ding, S. Tang, and Y. Wang, "Privacy-Preserving Data Aggregation with Dynamic Billing in Fog-Based Smart Grid," *Applied Sciences*, vol. 13, no. 2, p. 748, 2023.
- [205] C. Yapa, C. de Alwis, M. Liyanage, and J. Ekanayake, "Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research," *Energy Reports*, vol. 7, pp. 6530–6564, 2021.
- [206] Y. T. Akililu and J. Ding, "Survey on blockchain for smart grid management, control, and operation," *Energies*, vol. 15, no. 1, p. 193, 2022.
- [207] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *2017 21st Conference of Open Innovations Association (FRUCT)*. IEEE, 2017, pp. 321–329.
- [208] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2018.
- [209] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680–3689, 2019.
- [210] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.
- [211] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A secure communicating things network framework for industrial IoT using blockchain technology," *Ad Hoc Networks*, vol. 94, p. 101933, 2019.
- [212] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porrambage, I. Ahmad, M. Liyanage, A. Braeken, and M. Ylianttila, "BlockEdge: blockchain-edge framework for industrial IoT networks," *IEEE Access*, vol. 8, pp. 154 166–154 185, 2020.
- [213] X. Liu, W. Wang, H. Guo, A. V. Barenji, Z. Li, and G. Q. Huang, "Industrial blockchain based framework for product lifecycle management in industry 4.0," *Robotics and computer-integrated manufacturing*, vol. 63, p. 101897, 2020.
- [214] G. Rathee, M. Balasaraswathi, K. P. Chandran, S. D. Gupta, and C. Boopathi, "A secure IoT sensors communication in industry 4.0

- using blockchain technology,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 533–545, 2021.
- [215] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, “Blockchain assisted secure data sharing model for Internet of Things based smart industries,” *IEEE Transactions on Reliability*, 2021.
- [216] N. D. Sarier, “Efficient biometric-based identity management on the Blockchain for smart industrial applications,” *Pervasive and Mobile Computing*, vol. 71, p. 101322, 2021.
- [217] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, “A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things,” *Journal of Industrial Information Integration*, vol. 21, p. 100190, 2021.
- [218] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, “Blockchain for the IoT and industrial IoT: A review,” *Internet of Things*, p. 100081, 2019.
- [219] Ericsson, “Unlock the value of Industry 4.0,” accessed on 29.01.2021. [Online]. Available: https://www.ericsson.com/en/industry4-0?gclid=CjwKCAiAgc-ABhA7EiwAjev-j08E-tWodAFp1Q1Kb44_jyNBqfYgSnalBqX-2jDjHxXhYp0SfoHhOCi28QAvD_BwE&gclidsrc=aw.ds
- [220] J. Robert, S. Kubler, and S. Ghatpande, “Enhanced lightning network (off-chain)-based micropayment in iot ecosystems,” *Future Generation Computer Systems*, vol. 112, pp. 283–296, 2020.
- [221] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, “Blockchain technology for secure supply chain management: A comprehensive review,” *IEEE Access*, 2022.
- [222] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, “Blockchain for smart communities: Applications, challenges and opportunities,” *Journal of Network and Computer Applications*, vol. 144, pp. 13–48, 2019.
- [223] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, “A taxonomy of blockchain-enabled software for secure UAV network,” *Computer Communications*, vol. 161, pp. 304–323, 2020.
- [224] P. Mehta, R. Gupta, and S. Tanwar, “Blockchain envisioned UAV networks: Challenges, solutions, and comparisons,” *Computer Communications*, 2020.
- [225] B. Bera, D. Chattaraj, and A. K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment,” *Computer Communications*, vol. 153, pp. 229–249, 2020.
- [226] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, “Applications of blockchain in unmanned aerial vehicles: A review,” *Vehicular Communications*, p. 100249, 2020.
- [227] T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, “An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology,” in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2019, pp. 162–167.
- [228] E. H. Abualsaud, “A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network,” *Computers & Electrical Engineering*, vol. 99, p. 107847, 2022.
- [229] A. Islam and S. Y. Shin, “Bus: A blockchain-enabled data acquisition scheme with the assistance of uav swarm in internet of things,” *IEEE Access*, vol. 7, pp. 103 231–103 249, 2019.
- [230] X. Xu, H. Zhao, H. Yao, and S. Wang, “A Blockchain-enabled Energy Efficient Data Collection System for UAV-assisted IoT,” *IEEE Internet of Things Journal*, 2020.
- [231] A. Islam and S. Y. Shin, “BHMUS: Blockchain Based Secure Outdoor Health Monitoring Scheme Using UAV in Smart City,” in *2019 7th International Conference on Information and Communication Technology (ICOICT)*. IEEE, 2019, pp. 1–6.
- [232] —, “A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things,” *Computers & Electrical Engineering*, vol. 84, p. 106627, 2020.
- [233] J. S. Raj, “Security enhanced blockchain based unmanned aerial vehicle health monitoring system,” *Journal of ISMAC*, vol. 3, no. 02, pp. 121–131, 2021.
- [234] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, “Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead,” *IEEE Network*, vol. 35, no. 1, pp. 20–29, 2021.
- [235] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, “Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator’s Perspective,” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2019.
- [236] N. Pathak, A. Mukherjee, and S. Misra, “AerialBlocks: Blockchain-Enabled UAV Virtualization for Industrial IoT,” *IEEE Internet of Things Magazine*, vol. 4, no. 1, pp. 72–77, 2021.
- [237] Y. Tan, J. Wang, J. Liu, and N. Kato, “Blockchain-Assisted Distributed and Lightweight Authentication Service for Industrial Unmanned Aerial Vehicles,” *IEEE Internet of Things Journal*, 2022.
- [238] W. Gao, W. G. Hatcher, and W. Yu, “A survey of blockchain: techniques, applications, and challenges,” in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2018, pp. 1–11.
- [239] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, “Focus on Blockchain: A Comprehensive Survey on Academic and Application,” *IEEE Access*, vol. 8, pp. 187 182–187 201, 2020.
- [240] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to scalability of blockchain: A survey,” *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020.
- [241] I. Kotilevets, I. Ivanova, I. Romanov, S. Magomedov, V. Nikonov, and S. Pavelev, “Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions,” *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 693–696, 2018.
- [242] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, “Survey: Sharding in blockchains,” *IEEE Access*, vol. 8, pp. 14 155–14 181, 2020.
- [243] A. Hafid, A. S. Hafid, and M. Samih, “Scaling blockchains: A comprehensive survey,” *IEEE Access*, vol. 8, pp. 125 244–125 262, 2020.
- [244] A. P. Joshi, M. Han, and Y. Wang, “A survey on security and privacy issues of blockchain technology,” *Mathematical foundations of computing*, vol. 1, no. 2, p. 121, 2018.
- [245] R. Zhang, R. Xue, and L. Liu, “Security and privacy on blockchain,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.
- [246] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, “Addressing security and privacy issues of IoT using blockchain technology,” *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 881–888, 2020.
- [247] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data security and privacy-preserving in edge computing paradigm: Survey and open issues,” *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.
- [248] A. Erdem, S. Ö. Yildirim, and P. Angin, “Blockchain for ensuring security, privacy, and trust in IoT environments: the state of the art,” *Security, Privacy and Trust in the IoT Environment*, pp. 97–122, 2019.
- [249] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.
- [250] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, “The role of blockchain to fight against COVID-19,” *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 85–96, 2020.
- [251] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 515–532.
- [252] S. Kim and G. C. Deka, *Advanced applications of blockchain technology*. Springer, 2020.
- [253] M. N. Islam and S. Kundu, “IoT security, privacy and trust in home-sharing economy via blockchain,” in *Blockchain Cybersecurity, Trust and Privacy*. Springer, 2020, pp. 33–50.
- [254] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, “Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems,” *Information Processing & Management*, vol. 57, no. 6, p. 102355, 2020.
- [255] A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, and B. Minaei-Bidgoli, “Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management,” *IEEE Access*, vol. 8, pp. 140 008–140 018, 2020.
- [256] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, “Medibchain: A blockchain based privacy preserving platform for healthcare data,” in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2017, pp. 534–543.
- [257] K. Azbeg, O. Ouchetto, S. J. Andaloussi, L. Fetjah, and A. Sekkaki, “Blockchain and IoT for security and privacy: A platform for diabetes self-management,” in *2018 4th international conference on cloud computing technologies and applications (Cloudtech)*. IEEE, 2018, pp. 1–5.
- [258] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for IoT,” *Sensors*, vol. 19, no. 2, p. 326, 2019.
- [259] S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, and A. Khanna, “An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy,” *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, 2020.

- [260] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533.
- [261] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustisek, "Towards decentralized IoT security enhancement: A blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266–273, 2018.
- [262] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.
- [263] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*, 2016, pp. 45–59.
- [264] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, "On-chain vs. off-chain storage for supply-and blockchain integration," *it-Information Technology*, vol. 60, no. 5-6, pp. 283–291, 2018.
- [265] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," URL: <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>, vol. 72, 2014.
- [266] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Software*, vol. 34, no. 6, pp. 21–27, 2017.
- [267] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2017, pp. 2567–2572.
- [268] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *2019 International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 2019, pp. 1–6.
- [269] J. A. Dev, "Bitcoin mining acceleration and performance quantification," in *2014 IEEE 27th Canadian conference on electrical and computer engineering (CCECE)*. IEEE, 2014, pp. 1–6.
- [270] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*. IEEE, 2018, pp. 1–6.
- [271] Digiconomist, "Bitcoin Energy Consumption Index," 2021, accessed on 24.05.2021. [Online]. Available: <https://digiconomist.net/bitcoin-energy-consumption>
- [272] H. El Bakoury, M. A. R. Chaudhry, W. Cerroni, H. He, and A. Barbir, "Standards for Major Internet Disruptors: Blockchain, Intents, and Related Paradigms," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 14–15, 2018.
- [273] V. Gramoli and M. Staples, "Blockchain standard: Can we reach consensus?" *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 16–21, 2018.
- [274] L. König, Y. Korobeinikova, S. Tjoa, and P. Kieseberg, "Comparing Blockchain Standards and Recommendations," *Future Internet*, vol. 12, no. 12, p. 222, 2020.
- [275] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, and J. Al-Jaroodi, "Applications of big data to smart cities," *Journal of Internet Services and Applications*, vol. 6, no. 1, pp. 1–15, 2015.



Shikha Mathur received her B.Tech. degree in 2013 and M.Tech. degree in 2016 in computer science and engineering (First class honors) from the Rajasthan Technical University, Kota. She is currently pursuing a Ph.D. degree from Manipal University Jaipur, Jaipur, India. She has authored over 10 publications. Shikha has over three years of experience with esteemed organizations of Rajasthan, in academics, project progress documentation, and graduate student co-supervision/mentoring, skills. Shikha's research interests are cryptography

and blockchain/DLT.



Anshuman Kalla (Senior Member IEEE) is working as Professor at the Department of Computer Engineering, CGPIT, Uka Tarsadia University (UTU), India. Dr. Kalla has more than twelve years of teaching and research experience. He has worked as a Postdoctoral Visiting Researcher at Center for Wireless Communications (CWC), University of Oulu, Finland. He graduated as an Engineer from Govt. Engineering College Bikaner in 2004. He did Master of Science in Telecommunications and Wireless Networking from ISEP, Paris, France in 2008 and another Master from University of Nice Sophia Antipolis, France in 2011. He obtained a Ph.D. degree in 2017. Dr. Kalla was recipient of Master's scholarships for pursuing both the Master programs. He has published papers in reputed international journals such as Elsevier (JII, IPM, JNCA, COMNET, ICT Express), IEEE Consumer Electronics Magazine, IEEE OJ-COMS, IEEE Computer, and IEEE EMR. His area of interests are Blockchain, 5G, 6G, IoT, Information Centric Networking, Software Defined Networking, Next Generation Networks. For more info: <https://sites.google.com/site/kallanshuman>



Gürkan Gür (Senior Member, IEEE) is a senior lecturer at Zurich University of Applied Sciences (ZHAW) – Institute of Applied Information Technology (InIT) in Winterthur, Switzerland. He received his B.S. degree in electrical engineering in 2001 and a Ph.D. degree in computer engineering in 2013 from Bogazici University in Istanbul, Turkey. His research interests include Future Internet, 5G, and Beyond networks, information security, and information-centric networking. He has two patents (one in the US, one in TR) and published more than 80 academic works. Currently, he is involved in EU H2020 RIA – INSPIRE-5Gplus project. He is a senior member of IEEE and a member of ACM.



Manoj Kumar Bohra (Senior Member, IEEE) is currently Professor at Manipal University Jaipur, India. Dr. Manoj received bachelor's Degree in Computer Science and Engg. (CSE) from MBM Engg. College, Jodhpur, India in 2003 and later the master's degree and PhD in CSE from MNIT Jaipur, India in 2011 and 2017 respectively. He is having 15+ years' experience in academia and research. His research work is in use of Machine Learning algorithms in Health Care IoT, Security, Blockchain Technology and Networks-on-Chip (NoC).



Madhusanka Liyanage (Senior Member, IEEE) received his B.Sc. degree (First Class Honours) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016.

From 2011 to 2012, he worked as a Research Scientist at the I3S Laboratory and Inria, Sophia Antipolis, France. He is currently an assistant professor/Ad Astra Fellow at the School of Computer Science, University College Dublin, Ireland. He is also acting as an adjunct Professor at the Center for Wireless Communications, University of Oulu, Finland. He was also a recipient of the prestigious Marie Skłodowska-Curie Actions Individual Fellowship during 2018-2020. During 2015-2018, he has been a Visiting Research Fellow at the CSIRO, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France and Computer Science and Engineering, The University of Oxford, U.K. He is also a senior member of IEEE. In 2020, he has received the "2020 IEEE ComSoc Outstanding Young Researcher" award by IEEE ComSoc EMEA. Dr. Liyanage's research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile, and virtual network security. More info: www.madhusanka.com