Journal Pre-proof

A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions

Md.Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, Venki Balasubramanian

PII: S2096-7209(21)00001-4

DOI: https://doi.org/10.1016/j.bcra.2021.100006

Reference: BCRA 100006

To appear in: *Blockchain: Research and Applications*

Received Date: 5 September 2020

Revised Date: 25 January 2021

Accepted Date: 30 January 2021

Please cite this article as: M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions, *Blockchain: Research and Applications*, https://doi.org/10.1016/j.bcra.2021.100006.

A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions

Md.Ashraf Uddin, Andrew Stranieri, Iqbal Gondal and Venki Balasubramanian

Internet Commerce Security Laboratory, Federation University Australia, Mount Helen, Ballarat, VIC 3350, Australia

ARTICLE INFO

Keywords:
Blockchain, consensus mechanism
BC cryptographic primitives
healthcare
smart home
Patient Centric Agent
Cloud of Things
Internet of Things
Fog of Things
SDN
Vehicular Network.

ABSTRACT

Conventional IoT ecosystems involve data streaming from sensors, through Fog devices to a centralized Cloud server. Issues that arise include privacy concerns due to third party management of Cloud servers, single points of failure, a bottleneck in data flows and difficulties in regularly updating firmware for millions of smart devices from a point of security and maintenance perspective. Blockchain technologies avoid trusted third parties and safeguard against a single point of failure and other issues. This has inspired researchers to investigate Blockchain's adoption into IoT ecosystem. In this paper, recent state-of-the-arts advances in Blockchain for IoT, Blockchain for Cloud IoT and Blockchain for Fog IoT in the context of eHealth, smart cities, intelligent transport and other applications are analyzed. Obstacles, research gaps and potential solutions are also presented.

1. Introduction

Nowadays, the Internet of Things (IoT) has attracted huge interest from academics, researchers, and entrepreneurs thanks to its capacity to offer innovative services across various applications[1, 2, 3]. IoT seamlessly interconnects heterogeneous devices and objects to create a physical network in which sensing, processing, and communication processes are automatically controlled and managed without human intervention[4]. With the advent of smart homes, smart cities and other intelligent things, IoT has become a field of immense influence, opportunities and development with the anticipation of more than 50 billion connected devices by 2020[5]. Different network technologies, including Wireless Sensor Networks (WSNs), Machine-to-Machine (M2M) or Cyber-Physical Systems (CPS) have been developed as indispensable elements for the broader term IoT in the literature. Consequently, security concerns relating to WSN, M2M, or CPS arise in IoT with the standard IP network protocol that requires protection for the entire network framework against security attacks. Otherwise, malicious attacks can obstruct IoT services as well as endanger the data security, users' privacy and confidentiality of the entire network.

However, Blockchain (BC) first successfully applied in cryptocurrencies has potentially emerged to be a highly secure and privacy-preserving technology for IoT applications[6, 7]. Blockchain refers to a decentralized, tamper-proof and transactional database that provides a secure way to store and process information across a large number of network participants[8]. In current settings, large quantities of data produced from large numbers of IoT devices may bottleneck an IoT system, resulting in poor quality of service (QoS)[9]. A single point of failure refers to a component of a system that can interrupt the entire network from running if it crashes, which is undesirable in any system for achieving high availability and reliability[10]. The Blockchain's peer-to-peer architecture is regarded as a possible solution to problems with a single point of failure and bottleneck[11, 12]. The adoption of Blockchain in IoT can overcome the single point of failure and serve as an adequate means to securely and efficiently store and process IoT data[8].

Further, Blockchain technology has evolved as an important remedy for eliminating trust in conventional authorities or more broadly, online intermediaries, as BC supposedly removes the need for trust amongst entities. In BC technology, participants are subject to the authority of a technological mechanism rather than using the authority of a centralized organization that can be perceived to be untrustworthy. Filippi et al.[13] made a point that Blockchain-based systems are intended to create trust in a particular system, not by entirely removing trust, but rather by maximising the degree of confidence between participants as a means of indirectly reducing the need for trust. BC allows a circle of

*Corresponding author
thumbnails/cas_email.jpeg
mdashrafuddin@students.federation.edu.au (Md.Ashraf Uddin); a.stranieri@federation.edu.au (A. Stranieri); iqbal.gondal@federation.edu.au (I. Gondal); v.balasubramanian@federation.edu.au (V. Balasubramanian)
ORCID(s):

trust between independent parties who do not agree to rely on a single third-party trust. This confidence or trust can be achieved more readily because of technical arrangements, particularly open-source software which indicates that to the extent, the code of a specific piece of software can be open, the possible outcome can be more readily predicted theoretically. Therefore, the higher predictability of the software code, the greater belief in the system and the lower need for faith in that technical system's developers or operators. For instance, anybody can study the open Bitcoin protocol. As a result, this assures participants that the network will produce a certain amount of new Bitcoins (12.5 bitcoins) at a particular speed(one Block per 10 minutes) when a miner wins in Proof of Work without relying on any financial institution or a centralized authority. Therefore, BC technology makes participants believe that no one needs to be trusted, and no one can pretend to be a trusted party[14].

However, Blockchain's complexity, including high computing costs and delays, is a challenge in the amalgamation of Blockchain with IoTs that have restricted power and storage capacities[15]. The challenges while handling IoT data on the Blockchain are depicted in Figure 1 and summarized below.

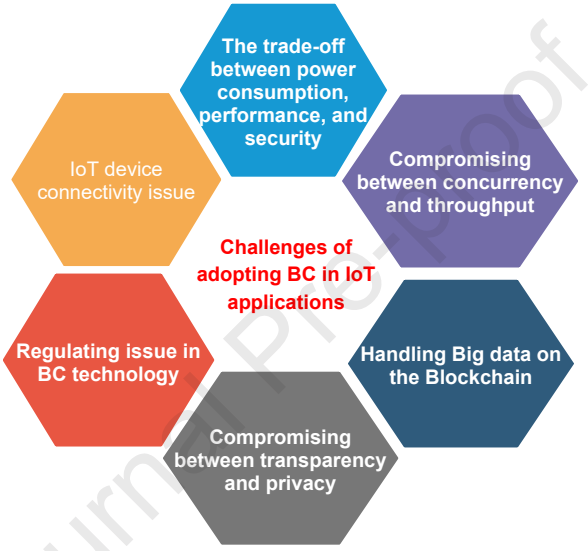


Figure 1: The challenges of adopting Blockchain in IoT

- **The trade-off between power consumption, performance, and security:** The high computational power required to run Blockchain algorithms has slowed down the advancement of these technology-based applications on resource constrained devices. Bitcoin's energy consumption are compared with the domestic power consumption of Ireland, which IoT devices cannot undertake[16]. Zhou et al. [11] reported that the entire Bitcoin network absorbs considerably more energy than several nations, including Austria and Colombia. In addition, researchers have questioned the performance of Blockchain to process IoT data and suggested optimizing its central algorithms to increase the number of confirmed Blocks per second[9]. For instances, elimination of the BC Proof of Work (PoW) consensus mechanism can reduce power consumption and improve performance[17]. On the contrary, PoW prevents malicious, Sybil attacks and makes the Blocks tamper-proof. Consequently, the goal is to refine BC processes to appropriately align security and efficiency[10].

- **Data concurrency and throughput issue[9]:** In IoT systems, the IoT devices continuously stream data which results in high concurrency[18]. The Blockchain throughput is limited thanks to its complex cryptographic security protocol and consensus mechanisms. The rapid synchronization of new Blocks among BC nodes in a chain-structured ledger requires a higher amount of bandwidth, which can improve BC throughput[11, 19]. Therefore, the challenge is to boost Blockchain's throughput to meet the need of frequent transactions in IoT systems.

- **Connectivity challenges of IoT[20]:** The IoT devices are expected to be connected to high computing storage

and networking resources to share IoT data with potential stakeholders. The IoT has limited capabilities to connect them with BC technology in order to provide novel business opportunities for the implementation of new applications and services in various domains.

- **Handling Big data on the Blockchain:** In the Blockchain network, every participant maintains a local copy of the complete distributed ledger. Upon the confirmation of a new Block, the Block is broadcast throughout the entire peer-to-peer network, and every node appends the confirmed Block to their local ledger. While this decentralised storage structure improves efficiency, solves the bottleneck problem and removes the need for third-party trust[21], the management of IoT data on the Blockchain puts a burden on participants' storage space. The study in [22] calculated that a Blockchain node would need approximately 730 GB of data storage per year if 1000 participants exchange a single 2 MB image per day in a Blockchain application. Therefore, the challenge is to address the increasing data storage requirements when Blockchain deals with IoT data.

- **Challenges in maintaining both transparency and privacy:** Blockchain can guarantee transparency of transactions, which is essential in some applications like finance. However, user's confidentiality may be adversely affected when storing and accessing IoT data from certain IoT systems such as eHealth on the BC[23]. To maintain a balanced degree of transparency and privacy, the development of cost-effective access control for IoT using Blockchain is necessary.

- **Regulating challenges of BC in IoT:** While several BC technological features including decentralization, immutability, anonymity, and automation are promising security solutions for diverse IoT applications, these features combined pose various new regulatory challenges[24]. The immutability feature implies that data is permanently published in DTL on the peer-to-peer network and cannot be deleted or modified. In addition, due to the absence of governance, records cannot be filtered for maintaining privacy before publishing them on the BC. Actions resulting from executing code such as smart contracts on a DTL can breach law. Due to the anonymity of the DTL, it is not so straightforward to distinguish the parties carrying out transactions for illegal services. Whilst the automation feature of the BC brings many advantages, the actors that cause some behaviours including errors in code and obfuscating code are ambiguous. Current IoT laws and regulations are becoming outdated especially with the advent of new disruptive technology such as Blockchain and need to be revised to undertake the DTL[25].

Recently, researchers[26, 27, 28, 29] have published a variety of works in the fields of IoT for eHealth, smart cities/home, supply chain, agriculture and industries by leveraging Blockchain technology. Miglani et al.[30] surveyed recent state-of-the-art works on BC technology in the context of the Internet of Energy (IoE) to provide readers with a broad insight into future potential and applications of BC in IoE sector. They described a range of applications of BC smart contract for energy management such as automated data exchange, energy transactions, energy-demanding and trading on the secure BC peer to peer network. Alladi et al.[31] summarized diverse applications of Blockchain technology in Unmanned Aerial Vehicles (UAV) systems with an in-depth analysis of how features of BC can assist in overcoming the problems of the UAV system. UAVs refer to a class of robotic vehicles that can transport payloads and carry out strike missions with either remote or autonomous control stations. UAVs raise new challenges, such as an increase in air traffic, the establishment of optimum routes, the generation of flight plans, the management of emergencies and the management of UAV swarms and cyber-physical attacks on UAVs. Research has shown that by using disruptive technologies such as BC, these issues can be minimized. Alladi et al.[32] also reviewed the latest research in diverse industrial sectors that adopted Blockchain technologies and addressed industry-specific obstacles for implementing BC. Hassija et al.[33] presented many security issues and identified multiple sources of cyber threats for IoT applications with regard to different layers of the IoT platform. Four emerging technologies; Blockchain, Fog, Cloud and Machine Learning have been explored to deal with security and privacy issues of IoT applications. Hassijai et al.[33] further discussed numerous issues raised from the solution itself. Alladi et al.[32] summarized major applications of Blockchain in smart grids with its important technical details, and prospects of commercial implementation. The challenges of adopting Blockchain into smart grid and future research directions in this field are discussed in this survey article. Vangala et al.[34] conducted a comprehensive literature review to analyze the security of the state-of-the-art advancements in smart agriculture utilizing BC technology. They also suggested a generalized BC-based security architecture for smart farming. The authors highlighted the drawbacks of existing research and presented future research directions in the field of artificial intelligence.

Table 1
The list of acronym

Acronym	Definition	Acronym	Definition
IoT	Internet of Things	BC	Blockchain
WSN	Wireless Sensor Network	M2M	Machine-to-Machine
CPS	Cyber-Physical Systems	QoS	Quality of Service
PoW	Proof of Work	BCIoT	Blockchain and Internet of Things
BCCoT	Blockchain and Cloud of Things	BCFoT	Blockchain and Fog of Things
DS	Digital Signature	PKI	Public Key cryptography
PoS	Proof of Stake	BFT	Byzantine Fault Tolerance
PoA	Proof of Authority	PoET	Proof of Elapsed Time
SGX	Intel Software Guard Extensions	DDoS	Distributed Denial of Service
LPoS	Leased Proof of Stake	DPoS	Delegated Proof of Stake
DTL	Distributed Transaction Ledger	P2P	Peer to Peer
EHR	Electronic Health Record	EMR	Electronic Medical Record
IoE	Internet of Everything	NOS	Network Operating System
CAT	Computed Tomography	TRL	Transaction and Read Latency
TRT	Transaction and Read Throughput	TL	Transaction Latency
RL	Read Latency	ABE	Attribute-Based Encryption
IPFS	Interplanetary File System	SAT	security access token
GDPR	General Data Protection Regulation	CSP	Cloud Service Providers
AHS	Artificial Healthcare System	API	Application Programming Interface
ARX	Add Rotate Xor	SVM	Support Vector Machine
VANET	Vehicular Distributed Ad-hoc	OBU	On Board Unit
CORE	Common Open Research Emulator	MAS	Multi-Agent System
RSU	Roadside Unit	AV	Autonomous Vehicle
NFV	Network Function Virtualization	SDN	Software Defined Network
CH	Cluster Head	SC	Smart Contract
IoUT	Internet of Underwater Things	PoBT	Proof of Block Trade
ACL	Access Control List	BASN	Body Area Sensor Networks
RFID	Radio-Frequency Identification	PCA	Patient Centric Agent
RPM	Remote Patient Monitoring	DAG	Directed Acyclic Graph
HLF	Hyperledger Fabric	LSTM	Long Short Term Memory
G2V	Grid to Vehicle	V2G	Vehicle to Grid
SWF	Simple Workflow Services	EVM	Ethereum Virtual Machine
VANET	Vehicular Adhoc Network	IoE	Internet of Energy

The goal of our article is to review the very recent state-of-the-art works related to Blockchain in various IoT fields and discuss those works with respect to different Blockchain terminologies. Our paper differs from the existing review articles in several ways. Most of the review articles [26, 27, 28, 29] focus on the adoption of Blockchain in a specific IoT area. In contrast, we reviewed state-of-the-art works from diverse IoT fields including eHealth, smart home and smart vehicular networks. The current survey papers presented the existing Blockchain research concerning a limited number of features while we outlined the breakdown of the reviewed studies in the context of various components. In addition, the basic of Blockchain technology has been described in detail in order to attract a broad group of readers.

Our contributions in the article are presented below:

1. Description of different components of Blockchain technologies such as transactions, digital signature, Block, consensus mechanisms, and BC types with their advantages and limitations when applied in the IoT domain.
2. Reviewing of recent research works that use Blockchain. Analysis of the literature with respect to the following

attributes: a) the type of BC to be utilized b) the consensus mechanism to be applied c) has an access control mechanism been implemented d) is scalability addressed, e) is the storage method on-chain or off-chain, f) what tools or simulators are utilized, g) what major contributions/outcomes are advanced and h) limitations/remarks.
3. The research gap and challenges in contemplating Blockchain into IoT are identified and discussed with possible solutions addressed in the literature.

Table 1 presents the list of the acronym used in this article. The rest of the paper is organized as follows: to accommodate a wide variety of readers, the paper starts with the basics of Blockchain technology. Section 2.1, 2.2, 2.3, and 2.4 provide an overview of Blockchain's fundamental components, the description of BC technology, the objectives and the limitations of this technology in IoT applications respectively. Following this, the paper discusses the potential adaptability of Blockchain in Internet of Things, Fog, Cloud of Things and SDN technologies in Section 2.5, 2.7, 2.6, and 2.8, respectively. The state-of-the-art works that explored BC and the Internet of Things, BC and Cloud of Things and BC and Fog of Things model in healthcare, supply chain, smart home, smart vehicular network, and miscellaneous IoT applications are presented in Section 3.1, 3.2, 3.3 and 3.4, respectively. The identified research gaps and solutions are described in Section 4 before concluding the article in Section 5.

2. Blockchain, Internet of Things, Fog, Cloud of Things, and SDN paradigm

This section describes BC technologies in detail and includes issues that arise with BC and Internet of Things, Fog of Things, Cloud of Things, and Software-Defined Networks (SDN). The basics of BC are provided in the next section 2.1 followed by a detail description of each component 2.2. In 2.3, the objectives of deploying BC with IoT are described followed by some limitations. The studies reviewed in this article included Internet of Things, Fog and Cloud of Things with Blockchain technology to construct a framework for eHealth, wireless sensor network and smart home etc. The Internet of Things, Fog, Cloud of Things, Software Defined Network together with Blockchain technologies are described in this section 2.5, 2.7, 2.6, and 2.8, respectively before reviewing existing research from diverse domains that incorporated the technologies mentioned above.

2.1. Basics of Blockchain technology

Blockchain is typically defined as a transparent, trusted, and decentralised ledger on a peer-to-peer network[10] and mostly known as the underlying technology of the virtual Bitcoin cryptocurrency invented by Satoshi Nakamoto in 2008. The data unit on the Blockchain is called a transaction, and certain numbers of transactions are bundled in a Block. A decentralized Blockchain ledger is created with all confirmed Blocks. A Block in the distributed ledger is linked to the previously approved Block using a cryptographic hash code of the Block [36].This emerging technology has already been widely explored to develop a range of applications beyond digital cryptocurrencies. Every participant on a peer-to-peer network can verify the behaviour of other participants within the network, as well as make, verify and approve a new transaction to be recorded in the Blockchain. This infrastructure guarantees stable and efficient Blockchain operations with the benefits of tamper resistance and reduce single point of failure vulnerabilities [37]. The Blockchain ledger is available to all participants but still not regulated by any network authorities. This principle is accomplished by imposing strict rules and mutual agreement among the network nodes, which is characterised as the consensus mechanism. The consensus mechanism refers to the process of synchronising the decentralised ledger across all the nodes in the Blockchain network. Figure 2 provides an overview of how the Bitcoin Blockchain operates.

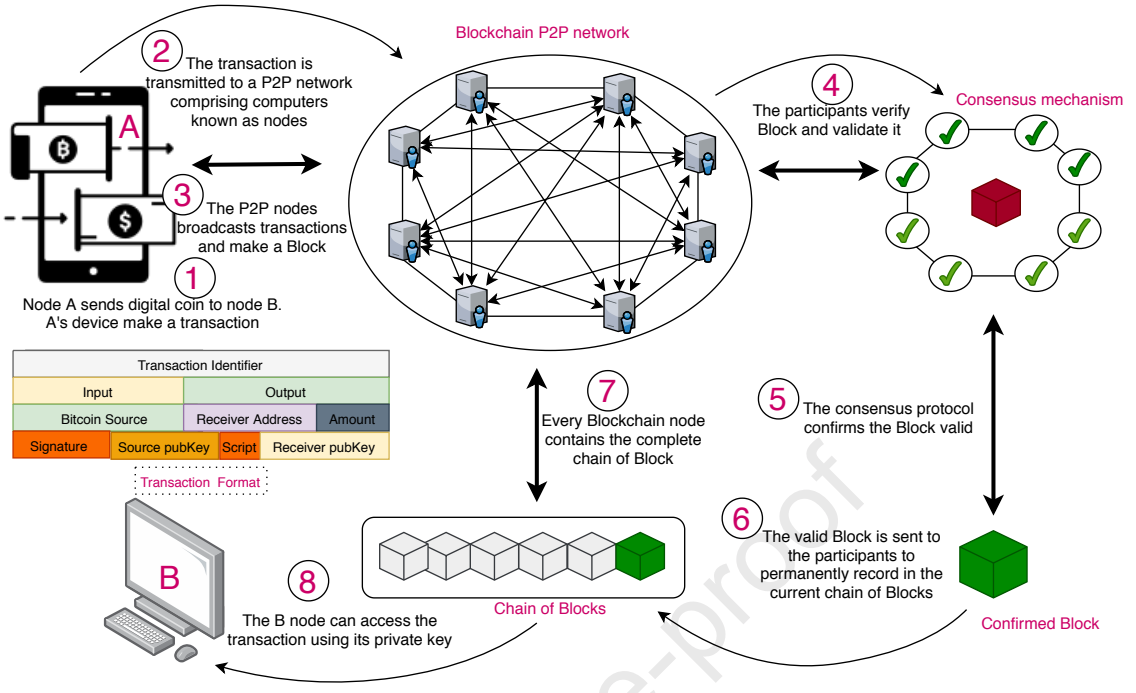


Figure 2: The basic operation of Bitcoin Blockchain (adopted from [35])

Here, the superscript in front of the bullet points is mapped to the different steps of Figure 2.

- [1] A participant **A** transfers a certain amount of digital coins to another participant **B**. **A**'s device initiates a transaction. Participants can usually use their portable devices such as smartphone, laptop and low-processing computer for making transactions. The transactions are signed with **A**'s private key and if necessary, the transaction contents are encrypted with **B**'s public key.
- [2] **A**'s device transmits the transaction to a peer-to-peer network comprising of high-processing devices also called nodes. The Blockchain protocols are implemented on this network.
- [3]The nodes on the Blockchain network replicate the transaction and broadcast it throughout the network. The nodes packed a certain numbers of transactions in a Block. The structure of a typical Block is depicted in Figure 4.
- [4,5,6] All the participants append the Block to existing chain of confirmed Blocks only if a target hash code is created by solving complex mathematical puzzle known as Proof of Work. This process called consensus mechanism varies in terms of computational cost and turnaround time. Some of the popular consensus mechanisms are discussed in the later section.
- [8] **B**'s device can access the transaction from the confirmed Block using its private key.

2.2. Description of the Blockchain technologies

Many research articles[38, 39, 32] partitioned Blockchain technologies into different layers. The section describes five layers of a BC technology along with the investigation of Blockchain's core properties related to immutability, security, and integrity. The layered structure of the BC depicted in Figure 3 is discussed below.

2.2.1. The data layer

This layer consists of transactions, Blocks, Hash function, Merkle tree, and the Digital signature. Important components of this layer are discussed below:

Data Block: Blockchain is fundamentally a chain of Blocks, a linear structure that starts with a so-called genesis Block and continues with each new confirmed Block connected to that chain. Each Block comprises several transactions and has a field containing the hashtag of its immediately preceding Block, which creates links between them.

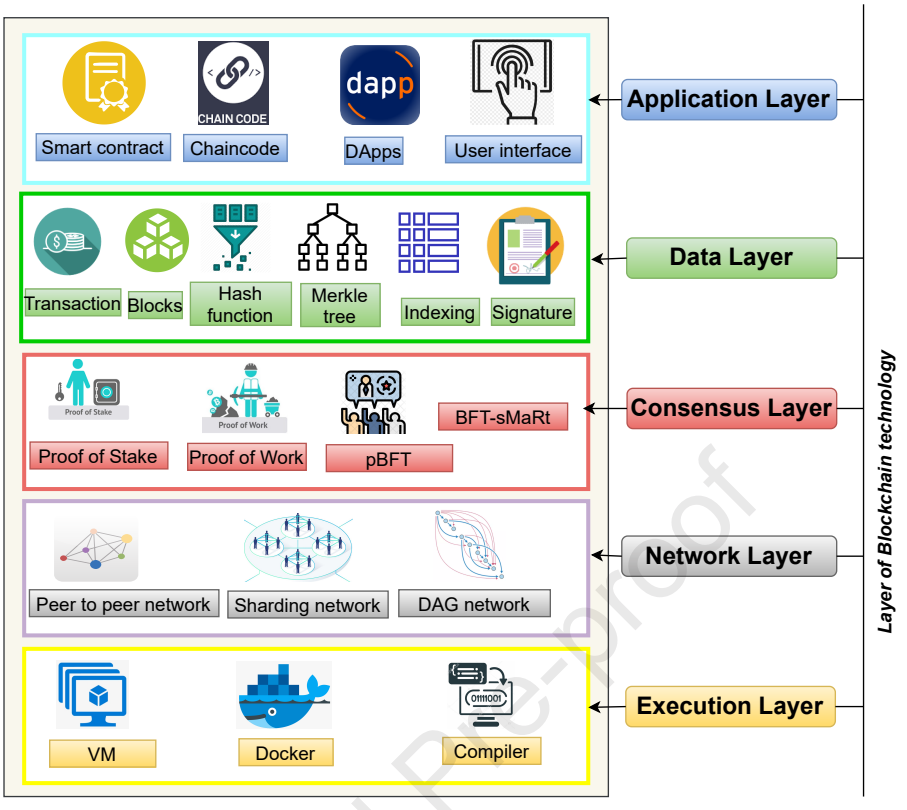


Figure 3: The layered structure of Blockchain technology

Consequently, all confirmed Blocks in the chain can be traced back through cryptographic hash code; any modification or alteration to the data of any Blocks is not possible. A typical data Block is divided into two parts: transaction records and a header.

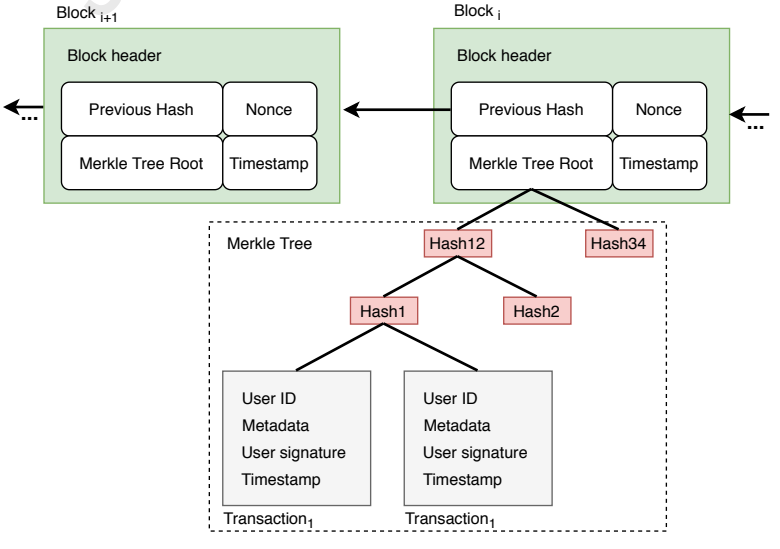


Figure 4: The structure of a Block

Transaction records are organised in a Merkle tree as depicted in Figure 4. A Merkle tree refers to a binary tree structure that summarizes and allows content to be checked efficiently and securely within a large data set. If the transactions are not packed into Merkle trees, each node of the network would need to keep a complete copy of each transaction which has ever taken place on the Blockchain[9]. A Merkle tree summarises all transactions within a Block by generating a digital fingerprint of the entire collection of transactions, enabling a user to check whether a transaction is included in a Block or not. If a single transaction is modified or altered, the Merkle tree root is also modified. One field in the Block's header contains the Merkle tree root that is generated while making the Block. Merkle trees are generated by hashing node pairs repeatedly until just one hash is left and this hash is called the root hash, or the root of the Merkle tree. Each leaf node holds a hash of transaction data, and each non-leaf node contains a hash of its previous hashes. A transaction is made when a user carries out activities on the Blockchain. For instance, a transaction with associated metadata and signed with a user's private key to ensure trust is created if the user exchanges digital currencies or makes a contract.

In general, the Block header includes: 1) a hash of the previous Block for authentication, 2) a Merkle tree root for packing a group of transactions 3) a Nonce that produces a hash value below the target level by means of a consensus mechanism and 4) a Timestamp referring to the time when the Block has been created.

Figure 5 adopted from [40] demonstrates a typical procedure for producing a digest from the header of a BC Block. The header is partitioned into two portions. The first portion is fed to an SHA 256 hash function which output as Initialize Vector (IV) along with the second portion of the header is input to the second SHA 256 hash function. Finally, the digest from the second SHA256 hash function with 256 bits padding is fed to the third SHA 256 function to produce the final digest from the Block header. In the Proof of Work BC, the nonce field in the Block header is continuously incremented by Miner nodes until the target hash code is generated.

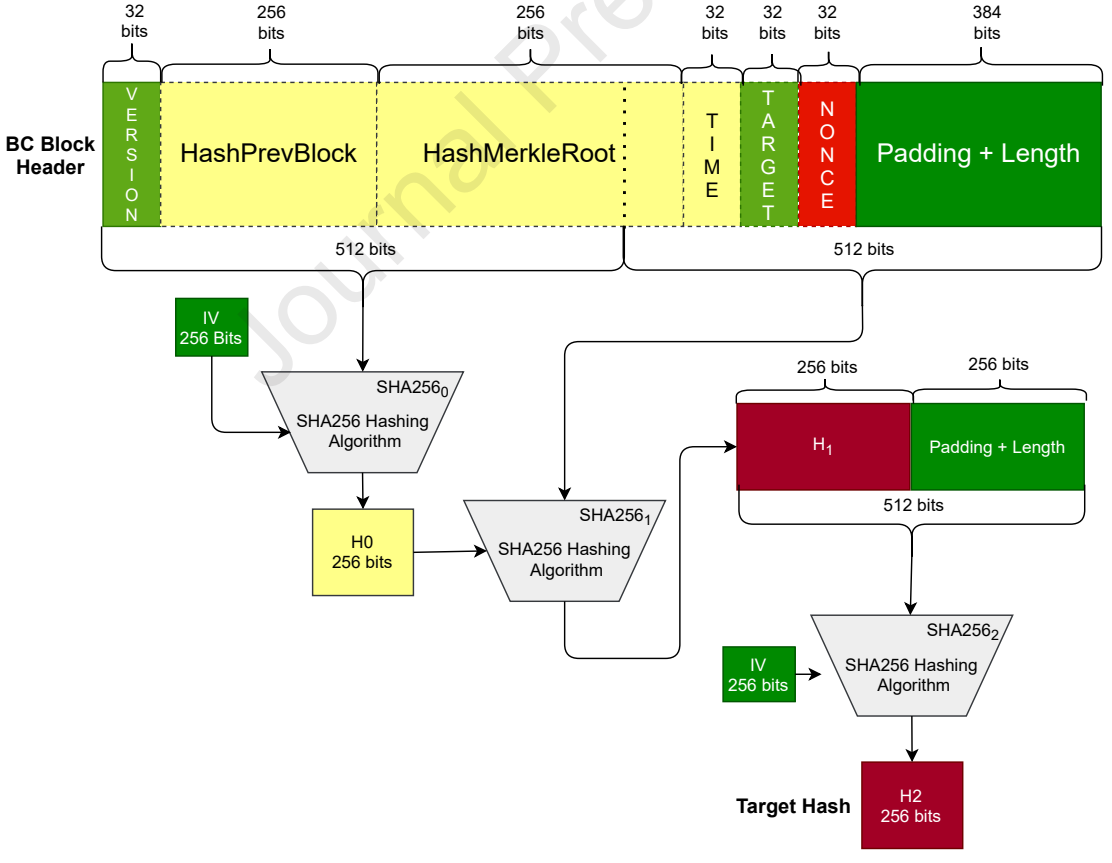


Figure 5: The Bitcoin Block Header Hashing Algorithm

The Block is shared among the participants on the peer-to-peer network, and each participant links the Block to

the existing chain of Blocks only if the Block is approved by the consensus mechanism described in the later section. Thus, a decentralized ledger is formed on the Blockchain and each node stores one copy of that ledger. This eliminates the need for the central control point, resulting in a high level of equity among the participants of the Blockchain. In addition, each Block in the distributed ledger always has a distinctive cryptographic signature associated with a timestamp which makes the ledger auditable and unchangeable.

Digital Signature A digital signature (DS)[41] refers to a cryptographic approach to authenticate digital content and guarantee its integrity. DS utilizes a public key cryptography (PKI) system. Public key cryptography (PKI) consists of a public and private key that are paired together but asymmetric (not identical). The public key in the pair is usually shared with the authorized entities and the owner of this key pairs does not disclose the private key. Either of the keys can be applied to encrypt a message; the opposite key that is not employed to encrypt the message from the pairs is utilized to decrypt the message. Figure 6 (a) demonstrates that a message is encrypted with a public key, a private key is utilized to decrypt the message. Alternatively, Figure 6 (b) shows that the ciphertext of the message is generated using private key and plaintext is produced using the public key.

The public key of a user is known as his or her address like a bank account in BC technologies such as Bitcoin or Ethereum. Anyone can send digital currencies to a user's address (Public Key) and only the user can access the currencies using his private key of the corresponding PKI. Figure 7 explains signing a message using the private key and verifying the message with the public key in the Bitcoin BC.

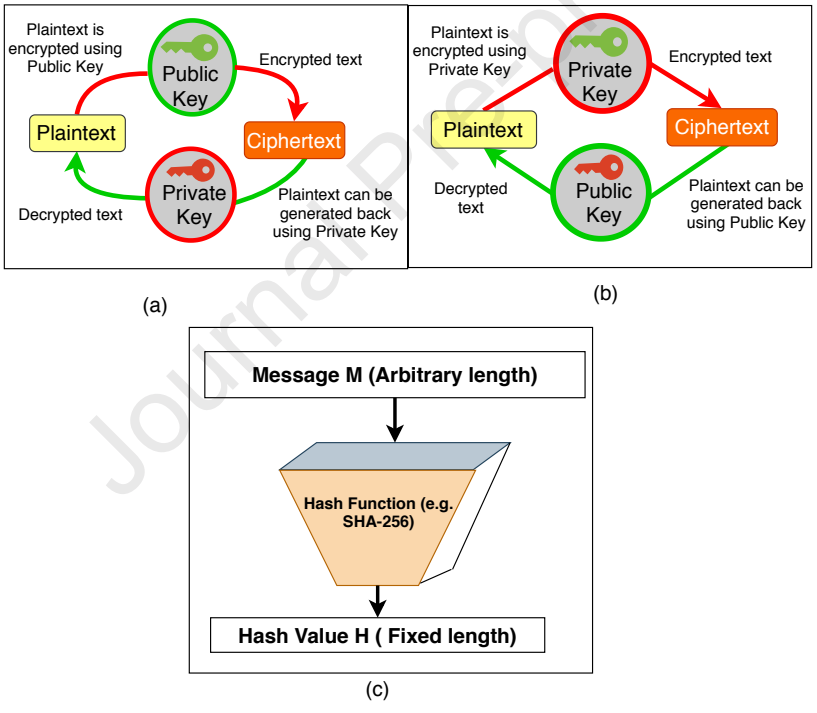


Figure 6: The properties of public and private key pairs

- Signing a message with a sender's private key: To generate a digital signature of a message, the sender's signing algorithm produces a one-way hash of the message. A cryptographic hash function depicted in Figure 6 is a mathematical algorithm that takes an arbitrary amount of data input to map the content to a bit array of a fixed size called hash value or just a "hash". The hash algorithm is a one-way function which is practically infeasible to invert[40]. The hash also known as digest of the message is encrypted with the sender's private key. The digest along with other information such as the hashing algorithm is appended with the original message as a DS of the transmitted data.
- Verifying the message with the sender's public key: The receiver's signature algorithm verifies the electronic

signature associated with the original content in two steps: 1) generating the hash or digest of the message 2) decrypting the appended digital signature using the sender's public key. If both digests are identical, the data has not been changed. Otherwise, either the message or signature has been altered or the digest has not been decrypted with the private key of the corresponding public key.

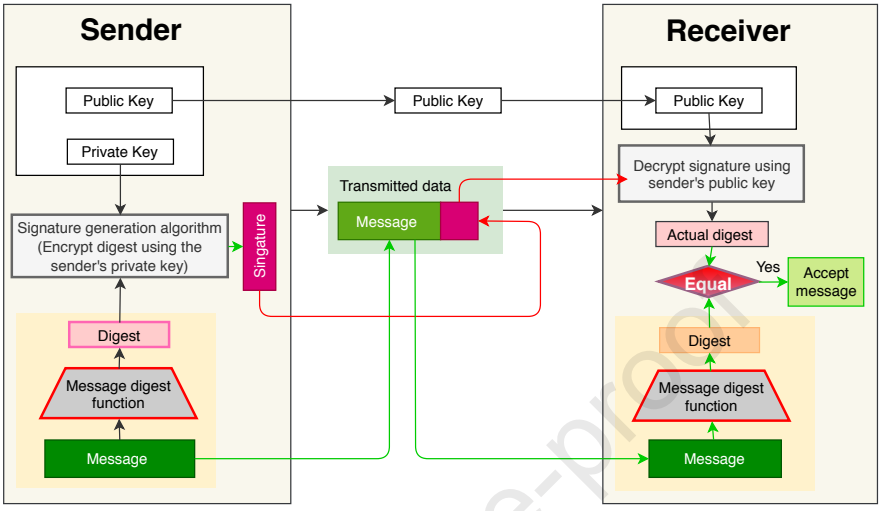


Figure 7: The processing of forming and verifying digital signature in Bitcoin BC

Different Types and Schemes of Digital Signature In this section, we briefly discuss different forms of digital signature schemes with the merits and demerits of various technologies utilized to implement digital signature in Blockchain are presented in Table 2.

1. Aggregate signature: The aggregate signature[42] is a traditional digital signature scheme based on co-GDH (Gap Diffie-Hellman)[43] and bilinear mapping with an aggregation function. This scheme combines signatures of multiple documents into a single signature. For instance, users with public keys $PK_1, \ldots, PK_n$ sign messages $M_1, \ldots, M_n$ and create signatures $s_1, \ldots, s_n$. Using aggregate signature scheme, signatures $(s_1, \ldots, s_n)$ can be compacted into a tiny signature s. This single signature can be verified using respective set of public keys to check integrity of messages$(M_1, \ldots, M_n)$. Consequently, aggregate signatures can address the issue of limited storage and bandwidth.
2. Group signature: A group signature scheme[44] is a method for enabling one of the members of the group to sign anonymously on behalf of the group and in special cases, provide the possibility of tracing the identity of the signer. A participant in the group can verify the signature using the verification key that it was indeed created by someone in the group but cannot discover who creates the signature. The authority can track the signer back in the event of conflicts or misbehaviour using the tracing key. Helix Blockchain[45] implemented group signature for ensuring that transactions are ordered in a fair way in a Block.
3. Ring signature: Ring signature schemes[46, 47] enable the participants to sign a document in an anonymous way on behalf of a spontaneous group. The ring signature scheme, unlike group signature, does not need the group manager to construct the group or allocate keys to members of the group. The signer, in other terms, will spontaneously create the group without the assistance of other group members. Several cryptocurrencies including Bytecoin[48], ShadowCash[49], Monero[48], Zcoin[50], and Dash[49] implemented ring signature to preserve users' privacy.
4. Blind signature: Blind signature[51] is a form of digital signature that blinds the document before signing it. The signer will therefore not know the content of the document. A variety of public-key encryption schemes can be applied to create blind signatures. PayCash[52] and Moneta Express[51] have already implemented blind signature in their payment system.

5. Proxy signature: A proxy signature scheme[53] enables an entity known as the designator or original signer to delegate authorization to another entity called as a proxy signer to sign messages on its behalf in case the original signer is unable to sign due to temporal absence, lack of time or processing power.

Different digital signature algorithms vary in the technique for generating public/private keys. Several schemes of forming digital signature is presented in Table 2 and 3.

Table 2
Different schemes to form digital signature

Digital Signature	Description	Merits and demerits
RSA[54, 55]	This signature scheme is based on the RSA cryptography. The strength of RSA is derived from the computational complexity of factoring large integers which are the multiplication of two large prime numbers.	• Key distribution is convenient • Smaller numbers of key are required for large network compared to symmetric key • Low operating speed and high computational cost • Vulnerable to multiplicative attacks
ECDSA[56, 55]	Elliptic Curve Cryptography (ECC) is an alternative to RSA for digital signature development based on elliptic curve theory that produces quicker, smaller, and more powerful cryptographic keys. The algorithm's strength levels derive from the problem of solving the discrete logarithm in the elliptic curve point group.	• Faster, smaller, and powerful • No application-based performance issues • A little chance of identical signature for two different contents
ElGamal Encryption System[57]	The security of this technique stem from the complexity of computing discrete finite field logarithms. The ElGamal encryption system encompasses both encryption and digital signature algorithms.	• Providing high level of security because of probabilistic nature • Facilitating digital signature for large numbers using a single key • longer computing cost for doubling the length of texts

Table 3
Different schemes to from digital signature

Digital Signature	Description	Merits and demerits
DSA[58]	DSA is a Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiation and the discrete logarithm problem. DSA is a variant of the Schnorr and ElGamal signature schemes.	• Lower computational costs and storage space • Complicated remainder operators for verifying signature
GOST R 34.10-2012[59]	This is the Russian standard algorithms for generating and verifying digital signature based on elliptic curves.	Recommendations for curve uses are not required provided that only a set of requirements for such curves is needed
Schnorr Signature Algorithm[60]	This is a variation of the ElGamal encryption system and the FiatShamir scheme	Smaller signature size
Rapid Digital Signature[61]	This underpins BLS, DiffieHellman, and the Fiat-Shamir scheme.	• Simplified computing, pushing up performance levels • limited to groups with the pair matching function
Rabin Crypto system[62]	Security strength stems from the difficulty of integer factorization	• Higher operating speed • Susceptible to an attack based on the selected ciphertext

2.2.2. The consensus layer

No centralised body is commissioned to monitor the transaction or prevent attackers from manipulating or altering data when a node exchanges data on the Blockchain network. To avoid fraud-related activities such as double-spending attacks, the trustworthiness of the Block must be checked, and the data flow should be controlled to ensure the smooth exchange of information[63]. These requirements are met using validation protocols known as consensus algorithms. In the Blockchain context, a consensus algorithm is a method of reaching an agreement between multiple insecure nodes on a single data block. Several consensus mechanisms from the literature are described below and presented in Figure 8 which shows five categorizations of consensus mechanism: Proof of Work(PoW), Proof of Stake(PoS), Byzantine Fault Tolerance(BFT), Proof of Authority(PoA) and Proof of Elapsed Time(PoET). Several consensus protocols are described below.

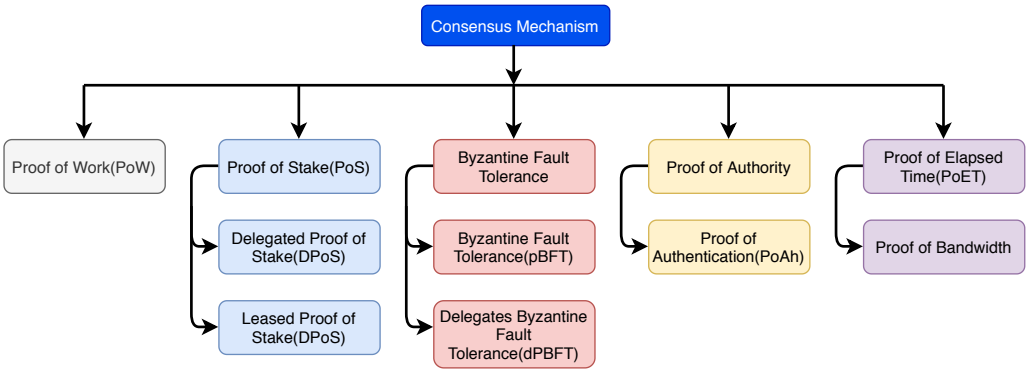


Figure 8: The taxonomy of consensus mechanism

1. **Practical Byzantine Fault Tolerance(pBFT):** Byzantine Fault Tolerance(BFT)[64] derived from Byzantine general problems aims to reach an agreement between nodes in a distributed network even if some nodes of the network fail to respond or respond with false information. The BFT mechanism can defend network failures through collective decision-making that reduces the impact of the flawed nodes. The practical BFT consensus mechanism is described below:
   (a) A centralized authority chooses a group of nodes[65]. One node from this group is elected as the primary node, often called a leader. Other nodes which are also to be picked by turn as primary nodes are called secondary nodes or backup nodes.
   (b) Next, a client's request is submitted to the primary node.
   (c) After that, the primary/leader node broadcasts the request throughout the network so that all the secondary/backup nodes receive the request.
   (d) Both primary and secondary nodes perform the service requested by the client and send it a reply. The service is successfully confirmed if the client receives $m + 1$ number of responses with the same result where m is the number of defective nodes permitted within the network.

   Practical BFT effectively works well in distributed networks with a limited number of nodes, but with this protocol, communication overhead exponentially increases for each additional node that joins the network. Further, practical BFT is prone to Sybil attacks (one participant maintains many identifiers that can influence this mechanism)[66].
2. **Proof of Elapsed Time (PoET)** [37, 67, 68]: In Proof of Elapsed Time, participants on the Blockchain must wait for a random time. The participant who first finishes the waiting period is nominated as a leader for making a new Block. However, a participant can intentionally choose a short waiting time to be a winner or the winner might not complete its waiting time. To tackle this issue, Intel implemented Intel Software Guard Extensions (SGX) which enables the running of an enterprise providing trusted code for an application in a secure environment. SGX[12] referring to a particular set of CPU instructions prevents participants from manipulating waiting time in PoET. Intel SGX creates a certificate which ensures that a specific trusted code was correctly run in a protected environment. A new participant is required to download the trusted program to join the Blockchain. The trusted program executed on SGX hardware generates an SGX certificate for the participant, which includes the user's public key. The participant sends this certificate to the rest of the network requesting permission to join the Blockchain. The trusted program provides the participant with a timer object authenticated using the private key of the trusted program. The participant is required to wait for the time specified in the timer object. This approach is much more energy-efficient than other consensus protocols such as Proof of Work.
3. **Leased Proof of Stake:** Leased Proof of Stake(LPoS)[69] is a variation of the standard Proof of Stake consensus protocol. In regular PoS, every node with a certain amount of digital coin is eligible to mine the next Block. But, nodes that hold a higher amount of cryptocurrency have a higher chance of winning in the mining process. As a result, nodes with small digital coins are unlikely to succeed to mine the next Block or need to wait for long periods. LPoS has been suggested to overcome the drawbacks of standard PoS. With LPoS, a participant owning a low amount of stake can lease or rent its stake to a full node (staking node), which increases the full node's chance of becoming the next miner. The leased funds remain in total control of the holder. If that staking node gets the opportunity to add a Block, it receives incentives which are shared proportionally between the staking node and its leasing nodes. A Blockchain user has the choice of operating as a full node or leasing their stake to a full node to earn a proportional reward.
4. **Delegated Proof of Stake(DPoS)** [70]: In DPoS, users can vote for the nodes that invest resources in the Blockchain system. The strength of a user's vote is proportional to the number of tokens the user holds[11]. As a result, a group of rich nodes can dominate the network and decide who will be the witness. The nodes with a higher number of votes called the witnesses are responsible for making Blocks and get paid for their services. Nevertheless, as the network expands, the witness has to compete to remain paid. Voting in this protocol is an ongoing operation. The network users disqualify a witness if the witness plays bad roles in processing the Block.
5. **Proof of Bandwidth:** In this process, the miner is selected and rewarded based on the bandwidth they contribute to the network. However, malicious nodes can falsely report their bandwidths. Therefore, a bandwidth measurement scheme is adopted to estimate the bandwidth that each participant contributes to the Blockchain. Blockchain nodes can evaluate and measure each other's bandwidth contribution to reach an accurate consensus about relaying bandwidth. This approach can resist attacks that are occurred by malicious nodes' colluding[71].

6. **Proof of Authority:** Proof of Authority(PoA)[72] is a consensus protocol that provides a small and designated group of Blockchain actors with the power to validate transactions. The PoA protocol leverages authorities' trust, which indicates that Block validators are not required to stake coins; instead, they stake their reputation to the system. The PoA is applicable for private Blockchain and scalable since the limited numbers of pre-approved validators.
7. **Proof of Authentication[73]:** In Proof of Work, the first step a miner performs is to validate the Block, followed by calculating the target hash value of the Block. Conversely, Proof of Authentication[74] intends to authenticate the Blocks by verifying the Blocks' transactions according to PoW. In Proof of Authentication, a small group of trusted nodes are selected to confirm the Block and then add it to the distributed ledger. The authentication process involves two steps: verifying the source of the Block and increasing the point of each node that performs the authentication by one as its reputation. Every time a node conducting false authentication loses a specific unit of trust value and is reported as a regular node after a certain number of invalid authentications have been performed by it. Finally, the validators broadcast the Block throughout the network for all the nodes to update the distributed ledger. Proof of Authentication is deemed as appropriate consensus protocol in IoT as it avoids the inverse hash computation for energy-efficient distributed secure communications and computing in IoT[74].

2.2.3. The network layer

The network layer, also known as the P2P network, establishes communication between nodes. The P2P network ensures that all nodes can discover and connect each other to propagate Blocks throughout the network and synchronize the valid current state of the BC. A P2P network is a network of computers where computers (nodes) are distributed, and the workload of the network is shared across multiple nodes to achieve the end target nodes on the Blockchain for processing transactions and Blocks. Two kinds of nodes are maintained in the BC peer to peer network: the full node and the light node. Full nodes ensure that transactions and Blocks are checked and validated using rules prescribed in the consensus mechanism, which is also called mining. Full nodes are accountable for holding trust in the network, whereas light nodes can make transactions and send those to the full node. Light nodes can only store the header of the Blockchain (keys) while the full nodes store the complete distributed ledger.

Sharding: Sharding[75] that partitions a peer to peer network is introduced to improve Blockchain's performance. Sharding is a splitting strategy that distributes computing and storage workloads across a P2P network such that unlike conventional BC, each node is not responsible for managing the entire network's transactions load, but instead handles information related to its partition or shard. Figure 9 presents an example of BC sharding. In this technique, several Blockchains called a chain of a shard are managed by network nodes instead of maintaining a single BC for all transactions. Each shard consists of its own nodes or validators that apply a PoW or staking or voting consensus mechanism. Readers are suggested to go through [75, 76, 77] to have comprehensive knowledge on BC sharding.

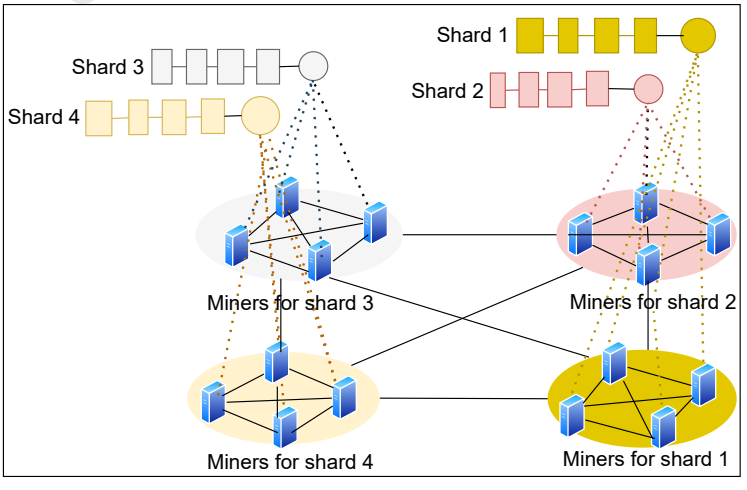


Figure 9: Example of a BC sharding

2.2.4. The infrastructure layer

We describe the infrastructure layer of Blockchain technology for two enterprise BCs: Ethereum[78] and Hyperledger Fabric (HF)[79].

A user's computer can participate in Ethereum Blockchain by running a client software such as Geth, Parity or Pantheon. Ethereum maintains two kinds of nodes: light node, and full node. The light node runs the client software stores the cache, and the state of the Ethereum. Further, the light node engages in verifying the execution of transactions while the full nodes download the entire ledger in their local storage, participate in full consensus enforcement, verify signature, transactions, and Block formats and check double-spending. The Ethereum nodes execute the Ethereum Virtual Machine (EVM) which is like Java Virtual Machines (JVMs) running byte code. EVM acting as sandboxes offers an execution environment for a smart contract. EVM is a Turing complete software; a stake-based virtual machine that handles the internal state and computation for smart contract.

The Hyperledger Fabric BC[79] is comprised of three types of nodes: 1) endorsers, 2) orderers, and 3) peer nodes. The peer nodes host ledgers and chaincode that is also known as smart contracts. The uses' applications and administrators using Fabric Software Development Kit (SDK) APIs can always communicate with peer nodes to access the chaincode or distributed ledger. The Hyperledger Fabric manages multiple channels that refer to different private subnetworks consisting of a number of peers(member). Each channel maintains its separate ledger which is stored in each peer on the channel. A specific set of applications and peers can communicate to HF via channels. The transactions flow in the Hyperledger Fabric in the following three phases.

- Endorsing phase: First, the endorsing peers receive update transactions from an application. These nodes endorse a transaction without committing it in the ledger. They send the endorsement of the transaction to the orderer nodes.
- Ordering phase: The orderer nodes collect endorsed transactions for various applications from the endorsing nodes. These nodes order the transactions into Block.
- Distribution phase: Finally, the Block is distributed to all the peer nodes on the BC business network. These peers will validate the transaction and will commit the transaction to their local copy of the ledger upon successful validation.

2.2.5. The application layer

The BC application layer includes smart contracts, chaincode, and dApps. This layer comprises two sub-layers: 1) presentation layer and 2) execution layer. The presentation layer includes scripts, APIs, and user interface. These tools are used to connect the application layer with the Blockchain network. The execution layer includes smart contracts, chaincode and underlying rules. The presentation layer sends instructions to the execution layer, which runs transactions. For example, instructions are sent to chaincode in Hyperledger Fabric and smart contract in Ethereum Virtual Machine. The components of the application layer are listed below.

- **Smart Contract:** Smart contract[80] written in Solidity language runs on the Ethereum runtime engine. The compiler produces bytecode of a smart contract that runs faster on the EVM. Code executed on an EVM is isolated from the network or file system. A smart contract refers to a set of business logic presented in various functions that are executed when a transaction against those functions is issued. The bytecode of a smart contract is assigned a unique address after deploying it on the EVM. A transaction associated with a smart contract can result in a state change in the decentralized ledger. Figure 10 is an example of a smart contract application for managing the trust for e-commerce sites. Many studies reviewed in this paper used a smart contract for different purposes in IoT applications as provided in Table 4.
- **Chaincode:** In Hyperledger Fabric, several related smart contracts are packaged together into chaincode that is deployed in the BC business network. For example, an insurance application needs to implement their business logic in the form of multiple smart contracts named as claims, liability, processing, and so on, which together constitute a chaincode. The chaincode governs packaging and deployment of smart contracts in the Hyperledger Fabric. Further, chaincode defines the schema of ledger's data, initiates it, performs updates to ledgers based on consensus, and responds to queries for ledger data.

  Unlike EVM, in Hyperledger Fabric, chaincode written in standard languages such as Java, Node.js and Go is deployed on peer nodes owned by different organizations. The chaincode runs on a secure Docker container. The

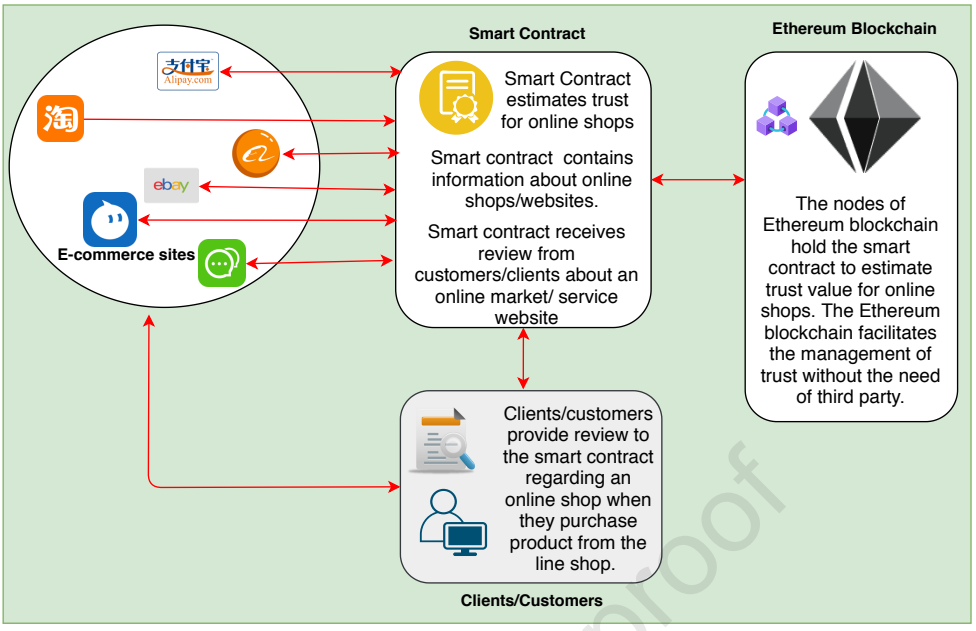


Figure 10: Example of a smart contract application

Table 4
Smart contracts in different IoT applications

References	Purpose	Applications
[81] [82][83][82][84]	Access control	eHealth
[85][83] [86]	Tracking access behaviour, access policies	eHealth data sharing, Edge network
[87][88] [89] [90][91][92]	Store sensor data	Body Area Sensor Networks
[93, 94]	Crowdsourcing	eHealth
[95] [96][97] [98] [99]	Incentive and payment management	EMRs, IoT smart cities
[100]	Enrolling patients and healthcare professionals	Remote patient monitoring system
[101] [102][103][104]	Authorization	Medical Forensics, Edge services
[105] [106] [107]	Maintain log information, auditing, analyzing	Biomedical queries, IoT
[108][109]	Maintaining policies for updating firmware	Vehicular network, supply chain in IoT
[110] [111]	Managing node's reputation	IoT ecosystem
[112]	Resource management in Edge network	SDN-IoT ecosystem
[113][114]	Detection of malicious activities	SDN-IoT ecosystem
[115]	Energy management	Smart grid
[116]	Trust management	Edge-Cloud network

client applications can access the chaincode via REST APIs or SDK. Chaincodes are initiated for a particular channel where an administrator determines the endorsement policy for a chaincode running on the channel.

- **dApps:** dApp refers to a distributed web application that runs on top of a distributed Blockchain technologies such as Ethereum, Bitcoin, and Hyperledger Fabric. dApp can interact with Blockchain using smart contract or

chaincode. Unlike a conventional app, dApp is no longer controlled by a single entity or an organization once it is deployed on the BC network.

2.2.6. Types of Blockchain technology

Figure 11 shows a classification of decentralized ledger technology (DTL). The forms of DTL in the literature differ with respect to data structure and accessibility.

In chain structured DTL, Blocks are interlinked in linear sequential orders while graph-structured DTL stores transactions in a Distributed Acyclic Graph (DAG)[10, 117]. Individual DAG transactions are directly connected to each other rather than joined together and processed in Blocks. Depending on the accessibility, BC can be further categorized into two major types: public Blockchain (or permission-less) and private Blockchain (or permitted). A public Blockchain is a non-restrictive, permission-less distributed ledger system that allows anyone to join the network and make transactions as well as engage in the consensus process[107]. Bitcoin and Ethereum with open source nature and smart contracts are the most prominent public Blockchains. Public Blockchains are mostly reliable if the users strictly abide by the rules and regulations of the Blockchain[86]. On the other hand, private Blockchain is an invitation-only network operated by a central authority, and a validation process would allow participants to confirm transactions in the Blockchain.

However, a group of BC developers debate that private Blockchains cannot be considered to be a Blockchain as the principle of monitoring, tracking, and restricting the number of participants in the private Blockchain contradicts the trustless and open nature of the Blockchain[118]. Private Blockchain differs from public Blockchain in many aspects. The validators in public Blockchain are unlimited and can not be trustworthy whereas a premeditated number of validators process transactions in the private Blockchain which results in higher throughput and ensure strong privacy of users' data on the private distributed ledger. If a transaction is submitted on a public Blockchain, the transaction is tamper-proof and can never be altered or modified while a committed transaction can be updated in a private Blockchain following consensus of a certain number of authorized participants.

To set up a network, public Blockchains require no infrastructure costs, while private Blockchains need wide-scale deployment and operational costs[119]. Rimba et al.[120] compared the computation and storage cost of a Blockchain process with traditional Cloud system. They run two instances of business process from two different kinds of infrastructure: Ethereum Blockchain and Amazon Simple Workflow Services (SWF) to estimate costs of their business process logic. Rimba et al.[120] reported that the cost of execution of the business process on Ethereum Blockchain could be two orders of magnitude greater than on Amazon SWF (Simple Workflow Service).

Another important Blockchain type is called consortium Blockchain, which is a semi-decentralized and governed by a group rather than a single entity. Variations of these kinds of Blockchain applied in the existing research articles are presented in Table 5.

Sidechain: The sidechain [121] refers to a separate Blockchain which operates in parallel to the main Blockchain and the sidechain is attached to the main chain by means of a two-way peg. The parent chain is called the original or main chain, and all additional chains are referred to as side chains. The two-way peg depicted in Figure 12 is a bidirectional transfer mechanism which enables users to move digital assets to the side chain from the main Blockchain and vice-versa. A user on the main chain requires to send a certain amount of digital coin to an outside address of a system called Federations. The Federation releases the equivalent coin on the sidechain after waiting for a certain time of the transaction committed. The user can access and spend the digital coin on the sidechain. The reverse occurs when switching back from a sidechain to the primary chain. A federation is an intermediary point for determining when to lock and unlock digital coins between the main chain and side chains. The federation adds an extra layer between the main chain and the sidechain. The developers of the sidechain might choose members of the federation. A sidechain with its own protocols and implementation can independently run and is completely isolated from the main chain. As a result, if the main chain is hacked or compromised, the sidechain can still operate likewise, the cyberattacks on the sidechain cannot affect the operation of the main chain.

The sequence diagram of communications between the Main chain, Federation and Sidechain is presented in Figure 13 where:

1. A user sends 5 maincoins to the federation that locks the coin for transferring it to the sidechain.
2. The entities of the federation sign the transaction after performing verification. If the certain number of entities approve the transaction, the 5 maincoins are transferred to a user providing address on the sidechain.
3. The user can play rock paper, scissor game with another user using 5 sidecoins and obtains 10 sidecoins if it wins otherwise each user gets 5 sidecoins in case the game is draw.

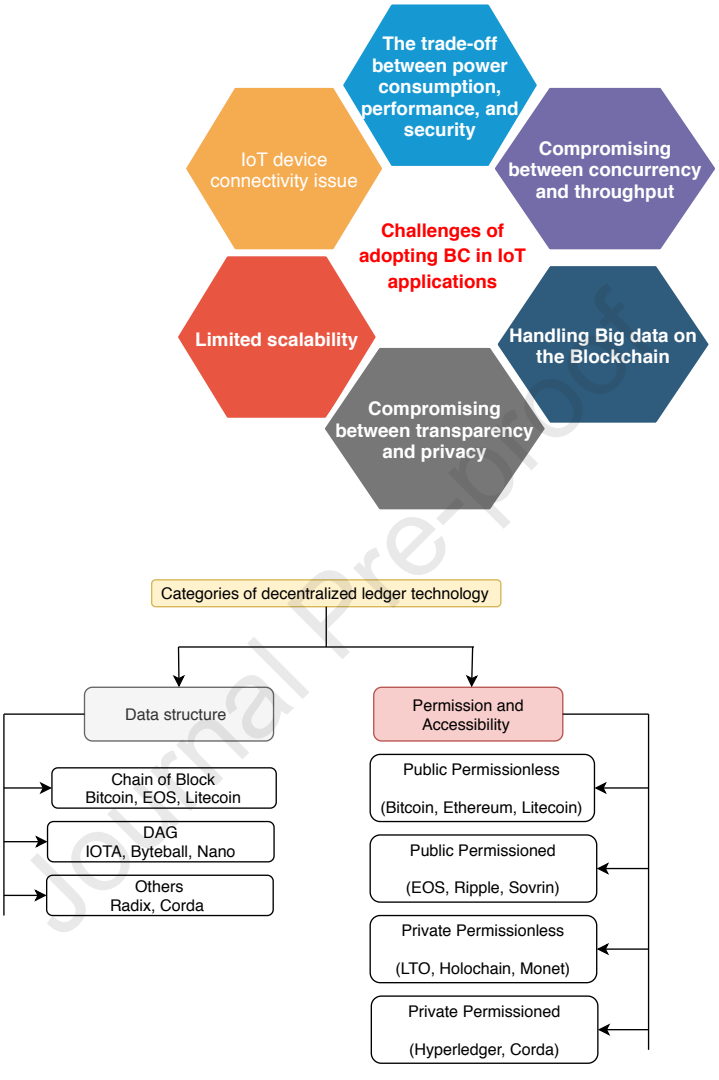


Figure 11: The types of decentralized ledger technology

4. The user sends back 5 sidecoins to the lockbox of the federation. The entities of the federation verify the transactions and transfer the coin back to the mainchain.

Table 5
The different types of BC in IoT literature

Acronym	Explication	Interpretation
PuB	Public Blockchain	Each of the transaction in a public Blockchain is open for the public to verify. Anyone can download BC protocols and read, write or participate in the network.
PrB	Private Blockchain	The private Blockchain allows only trusted parties to participate in the network to verify and validate transactions.
CoB	Consortium Blockchain	The consortium Blockchain is a semi-private which is controlled by a group of users across different organizations.
EEB	Enterprise Ethereum Blockchain	Ethereum is the second-largest enterprise open-source Blockchain which is used for general purposes. Ethereum facilitates smart contracts and Distributed Applications (DApps) to be built and run without the requirements of a third party, any fraud and downtime.
PrEB	Private Ethereum Blockchain	Ethereum Blockchain network describes a set of nodes connected to each other to create a network. Developers can build a private Ethereum network rather than the public network to make transactions and build smart contracts without the need for real Ether.
EHF	Enterprise Hyperledger Fabric	Hyperledger Fabric refers to an open-source, permissioned distributed ledger developed by the Linux Foundation-hosted Hyperledger consortium. The client application uses Hyperledger Fabric SDK or REST web service to interact with the Hyperledger Fabric network.
PuPB	Public Permissioned Blockchain	A Public-Permissioned Blockchain network is defined as a new kind of network that bridges the gap between the Public-Permissionless networks (such as Bitcoin or Ethereum) and the Private Consortium networks.
PrPB	Private Permissioned Blockchain	This Blockchain is permissioned and private, so only selected participants can join the network. (e.g., Hyperledger Fabric, R3's Corda).
CuB/ CPuB/ CPrB	Customized Blockchain/Customized Public Blockchain/Customized Private Blockchain	Developers or researchers use popular programming languages like C++, Java, Python, Go language to build their own private or public Blockchain for analyzing the performance of their applications.
EPB	Enterprise Permission Blockchain	This is industry level Blockchain such as Hyperledger Fabric where users require permission to participate in the network.
CB	Cloud Blockchain	Third-party Cloud such as AWS provides resources for building and operating Blockchain operations.

2.2.7. Performance metrics of Blockchain application

Nowadays, diverse kinds of Blockchain-based applications have emerged. Therefore, it is significant to evaluate the performance and success of BC for developing various use cases. Fan et al.[39] conducted a comprehensive survey on Blockchain performance assessment parameters, metrics, and tools. Fan et al. highlighted three tools presented

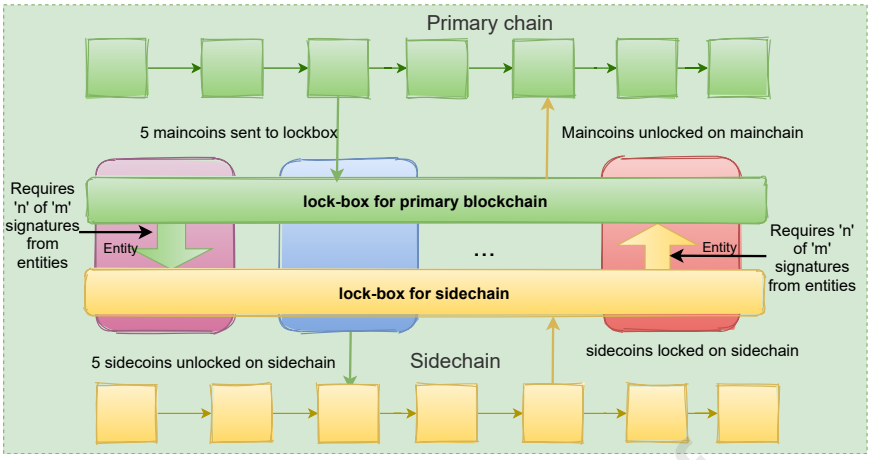


Figure 12: The Federated two-way peg communication

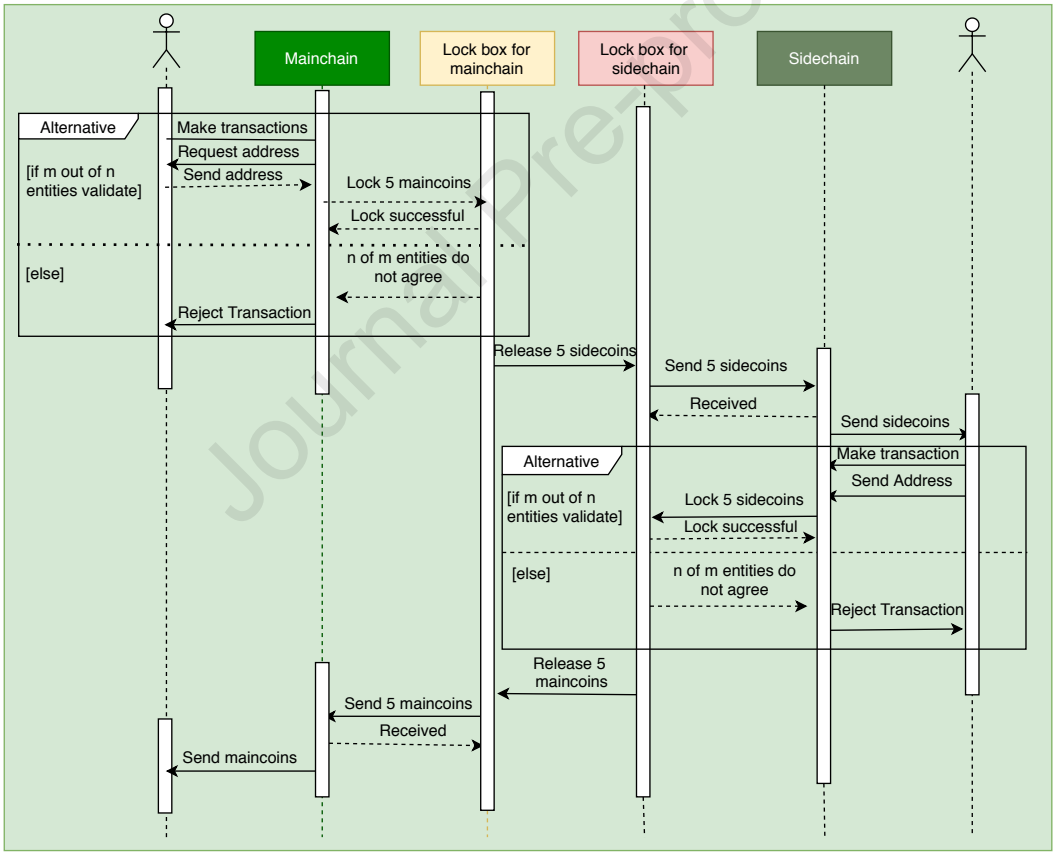


Figure 13: The sequence diagram of two-way peg communication

in Table 6: Blockbench, Hyperledger Caliper, and DAGbench for analyzing the performance of public and private BC applications under the category of BC benchmark tools and described two simulators: BlockSim and DAGSim. Studies[39, 122, 123, 124] presented a set of performance metrics and parameters for assessing DTL (Decentralized Transaction Ledger) and Blockchain leveraged IoT applications as shown in Figure 14.

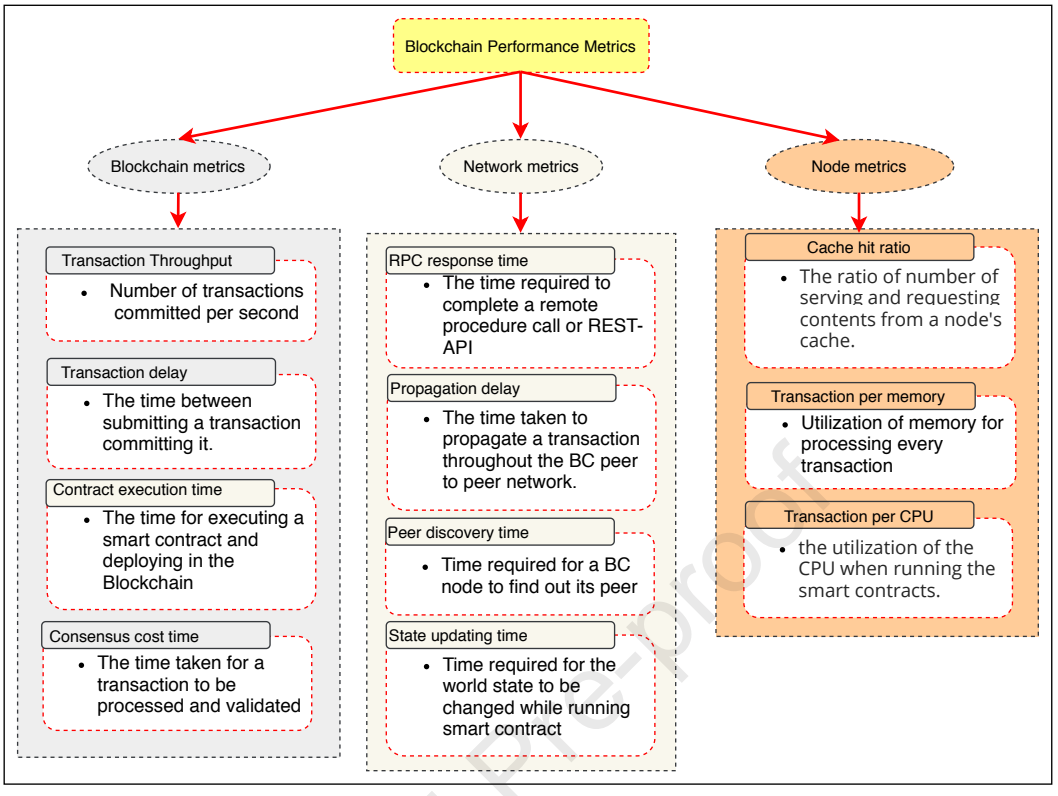


Figure 14: The metrics for evaluating BC leveraged applications

Table 6
Performance metrics for different BCs

Benchmark performance analysis		
Tools	Performance Metrics	Supported Blockchain
Blockbench[125]	throughput, latency, scalability and fault-tolerance.	Ethereum, Parity[126], HLF[127] and Quorum[128].
Hyperledger Caliper[129]	TPS (Transactions Per Second), transaction latency, resource utilization (CPU, RAM, network, and IO).	Hyperledger Fabric, Sawtooth[130], Iroha[131], Burrow[132] and Besu.
DAGbench[133]	throughput, latency, scalability, success indicator, resource consumption, transaction data size and transaction fee.	IOTA[134], Nano, Byteball[135]
Blockchain simulator		
BlockSim[136], BlockSIM[137]	Block creation rate, system stability and transaction throughput (TPS)	Any private Blockchain comparison with Bitcoin, Ethereum
DAGsim[138]	Transactions arrival rate	IOTA Tangle[139]

2.3. Objectives of Blockchain technology in IoT:

The advent of Blockchain technology has brought many benefits across a variety of industries in trustless environments[140]. In this section, several advantages and objectives of the Blockchain in IoT are shown in Figure 15 and described below.

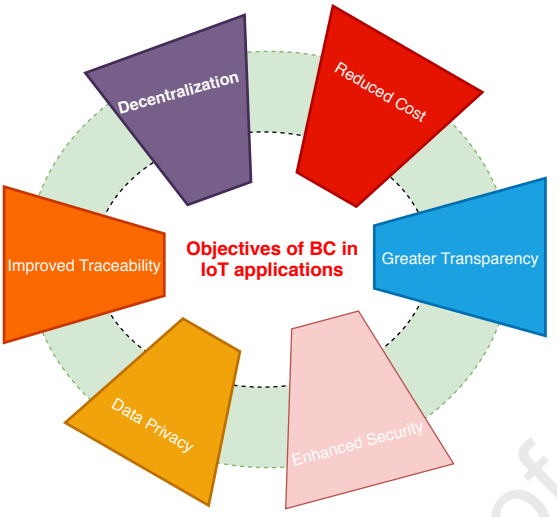


Figure 15: The objectives of BC

- **Decentralization:** Blockchain, with its decentralised nature, is a promising technique for effectively solving bottleneck and one-point failure problems by eliminating the need for a trusted third party in the IoT network[8]. The disruption of a Blockchain node does not affect the operation of the BCIoT network. Blockchain data is usually stored in multiple nodes on the peer-to-peer network, and the system is highly resistant to technological failures and malicious attacks. The availability or security of the network cannot be compromised even if some of the nodes go offline. On the other hand, many traditional databases rely on one or more servers and are more prone to cyber-attacks and technological failure. Furthermore, the peer-to-peer architecture of Blockchain empowers all network attendees with fair validation rights to check the correctness of IoT data and guarantee immutability.

- **Enhanced Security:** Blockchain is more reliable and secure than other record-keeping systems from several aspects[8]. Transactions must be agreed in advance of being documented by the network participants. A transaction is encrypted and linked to the previous transaction upon its approval. In addition to that, information is stored across a network of computers rather than on a single server, which stops hackers from compromising transaction data. In Blockchains, the main element of security is the utilization of PKI (private/ public key infrastructure). To secure transactions between participants, Blockchain systems use asymmetrical cryptography. These keys are generated with random numbers and strings so that an individual cannot mathematically formulate the private key from its public key. This protects Blockchain documents from future attacks, reduces data leakage problems and strengthens the security of a Blockchain network.

  Moreover, Blockchain has an ability to transform how confidential information is shared to prevent fraud and illegal activities in any sector where protecting sensitive data from different applications including financial services, government, and healthcare is important. Further, with Blockchain-enabled smart contracts[141], BCIoT can provide consumers with trusted access control, which automatically authorize all operations of IoT devices. In addition, smart contract services offer data provenance to users. This enables data owners to control the exchange of their data on Blockchain. Blockchain enables users to define access rules for self-executing smart contracts, which guarantees the privacy and ownership of personal data. Malicious access can be verified and disabled using smart contract-based authorisation.

- **Improved Traceability:** Goods traded in a complex supply chain using a traditional ledger cannot be traced back to their point of origin as quickly in other systems as in Blockchain. Historical data transactions in Blockchain can assist in checking the authenticity of assets and avoiding fraudulent activities. Similarly, the Blockchain can store and track the past records of a patient that are important for patient's care.

- **Greater Transparency:** The transaction histories in Blockchain are more transparent since these histories are available to all network users. Blockchain is a sort of distributed network in which all participants share the same documents as opposed to individual copies in the standard network. This shared document can be modified only by means of a consensus, meaning that everyone has to agree. In other words, the same copy of Blockchain data spreads over a wide network for public verification. Consequently, all Blockchain users have fair rights over the network to link, verify and track transaction activities. To alter a single transaction record, all subsequent records would need to be modified and colluding would be needed for the entire network. Consequently, data on a Blockchain is more accurate, robust and transparent than on the conventional network. Such transparency also leads to protecting the credibility of the Blockchain-based systems by reducing the possibility of unauthorised data alternations.

- **Data Privacy:** Thanks to Blockchain's immutable and trustworthy features, storage systems on the Blockchain are extremely efficient to protect IoT data from alteration[19]. Blockchain archives data transactions and events in an integrity-preserved, authenticity-guaranteed manner by means of immutable hash chains and digital signatures. Essentially, the Blockchain allows users to monitor transactions across the network so that computer and data rights are retained.

- **Reduced Cost:** Cost reduction is one of the main aims for many businesses. Blockchain does not require third parties or middleman and infrastructure's deployment cost for public BC to guarantee business operations, which can reduce the cost of operating business[142]. Blockchain users do not need to review too much paperwork to complete a transaction, as each party has access to a single, and unchangeable ledger. While BC can escape the cost of third-party services, Blockchain requires huge investment for dedicated infrastructure for private and consortium Blockchain and public BC still charges a certain fee for transaction processing (e.g. Gas in Ethereum BC).

- **Immutability:**Transaction data on the Blockchain remains immutable over time. Technically, transactions are timestamped after being checked by the Blockchain network and then inserted into a Block that is cryptographically protected by a hashing method. Hash mechanisms link Blocks together and constructs a sequential chain. One field of a new Block's header always holds the hash value of metadata of the previous Block, which makes the chain strongly immutable[143]. This way, the Block data cannot be updated, altered or removed after it is validated and recorded in the Blockchain. The cryptographic link between subsequent Blocks can withstand any attempts of transactions' alteration or modification. Even if any changes occur in a transaction, it will be easily identified.

2.4. Technical limitations of Blockchain

While Blockchain is increasingly committed to providing disrupting infrastructure for the Internet of Things, its implementation remains a series of critical challenges that need to be addressed in terms of scalability, computational cost, security and privacy[68].

- **Scalability limitations :**Current Blockchain platforms have some bottlenecks that result in poor scalability with restricted throughput, efficiency and high computational cost. Currently, due to constraints in Block size, many Blockchains have lengthy processing periods for transactions to be written into the chain of previously confirmed Blocks. Consequently, Block time increases rapidly, reducing the overall system performance. If all transactions are saved on the chain, the ledger over time will become extremely large[144]. Given complex IoT scenarios such as smart cities, eHealth, IoT data is enormous. Thus, the magnitude of IoT data would grow rapidly, making the processing of high volumes of data complicated in the Blockchain. Due to these limitations, many applications developers don't see Blockchain technology as an alternative solution to the existing systems for large IoT systems[145]

- **High computational cost:** Wood et al. [146] reported the cost of completing a transaction as the computational cost of a Blockchain. The processing of a transaction involves various steps, including defining heavy security, mining, validating, and storing it across multiple participants[147]. These steps combinedly consume considerable computing power. There are a variety of mining techniques such as PoW, PoS, pBFT described above that require various levels of energy. For instance, PoW, which is the most decentralized mining process, solves a

complicated mathematical puzzle that requires powerful computational hardware to perform transaction validation. Due to resource constraints of IoT systems, it is difficult for them to meet resource requirements of PoW for qualifying the most decentralized nature. Even for IoT devices with fairly large computational capabilities, the sophistication of the Blockchain system will demand heavy technical and human resources. This would trigger consumer's concerns about high running costs that would limit large scale implementation of Blockchain-based systems.

- **Security and privacy issue:** Although Blockchain can withstand major security attacks such as Sybil, DDoS, selfish mining and Ransomware attacks, the existing Blockchain has some inherent security flaws. If more than half of the machines running Blockchain can control computing resources, they can alter consensus processes and stop the confirmation of new transactions for malicious purposes. This is also referred to as a 51% attack in the Bitcoin philosophy. Without robust monitoring of transactions, Blockchain can be at risk of data loss and network disruption. In a Sybil attack, the malicious nodes create several identities to either flood the network with transactions or make false statements, such as fake traffic congestion[7, 10]. Distributed service denial (DDoS) attacks are difficult to conduct on a network of Blockchains. Still, Blockchain technology is susceptible to a message hijack, and DDoS attacks and these attacks are the most common on Blockchain networks[32]. DDoS attackers attempt to disrupt the network's mining process, e-wallets, crypto exchanges and other financial services. Selfish mining is a bitcoin mining strategy in which groups of miners collaborate to increase their earnings. A miner (or group of miners) tends to increase their revenue through selfish mining by strategically withholding and releasing Blocks into the network[36]. Although BCIoT can support safe data sharing, storing all genres of health data on a Blockchain causes a delay in committing transactions and risks data leakage and disclosure of patient's sensitive information.

2.5. Blockchain and Internet of Things(BCIoT)

The Internet of Things (IoT) links individuals, objects, and goods to provide opportunities for capturing data from embedding sophisticated processors, sensors, and actuators, each transmitting data to a centralized server, often Cloud servers. The IoT analytics tools exploit IoT data to turn them into ideas and practice to influence business processes and contribute to new services. However, security and privacy of the IoT ecosystem are significant concerns which have impeded its deployment on a broader scale. IoT network is often susceptible to security vulnerabilities including Distributed Denial of Service (DDoS), Ransomware and malicious attacks. DDoS refers to an attack where a target such as a central server is bombarded with many simultaneous data requests originated from several compromised computer systems, resulting in a denial of service for targeted network users. Further, as the number of devices joining in an IoT network increases, a bottleneck problem can occur in the existing centralised systems while authenticating, approving, and connecting new nodes within the network.

With the solutions of these IoT problems, Blockchain known as distributed transaction ledger (DTL) has emerged a breakthrough technology to potentially address some of the IoT security, privacy, and scalability problems. The distributed ledger in the Blockchain is a tamper-resistant, which removes the need to trust the participating parties. IoT covers a diverse range of applications, including smart cities, smart infrastructure, smart grids, smart transportation, smart home, and smart healthcare systems. Blockchain's deployment in the IoT domain has brought a new Blockchain domain in IoT called BCIoT. With BCIoT paradigm, no single organisation has control over the vast amount of data generated by IoT devices. Further, Blockchain technology enables participants to follow up on past transactions. Therefore, data leakage is rapidly detected and remedied. To ensure integrity has become the key research issue in IoT applications, as IoT source code is stored by internet third parties and telecommunications companies that result in lack of trust among consumers. The applicability of Blockchain in IoT network depends on several factors[148]:

1. Blockchain can resolve privacy and security issue if an IoT application needs a decentralized P2P ecosystem.
2. Blockchain could be a promising secured solution if IoT application requires to maintain payment process for its provided services without the control of third parties [149].
3. If IoT applications demand to preserve logs and traceability of sequential transactions, the Blockchain can be one of the most effective solutions.

Nonetheless, there are some key obstacles to be overcome when developing an architecture for IoT devices in conjunction with a Blockchain ledger.

1. One of the key challenges of integrating IoT with Blockchain is how the vast quantities of data produced by many IoT sensors can be handled in on-chain. Furthermore, the Blockchain suffers from potentially lower speeds or high latency when processing transactions.
2. Another key issue is to preserve network privacy and transaction confidentiality: the anonymity of transaction history cannot be granted on public Blockchain. Attackers can discover the identities of users or devices by analysing transaction pattern.

In the next section, we reviewed the literature, focusing on addressing the issue mentioned above with IoT and Blockchain.

2.6. Blockchain and Cloud of Things(BCCoT)

With the advancement in digital healthcare, a significant quantity of Electronic Medical Records (EMRs) is being generated and exchanged between health institutes and patients to facilitate data collection and provide QoS for the users. In particular, Cloud computing provides powerful health data exchange services, in which EHRs can be processed remotely on Cloud servers, while patients can access information on their mobile devices. The IoT integrated with Cloud computing promises to deliver treatment on-demand, save medical expenses and enhance the quality of experience.

However, information sharing in Cloud environments is susceptible to the risk of potentially malicious attacks and the lack of trust among Cloud vendors, Cloud-based storage, and users. This not only causes adversaries to the medical service and network degradation but also leads to severe data leakage issues. Blockchain technology with high immutable, stable, and trustworthy features can tackle the challenges raised while sharing health information in Cloud ecosystems[150]. Blockchain can secure data sharing across Cloud IoT enabled healthcare networks, in which Blockchain and Cloud are the key contributors to manage user access and data sharing. In particular, Blockchain's smart contracts can automate controlling and authentication of any entry in the Blockchain, ensuring security and protection for insecure healthcare settings. Blockchain paradigms promote cooperation between patients and healthcare organisations to ensure high data privacy and security. Integration of Blockchain into Cloud computing significantly increases security for storage services in Cloud eHealth. Cloud storage acts as peers in the P2P network under Blockchain administration. Many researchers suggest that health data can be encrypted and stored in the conventional Cloud storage whilst the hash code generated from metadata will be stored on the Blockchain, which allows traceability of data and quickly detects the risks of altering Cloud data. Blockchain can provide specialised, highly reliable, and productive health care services. Blockchain has the potential to transform clinical services, such as health monitoring, patient diagnosis or medical intervention assessment. Consequently, the use of Blockchain models in the health sector will transform healthcare delivery into better patient service and system security.

In addition, Blockchain can provide advanced security services for smart cities applications. Cloud computing offers powerful computational tools for managing massive data streams from all emerging IoT apps for people to deliver services in real-time. With its high-security features, Blockchain shows its high efficiency in managing smart city operations. The convergence of Blockchain and Cloud computing enables smart city architectures to tackle the issue of security and system performance. Blockchain platforms offer smart services such as home surveillance, home management, and device access control in smart home scenarios. In particular, Blockchain can be combined with distributed Cloud computing to make data storage and processing more scalable and efficient amongst IoT devices, homeowners, and external users.

Due to the restricted power and storage resources of IoT devices, vast amounts of data streamed from many devices creates a bottleneck for the current IoT systems, which results in low Quality of Service (QoS)[8]. The most common means of storing and processing data is a central database in many existing systems. The centralized repository suffers from several drawbacks:

1. Since a single server is meant to deal with all kinds of customers' queries, customers would not be able to access services during the period of failure[151].
2. There is a risk of violating the data owner's privacy because unencrypted data might be exposed to unauthorized individuals by the entity that administers the centralized storage medium[152].
3. The database can be changed from the server-side without the data owner having control or knowledge of the changes in the database [153, 7].

Meanwhile, Cloud computing has virtually unlimited storage and computational resources that can deliver on-demand, reliable, and secure IoT services. The integration of Cloud computing with IoT and BC opens up a new

paradigm named BCCoT, which will transfer applications' operation into a safe environment. Indeed, IoT frameworks greatly benefit from the abundance of resources available on the Cloud. At the same time, Cloud can be an additional prominence for real-life applications because of being merged with IoT ecosystems. Additionally, Cloud of Things can transform the current IoT system into a system with minimal managerial effort, high efficiency and quality of service. Cloud analytical tools can support a variety of IoT operations, including historical data processing, information storage and statistical analysis. Cloud data management is used to support end-users to improve IoT services and fulfil customer requirements. Various research identified several key features of Cloud computing, including on-demand support, high processing capacities, automatic management, ubiquitous communication and scalability to support multiple IoT applications. These properties of Cloud computing have motivated researchers to devise diverse kinds of frameworks that combine Blockchain, IoT and Cloud of Things technology.

2.7. Blockchain and Fog of Things(BCFoT)

Cloud computing alone finds it challenging to handle the flood of information with the proliferation of IoT devices and their constant interactions. Although the Cloud allows users' access to storage, processing and networking resources in cost-effective ways, these centralised services can cause delays and performance problems for IoT devices that are far from the Cloud data centre. Fog computing has emerged on the Internet of Everything (IoE) to reduce energy consumption for IoT devices and significantly increase the processing time of the client's services[154]. The term Edge computing and Fog computing are often synonymous, and both Edge and Fog computing have almost similar features. IoT devices in Fog computing are usually linked to Fog devices via wired or wireless media using Zigbee or LoRa protocol. Both the Edge and Fog computing systems bring facilitates of data processing closer to the data source, and data does not need to be sent to a remote Cloud or other centralised processing systems. Consequently, this technology can reduce the amount of data uploaded to the remote Cloud servers. This decreases the distance required for forwarding data and improves response time for the services, especially for a remote mission-critical application.

The Fog devices geographically spread across heterogeneous networks. Fog computing is a distributed platform that raises the challenges of guaranteeing privacy and security for the Fog devices and their affiliated IoT devices. Fog computing entails a mesh network in which all nodes have almost equal storage and network resource capacities. Fog devices require mutual trust and protection along with the facilities of distributed computing as Fog devices are owned and managed by diverse entities[116]. Therefore, a technology like Blockchain is required to maintain trust in a distributed Fog network where participants don't need to trust one another. Basically, Blockchains eliminate the need for an independent third party and can be undertaken in highly decentralised environments, where all parties including IoT devices, Edge/Fog and Cloud servers need a high degree of autonomy during operation[116].

The distributed feature of Blockchain technology has accelerated its adoption in Fog computing to introduce BCFoT paradigm. However, a full-featured Blockchain cannot be implemented on the Fog nodes due to their restricted storage and computing resources, wide distribution, heterogeneous network, and nodes' selfish behaviour[155]. Further, Not all BC consensus mechanisms are suitable in a Fog ecosystem due to their limited resources. For instance, Proof of Work (PoW) that solves a complex mathematical puzzle requiring massive computational capacity and power, is not appropriate for Fog miners[156]. However, several other protocols such as Proof of Stake (PoS), Practical Byzantine Fault Tolerance(pBFT) consensus are suggested for the Fog network.

2.8. SDN and Blockchain Technology

Software-Defined Networks (SDN) differ from traditional networks in several ways. For instance, unlike conventional networks, routing decisions in SDN are made remotely on a controller instead of on each router. SDN[157] isolates network control functions from the forwarding functions so that the network can be dynamic, structured, and programmatically configured to improve its performance and monitoring. Control functions may include the flow control to the switch/routers, routing decision of data packet, governing how router/switch that constitutes forwarding plane handles traffic. SDN manages and orchestrates physical networking tools, including switches, routers, etc., and transfers decision-making to a virtual network control plane. The SDN architecture depicted in Figure 16 comprises three planes: 1) Application, 2) Control and 3) Data plane. According to Figure 16, the upper layer is called an application plane that supports end-users with a range of services including mobility, routing, traffic management, network virtualization, and network security protocols developed by various third parties. The SDN application plane executes these services remotely and concurrently. The control plane resides in the middle layer of the SDN architecture that contains the SDN controller installed in the NOS (Network Operating System). The control plane realizes network policies, manages a global database of node placement, information regarding application requirements, and the data

flow path of the complete network. Also, the control plane can create virtual instances of the physical controller to meet the maximum number of requests in a limited time without sacrificing the QoS. The lower layer in Figure 16 is called a data plane that refers to the physical entities, including switches, routers, base station, and roadside units (RSU) etc. Network devices in this layer receive information from the SDN controller regarding where to transfer the data. Network administrators can use OpenFlow protocol to manage the actions of virtual and physical switches at the data plane.

- **Northbound Interface:** The application plane communicates with the SDN controller about what resources the applications need, and where to send data via a northbound interface which are often RESTful APIs. The control plane orchestrates available network resources and applies its intelligence to discover the optimal forwarding path for the application with respect to latency and security. The SDN controller can also automatically ensure that the traffic for an application is routed according to the network administrator's policies.
- **Southbound Interface:** The SDN controller uses the southbound interface to tell the network infrastructure such as routers and switches how these devices are moving application data. The routing tables that were stored on the devices in the traditional network no longer specify the data forwarding path. Instead, the SDN controller takes an optimized decision about the data path and instructs the router/switches to route data in compliance with the decision of the controller.

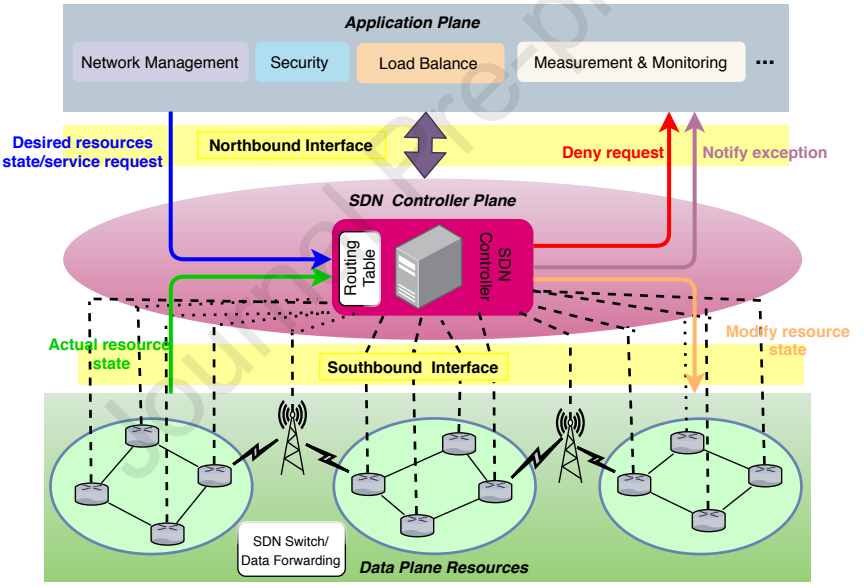


Figure 16: The SDN controller as a feedback node

The key concept behind the SDN technology is to separate the controlling functions from the network devices, and a centralized SDN controller manages network functions. This centralized SDN controller is vulnerable to various cyberattacks including DoS, and single point of failure attacks[158]. To tackle these issues with SDN technology, many recent studies suggest a decentralized SDN controller. However, a decentralized SDN controller raises some issues including the problem of maintaining state consistency among multiple SDN controllers, static flow control between the SDN controller and forwarding plane, which causes a non-uniform distribution of loads between the replicated SDN controllers[159]. Recently, researchers [159, 160] have sought Blockchain technology to integrate into decentralized SDN IoT framework to ensure uniform state among the instances of the SDN controller.

Figure 17 describes a modified IoT-SDN infrastructure inspired by Sharma et al. [159, 160]. The proposal incorporates an SDN controller for every infrastructure providers' network and maintains a multi-chain. The lightweight multi-chain enabled decentralized SDN-IoT architecture depicted in Figure 17 was suggested to address the issues of the current SDN based IoT architecture.

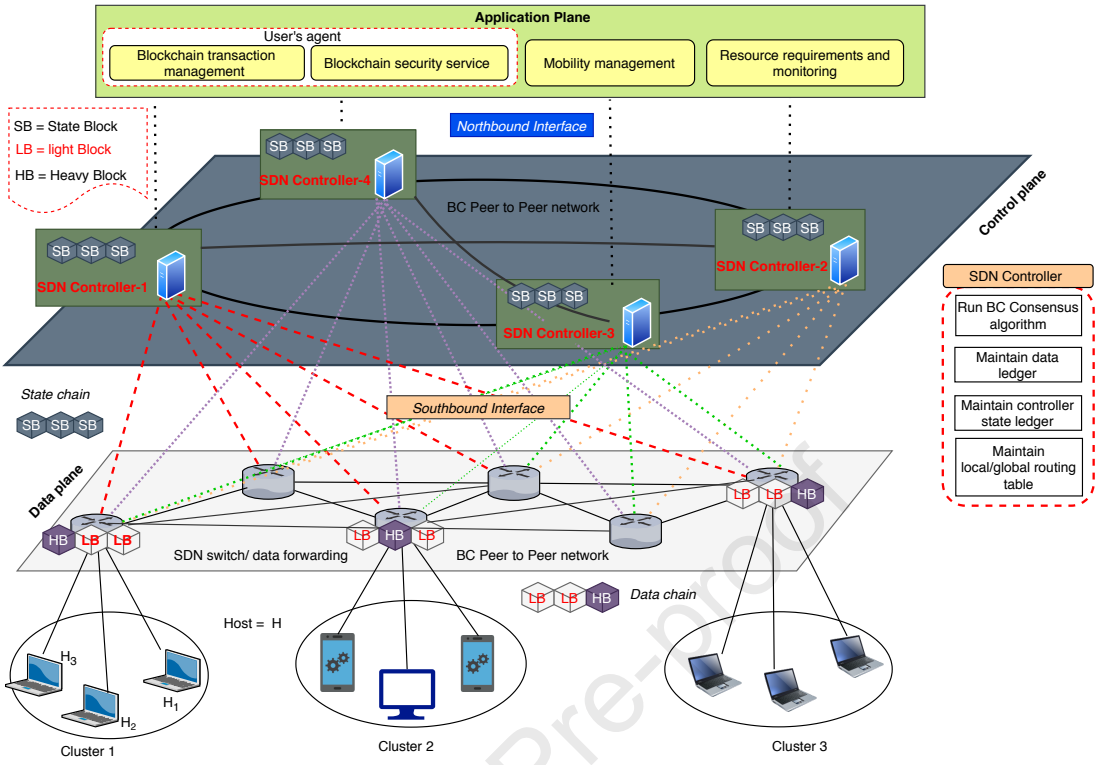


Figure 17: The BC enabled decentralized SDN architecture for IoT

Figure 17 shows that three clusters of host ($cluster_1$, $cluster_2$, $cluster_3$) contribute computing and storage resources for user's applications. The hosts are grouped, and each group is labelled as a cluster. A cluster of hosts is connected to a nearby SDN forwarding device such as router or switch. The data forwarding devices form a peer to peer network to facilitate Blockchain. In the control plane, multiple SDN controllers are installed where SDN controllers also form a peer to peer network to host a Blockchain. Each SDN controller has full control over the complete forwarding plane like a centralized SDN controller. However, unlike a centralized SDN controller, SDN controllers in Figure 17 replicated among multiple servers are connected using Blockchain technologies. Every server hosting SDN controllers executes consensus algorithm, stores distributed ledgers containing routing table for moving data from one host to another host.

The ledger that SDN controllers contain is called state ledger that saves SDN controller operations related information on BC in a linked list fashion after a specific time interval. As a result, the operation of an SDN controller can be resumed while it is down due to cyberattacks. Further, state ledger ensures the same state and integrity amongst the SDN controller's replication.

The other kind of ledger called a Data ledger is maintained by forwarding devices to store the data generated by their affiliated hosts. A Data ledger contains two kinds of Block: Heavy Block (HB), and Light Block (LB). HB includes data and the hash value of the data, whereas LB contains only the pointer/hash value of the Data. A forwarding device holds the LB for the data produced from its associated clusters and LB for other clusters. This process can provide users with better security than that of the approach to store all data Blocks in a centralized server and hash value/pointer of data Block on the chain.

3. BC State-of-the-art applications in IoT field

Blockchain and IoT, Blockchain and Healthcare, Blockchain and Fog computing, Blockchain and Cloud computing, Blockchain and Agent etc., are the keywords that were used to scan literature in this paper. The literature was downloaded from reputed databases and publishers, including IEEE Xplore,Sciencedirect, Elsevier, ACM, Springer, MDP, SAGE etc.

Figure 18 depicts the flow diagram of the literature reviewed in this article. In Figure 19, we presented statistics

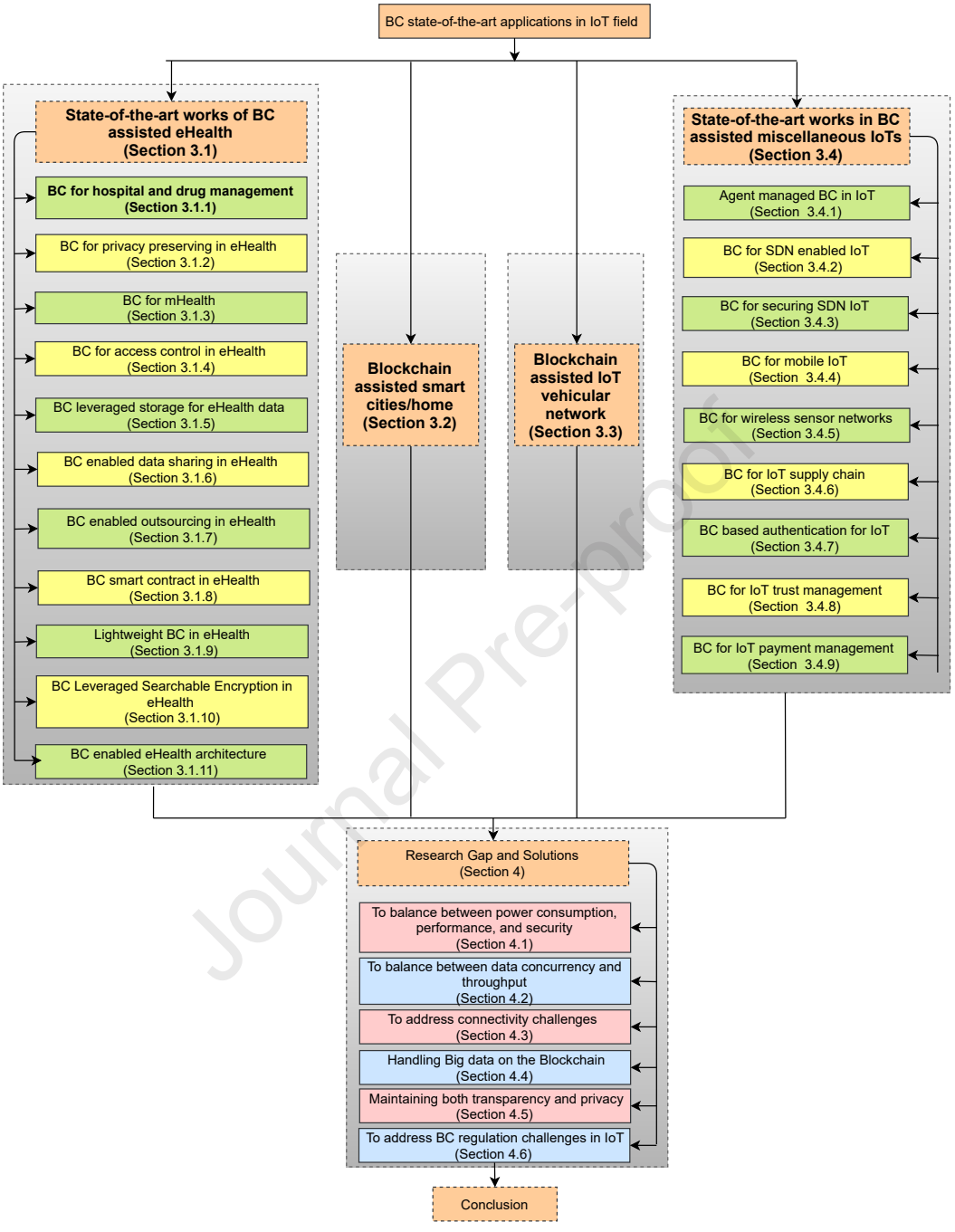
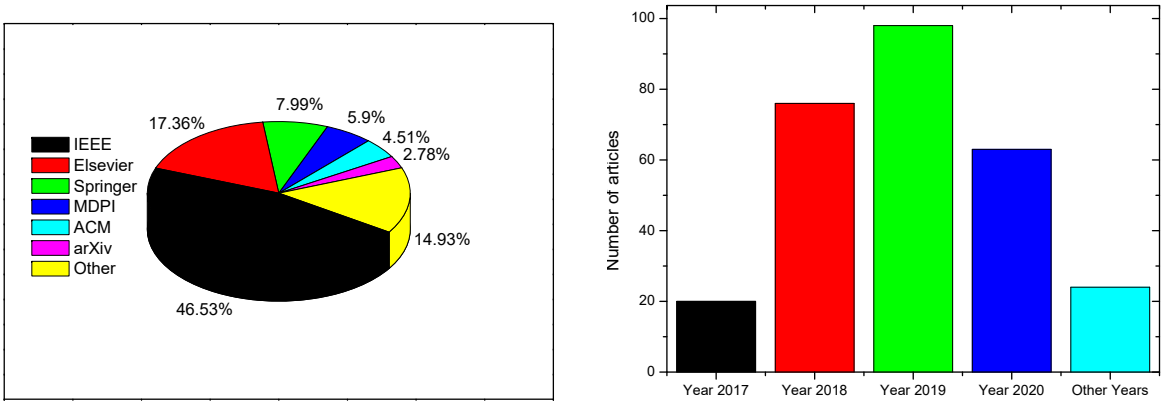


Figure 18: The flow diagram of the reviewed literature

of the papers reviewed throughout the article. The graph depicted in Figure 19(a) shows that the largest percentages of research papers have been retrieved from IEEE Xplore, while the second-highest percentages of publications have been collected from various Journals of Elsevier publisher.

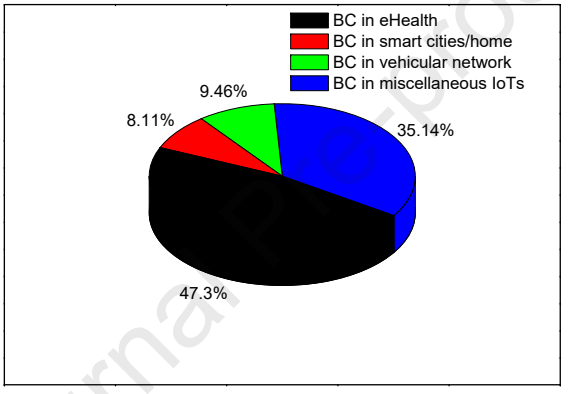
The graph in Figure 19(b) displays literature with respect to their publication year. We aimed to include the recent existing works on Blockchain and IoT, which are reflected in the chart. The majority of studies included in the paper were published in 2019. The statistics of reviewed articles according to applied fields and the BC roles in various



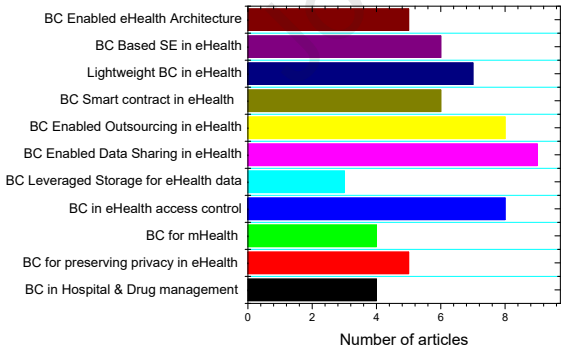
(a) The statistics of IoT literature with respect to publisher

(b) The statistics of IoT literature with respect to years

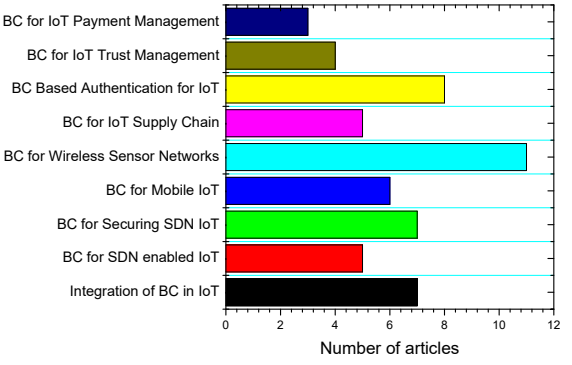
Figure 19: The statistics of state-of-the-art works in BC for IoT



(a) The statistics of BC's role in different IoT applications



(b) The statistics of BC's role in eHealth



(c) The statistics of BC's role in miscellaneous IoT applications

Figure 20: The statistics of reviewed articles according to the role of BC

IoT applications were shown in Figure 20(a), (b), and (c) where the majority of articles are from BC eHealth and the second-highest numbers of articles cover miscellaneous IoT applications. The chart depicted in Figure 20(b)(c) shows the breakdown of BC's role in eHealth and miscellaneous IoT applications, respectively. The articles from each major section are synthesized in different tables. The acronym used in summarizing different IoT studies are presented in Table 5 and 7 respectively.

Table 7
The acronym and interpretations

Acronym	Explication	Interpretation
SCM	Standard Consensus Mechanism	Common consensus algorithms that are frequently exploited in Blockchain include Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA), Practical Byzantine Fault Tolerance (pBFT), and Proof-of-Importance (PoI) etc.
CCM	Customized Consensus Mechanism	Customized consensus mechanism are variations of the standard consensus protocol. The researchers or developers modify the standard consensus protocol to optimize power consumption and increase Blockchain throughput
ECM	Enterprise Consensus Mechanism	The consensus mechanism adopted by the enterprise Blockchain communities such as Hyperledger Fabric, Ethereum
SC	Smart Contract	Smart contracts refer to lines of terms and conditions coded by computer language. Smart contracts are stored on a Blockchain and automatically execute if specified terms and conditions are met.
OfC	Off-Chain	The transactions that are not recorded on the Blockchain and typically stored into centralised databases like banks or other financial intermediaries are referred to as OffChain transactions. IoT data are not usually documented on the distributed ledger rather on traditional databases such as CouchDB, StateDB etc.
OnC	On-Chain	The transactions processed and stored on the distributed ledger in the Blockchain network is called On-Chain. Generally, the pointer or a hash value of the IoT data, financial transactions are recorded on the Blockchain.

3.1. State-of-the-art works of BC assisted IoT eHealth

In this section, we review state-of-the-art works that are related to eHealth frameworks. eHealth offers hospital services, and other medical benefits to enable people to rapidly access their health services. The adoption of the Blockchain paradigm in eHealth can effectively address critical issues of security and privacy, and increase service efficacy to promote patient care and gradual transformation of existing health systems into decentralized eHealth [161] [162, 163, 164]. Researchers aim at designing eHealth architecture using IoT, Fog, Cloud, and Blockchain for securely sharing data, managing data storage and network.

Blockchain leveraged healthcare can reform and promote interoperability, authorized access to patient medical records, secure tracking of prescriptions, hospitals assets, and wearable sensors during their entire life cycle. The clinician very often requires access to a patient's past disease histories that were created while the patient visited different physicians from different hospitals and clinics. In most current eHealth settings, patients do not have access to EMRs of the healthcare providers. However, a patient having access to his past history could avoid the duplication of medical records, and unnecessary medical tests. The Blockchain can dramatically impact the efficiency in healthcare delivery and costs by providing the patient with full control over his or her past medical records including reports, financial documents, laboratory test results, imaging studies of x-rays, CAT scans, and vital sign measurements. The health data in remote patient monitoring settings is rapidly expanding with other health data, which faces various challenges, including data access, and how data can be accessed outside healthcare facilities. Blockchain provides patients with the ability to boost the authorization and integrity of patient data. We organized relevant literature according to the role and purposes of BC in IoT eHealth below.

3.1.1. BC for hospital and drug management

Jamil et al.[81] developed a Blockchain-based vital sign monitoring platform for hospital facilities. The patients equipped with wearable sensors in the hospital transmit vital signs to the authorized nodes on the BC networks. The architecture was advanced based on a Cloud-driven model with the development of Cloud front-end technologies using HTML5 and JavaScript, to enhance the management of resources within the proposed framework. The BC provided product-centred services using the Representational State Transfer Application Programming Interfaces (REST API), which are either triggered by IoT devices or a web client. A smart contract supported controlled access to the BC ledger to ensure that patient vital sign information is confidential and consistent with data and hosted BC ledger functions across the proposed network. Further, the access control policy was implemented to allow system participants and users to access authorized content and transactions so that only authorized practitioners may access and manipulate the IoT device. The nodes on the BC P2P network installed a couch database to hold the vital sign transactions. A benchmark tool known as Hyperledger Caliper[165] was utilized to evaluate the system's performance in terms of several metrics, including Transaction Read Latency (TRL), Transaction Read Throughput (TRT), Transaction Latency (TL), and Read Throughput (RT). Celesti et al. [166] also proposed an eHealth system that connected the Clouds of a federated hospital using an Ethereum Blockchain to build a telemedical laboratory. Although the authors described the healthcare workflow for the proposed system, extensive performance analysis has not been carried out to demonstrate the feasibility of the system.

Malpractice within healthcare such as compelling patients to perform tests and purchases medicines from physician's preferred clinics or hospitals arises in many countries from a lack of adequate national policies and regulations[167]. Healthcare professionals often manage patient's health data, and medical tests are under their oversight and control where patients are not allowed to access those documents. Consequently, patients need to perform the same test twice when they switch to different physicians. To tackle these issues raised in the traditional healthcare system, Rathee et al.[167] proposed a Blockchain-based hybrid system for processing multimedia produced from IoT healthcare. The Blockchain network applied in the framework consists of two types of nodes such as authenticating nodes or miner nodes and executing nodes. The role of the executing node is to scrutinize whether the transactions that miners accumulate in the Block is legitimate or not. The proposed scheme was simulated using NS2 to analysis its security strength.

BC has an enormous potential to secure pharmaceutical supply chains. BC can provide an integrated solution for avoiding counterfeited drugs by making the entire drug distribution network traceable to all stakeholders at any point in the supply chain. Haq et al.[168] adopted BC in a drug delivery system to prevent counterfeit drugs. In this system, every transaction generated from drug production to distribution was recorded in a permissioned BC where only trusted authorities could join. As a result, the system can guarantee transparency and facilitates traceability while trading drugs.

Nguyen et al. [169] presented a conceptual, clinical assessment and control framework by integrating Blockchain, Cloud and IoT. They combined the data management system with a data-sharing platform using a decentralized mobile Blockchain network. Data integrity and privacy are ensured using a smart access based authentication approach on the access control layer. However, scalability and communication cost issue of the Blockchain were not investigated.

There has been tremendous interest among researchers to apply Blockchain technologies to provide secure and stable data storage for healthcare. However, only a few countries, including Estonia, Peru, have already adopted Blockchain health management in practice. In Peru, a Blockchain-based private health purchase management system[87] was recently introduced. The Blockchain was implemented in the Amazon Cloud to control the medical supply chain, ensuring secure communication between the sale managers, manufacturers and clients. Smart contracts are developed for storing medical sensor data to prevent data from malicious alternations or modifications. The drawback of the proposed scheme is that data confidentiality has not been addressed. Kang et al. [170] highlighted the effectiveness of the Blockchain paradigm in providing health services through IoT and Cloud of Things. However, performance assessments for the proposed scheme has not been carried out.

3.1.2. BC for privacy preserving in eHealth

Preserving privacy in eHealth system can make contact efficient between physician and patient, which is crucial for quality treatment, improved autonomy and tackling economic damage, embarrassment and discrimination[171].

Researchers[88, 89, 90, 172] designed BC-based IoT eHealth to ensure patients and healthcare providers privacy. The work in[88] is a privacy-preserving health data exchange approach that integrated IoT network and Cloud storage. The conceptual model comprises three layers: 1) data collection, 2) data storage and 3) data exchange layer. Electronic

medical records (EMRs) are securely stored in the Cloud layer using smart contract technology, while the indexing of the records is maintained in the Blockchain to secure medical records. Consequently, EMRs cannot be inappropriately changed or manipulated. However, a real prototype of the framework is yet to be implemented.

In [89], BC was undertaken to build a privacy-preserved Cloud health data platform. Smart contract regulated encrypted health records are stored on the Cloud BC ledger. The vulnerabilities to data confidentiality are effectively tackled by encrypting data before inserting into the Blockchain, which improves transparency and security of Cloud data storage. The limitation of the work is that comparisons have not been made between smart contract-based schemes and traditional schemes, and the model was not implemented to analyze performances.

Similar work in[90] advanced a stable Cloud-based Blockchain EHR platform with four entities: 1) a key generation centre, 2) healthcare professionals, 3) Cloud patients, and 4) data customers such as insurance firms. The time-stamped medical data is stored in the Blockchain, which increases the validity and traceability of health records. The weakness of the article is that a smart contract for managing data storage has not been implemented. The BC ledger is transparent to all the entities on the BC peer to peer network. Miners verify the contents of the Block before writing it in the distributed BC ledger. This openness of BC is a major threat to the privacy of patients in the eHealth system. To fix this issue, Rahulamathavan et al.[172] restructured the BC peer-to-peer network to adapt the techniques for Attribute-Based Encryption (ABE). The authors classified BC nodes as cluster head, attribute authorities, and miners based on their roles in the BC network. The cluster head of the BC network is connected to IoT devices for collecting IoT data. The cluster head performs computationally intensive operations, including processing and encryption/decryption for the data while Attribute Authorities(AA) is responsible for providing doctor, nurse and other healthcare professionals acting as miners with the attributes required to decrypt data. The selected miners can decrypt the Blocks using attributes obtained from AA for verifying and validating Blocks.

3.1.3. BC for mHealth

Mobile devices have enabled healthcare providers to improve patients' engagement and participation in treatment processes using mobile-assisted secure text messaging, patient apps, and telemedicine. In the existing settings, secure messaging between patients and healthcare professionals remain the primary use of mobile devices in IoT healthcare. However, BC related works[173, 82, 174, 175] had incorporated mobile apps to safely capture health data from a patient's wearable sensors and deliver rapid health services to patients.

Liang et al. [173] advanced a Blockchain-enabled mobile Cloud network where data streaming from wearable sensors are transmitted to Cloud servers via smartphone. The authors aimed to develop a patient-centric platform to share health data between healthcare providers and insurance farms. The system included six groups of users, including consumers, wearable devices, healthcare providers, insurance companies, the Cloud ecosystem and the Blockchain network. Hyperledger Fabrics, which is an enterprise permissioned Blockchain, was utilized to validate and preserve the patient's data while sharing the data with different stakeholders. Blockchain was deployed in the Cloud to serve three purposes:

1. To ensure the integrity of data entry.
2. To process requests from external sources to gain data access.
3. To implement access control for user verification.

The Cloud server is configured to connect to the participants on the peer-to-peer distributed Blockchain network using a Hyperledger Fabric client that protects the anonymity of the Cloud user's requests. However, they overlooked security issues such as malicious attacks on IoT devices.

Meanwhile, Nguyen et al. [82] projected a mobile Cloud Blockchain network that was designed to integrate various EHR systems to share health data between health care providers and patients. The Blockchain was embedded in a Cloud server where smart contracts handle user transactions for data access. In the Cloud, decentralised storage system(IPFS) made data sharing more effective as opposed to centralised distributed systems in terms of low latency and privacy. The system has enabled IoT users such as doctors or patients, to securely exchange data using their portable devices, including smartphones,and laptops. A private Ethereum Blockchain network implemented on the Amazon Cloud was used to analyze the performance of the proposed scheme. Ni et al.[174] figured out HealChain, which is a mobile healthcare system that comprised of three layers such as data collection, verification and storage layer. The research limits the number of Blockchain participants to keep mining cost moderate. Further, they developed an optimal decision-making process to maximize the economic benefit of carrying out mining tasks. However, the authors did not describe which kinds of simulation tools or programming language was used to conduct performance analysis.

Ichikawa et al. [175] presented a Blockchain leveraged mHealth framework to safeguard health data from tampering. They developed a mobile App using JavaScript Object Notation format to collect data from wearable sensors and store those in a private Blockchain of Hyperledger Fabrics. The authors examined the successful inclusion of health data in the fault networks. However, security issues between sensors, mobile App have not been addressed.

3.1.4. BC leveraged access control in eHealth

The security of eHealth systems is a vital issue because a security breach can endanger a patient's privacy, health, or even his or her life by maliciously altering diagnostic data[176]. As one of the key security features, access control ensures that only authorised users with correct privileges can access health services. Access control refers to a user, group, or organization's rights to access health information within the domain. Naturally, health systems need to implement fine-grained access control[177]. For instance, only previously registered healthcare providers should be given access to an Electrocardiograph (EKG) in a real-time monitoring service. Several approaches[143, 83, 178, 179] have been proposed in the Blockchain eHealth system to solve problems pertaining to authentication and access control.

Focusing on these issues, Tanwar et al. [143] suggested a Blockchain ledger to store access policies of the medical record. The authors designed several algorithms that defined access policies for healthcare providers on their patient-centric healthcare framework. They analyzed the performance of the system in terms of throughput and latency using different tools, including Hyperledger Fabric, Composer, Docker Container, Hyperledger Caliper, and the Wireshark capture engine.

Wang et al. [83] targeted a data-sharing system with fine-grained access control to better protect the privacy and accessibility of health data. Wang et al.[83] designed a decentralised Cloud architecture that incorporated an interplanetary file system (IPFS) for making decentralised storage, an Ethereum Blockchain and an ABE(Attribute-Based Encryption) platform. In this work, a smart contract-based access control management system has also been suggested to conduct keyword searches in the decentralised Cloud storage, which enhances the QoS(Quality of Services) and privacy of the framework. However, the drawbacks of the research is that data security and the delay arising from ABE and access control approach were not analyzed. Wang et al.[180] also sought the Blockchain Cloud infrastructure to store medical data using a Blockchain-enabled the authentication approach of medical data transactions. Any modification to the Cloud records is detected through the Blockchain's P2P network. In fact, this model eliminates the costs of managing data storage by third parties. However, Blockchain prototype has not been implemented in the article.

Islam et al. in [178] presented a framework to assist health prescriptions (HPA) so that patients receive recommendations from physicians. The system provides IoT devices with a security access token (SAT) upon successful authentication, which defines the privileges of medical IoT devices and their services or resources for the user. The IoT devices include the encrypted SAT while asking services from the system. The proposal also includes an access control mechanism based on OpenID to prevent unauthorized access to medical devices. However, the model is conceptual, and no performance analysis was carried out.

Ramani et al. [179] presented a medical data accessibility approach on the Blockchain. The system allows healthcare professions to append and retrieve health data with the consent of a patient. A private Blockchain was considered to analyze security. However, the authors did not evaluate the performance of the proposed technique using any simulator or by building a prototype.

GDPR health regulations[181] outlined privacy laws across Europe to protect user's control and confidentiality on his or her health data. According to the regulations, a service provider must incorporate facilities of the user's consent and the withdrawal of that consents in their system. The service provider must generate a report at the request of the user on how the user's data is being processed and used. Further, the service provider must also provide the customer with all the data in a format that is readable on the computer. The research in [182] presented a conceptual eHealth framework by augmenting Blockchain technology and Cloud to share health data with authorized users in an efficient, transparent manner and maintaining compliance with data regulations such as GDPR. The authors inspected the quality of health data using a machine learning technique to ensure the QoS of the shared data. The limitation of the paper is that performance analysis has not been done.

3.1.5. BC leveraged storage for eHealth data

Medical data is typically processed and stored in Cloud servers under the administration of different Cloud Service Providers (CSP) in traditional Cloud IoT-enabled healthcare systems. CSP should be transparent but vigilant about the risk of leaking out sensitive patient information. EHRs(Electronic Health Records) are also susceptible to various forms

of data-storage attacks while using Cloud security tools. BC can be an automated technological solution to make the current storage method for health data more secure and effective. BC can preserve the integrity of data while ensuring it remains tamper-proof. One way to store records with a Blockchain is on-chain storage. But, BC demands high cost to insert a Block on-chain[183]. On-chain storage is considered neither financially nor technologically feasible. However, another data storage method called off-chain can be implemented on the BC network. In an off-chain method, the hash code of a piece of data, which is relatively small, is stored in the BC ledger and the data is stored in traditional repositories. The storage cost in the on-chain method is low because the size of the hash value is relatively small[184]. Most research presented in Table 8, and 9 has addressed the storage cost issue on the BC network by following the off-chain database approach. Zheng et al. [182] outlined a conceptual model for continuously sharing personal health data using Blockchain-based decentralised Cloud storage. Health datasets are usually encrypted and stored off-chain in conventional Cloud storage, whereas only hash values of the data are inserted into the Blockchain to reduce the storage burden in the Blockchain framework. However, a prototype of the framework is yet to be developed.

3.1.6. BC enabled data sharing in eHealth

The protection of patient's privacy is a significant issue due to the sensitive nature of medical data while exchanging EHRs. BC has appeared as a potential solution to this issue because of its decentralisation and manipulation resistance characteristics[185]. In [85], Xia et al. schemed a medical data sharing model called MeDShare which utilized Blockchain for exchanging data amongst untrusted Cloud Service Providers (CSP). The researchers devised an access management architecture that exploited smart contracts to track access behaviours of data users and detect data breaches. The Blockchain-based CSPs could enable auditing and ensure healthcare professionals' provenance without compromising the confidentiality of data. However, concerns associated with access control of confidential data are needed to be efficiently resolved in the Cloud-based data processing. To address this issue, the research in [186] included a secure cryptographic approach for ensuring efficient access control and user's authentication for transferring data in the Cloud layer.

Physicians are normally specialized in delivering medication and care for a specific illness. However, treatment for many diseases needs cross-border medical knowledge from different medical practitioners worldwide. The BC platform can facilitate the exchange of healthcare professional's expertise for more precise medical care, personal diagnosis, and treatment. Wang et al. [83] suggested a hybrid healthcare system to combine knowledge from three fields: 1) artificial intelligence, 2) computational experiments, and 3) parallel execution (ACP) to expedite more precision medical care and treatment. Firstly, an artificial healthcare system (AHS), known as "descriptive intelligence" was developed to simulate and model the static and dynamic characteristics of patients and doctors. Secondly, computational experiments were used to integrate different types of disease scenarios to assess and evaluate the applicability of specific therapeutic regimens in AHS. The phase is called "intelligence predictive". Thirdly, the final regimen was chosen from a list recommended by experts and was carried out in parallel, both in the AHS and the current health care system, to provide "prescriptive intelligence". The system deployed a consortium Blockchain that involves patients, hospitals, health officials, healthcare institutions, medical researchers, and Blockchain-powered smart contracts to allow electronic health records (EHRs) to be exchanged, checked and audited.

Blockchain-based health data management is a transparent and open framework to support better healthcare services. Indeed, the combination of Cloud, IoT, and Blockchain can offer great advancements in smart medical services[187]. In [91], a decentralised Blockchain data security scheme was designed by Dwivedi et al. The infrastructure comprises five components: 1) overlay network, 2) Cloud servers, 3) healthcare providers, 4) smart contracts and 5) patients. In the work, Blockchain was linked to Cloud storage using a P2P network where each Cloud storage holds medical records in the form of Blocks and these Blocks' hash values are stored in the Blockchain which facilitates the tracking of any changes in the Cloud data. A dual encryption scheme is also proposed to safeguard data from potential attacks. The weakness of the article is that actual simulations have not been rendered on the suggested security scheme.

Nguyen et al. [82] advanced a novel EHRs sharing architecture based on Blockchain and shared interplanetary file system storage (IPFS). To enhance the security of EHRs during their exchange, smart contracts was designed to build a trustworthy access control mechanism. In addition, a data exchange protocol was developed to handle user access to the EHRs network. The usability tests were conducted on a mobile Android application, and Amazon Web Services provided Cloud. Results of the assessment indicate that the suggested approach is feasible on different e-health scenarios.

Shen et al.[188] proposed Medchain that is a platform for sharing medical record. The authors leveraged two separate decentralized networks: a BC P2P network and a normal P2P network. The Blockchain network stores data,

session, and operation fingerprints, such as immutable data digests, while the normal P2P network stores data and session descriptions, which are mutable. A session for packaging and removal of the mutable information is introduced in the data sharing process, which can reduce overhead storage considerably.

Fan et al.[189] designated a Blockchain-based medical sharing system where the provincial hospitals collect medical summaries from EMRs of the regional hospitals and community centres. The provincial hospitals pack medical data into Block after processing and then transmit the Block to the consensus nodes. Hospitals acting as both orders and endorsers play the role of initiating queries, verifying, and validating Blocks. A hospital can elect to maintain health data in their ledger locally or submit it to the Blockchain.

3.1.7. BC enabled outsourcing in eHealth

In recent years, outsourcing health services to a Cloud service provider has become significant to reduce the local computation burden[190]. Outsourcing is described as the act of shifting an organization's internal activities or services and decision-making to external suppliers following long-term contracts or agreements[191]. However, outsourcing tasks to a Cloud computing provider bring a few other challenges. The Cloud service provider might be curious about a user's sensitive data and breach the client's privacy. Also, the client needs to make contracts with the service provider so that the data privacy cannot be breached[192]. Research [93, 94, 193] has investigated Blockchain as a promising solution to the service outsourcing challenges such as security, privacy, payment and contract.

Cao et al.[93, 94] presented a Cloud assisted eHealth framework using Blockchain to secure outsourcing EHRs among medical users. An Ethereum Blockchain framework has been utilized for handling user transactions without the need of a trusted entity. The integrity and reliability of EHRs generated by patients and clinicians during the treatment process were guaranteed by inserting medical data into the tamper-proof Ethereum Blockchain in the form of transactions. However, a smart contract for managing service has not been investigated.

Park et al.[94] envisioned Cloud-based crowdsourcing to develop a medical remediation and evaluation framework called CORUS. Crowdsourcing refers to a process of collecting works, information, or views/opinions from a wide number of people who send their data via the internet, social media, and mobile applications. People interested in crowdsourcing often work as paid freelancers while others can voluntarily perform tasks[194].

Crowdsourcing on the traditional platform is exposed to several shortcomings such as a single point of failure, controller's silent misbehaviour, a conflict of opinions between the task requesters and the workers[193]. Blockchain, a revolutionary decentralised model, can be adapted not only to remove the limitations of the conventional crowdsourcing schemes but also to usher technological advancements including decentralisation and transparency[193, 195]. The decentralized ledger in the Blockchain technology increases the reliability of recorded documents and the efficiency of the proposed crowdsourcing system[94]. Additionally, Park et al. [94] applied Blockchain to attract large numbers of participants by offering an incentive for providing reliable information. The shortcoming of the article is that the performance analysis of the Cloud Blockchain has not been investigated.

3.1.8. BC smart contract in eHealth

With the emergence of Blockchain, smart contracts have become one of the most sought-after technologies because of their automated nature[196]. A smart contract refers to an agreement and rules encoded by computer programming. Smart contract stored in the public ledger is automatically running on the Blockchain without the need of the third party when the contract associated event is triggered[196].

Daraghmi et al.[95] developed a timed smart contract-based medical record access and permission management architecture. The contracts introduced in the research control transactions and monitor computations on the EMRs through implementing appropriate user's policies. The author suggested an incentive-based mining process to eliminate the need for digital currency. In this mining process, the next Block would be created by the node with the low rating and the nodes with higher rating participate in approving the Blocks on the Blockchain network. This ensures consistency between suppliers and ensures the system's sustainability. The experiment was carried out on Ethereum which is an open-source platform to feature the smart contracts using the Solidity language. However, the security and privacy was not addressed and accessing continuous health data onto the Blockchain was not done.

Kazmi et al. [100] developed a Blockchain-based remote patient monitoring system where smart contracts were made to enrol patients and healthcare professionals, to provide licence for the wearable sensors and other medical services. The system can generate an emergency alert in real-time, thus promote the consumer and healthcare professional's engagement in remote patient monitoring. The smart contracts for the proposed scheme were written on the Ethereum platform. The Remix which is an open-source web environment was utilized to test, debug and deploy their

smart contracts. However, the security and privacy issues while retrieving data from wearable sensors were ignored.

Hang et al. [92] proposed a Blockchain leveraged medical platform to protect the management of EMRs across different hospital departments. The EMR management system utilized smart contracts to store, health data, record logs, regulate the access to medical data among different health organizations. They carried out an experimental test of the framework on a network comprising different hospitals to demonstrate the feasibility of the system in terms of efficiency and efficacy. The smart contracts were designed on Hyperledger. The design and experiments were described in details. The article in [12] discussed how to build e-Healthcare systems and services using Blockchain and IoT technologies.

Malamas et al. [101] used Blockchain technology in a forensics enabled framework for medical devices. The system includes a fine-grained authorization technique using smart contracts on the Blockchain. The smart contract defines the policies and enforces the integrity and confidentiality of transaction logs. The Proof of Stake, consensus mechanism validates the transactions in the Blockchain.

A wide range of queries from patients, clinicians, healthcare professionals and researchers are usually issued to a biomedical database using suitable application programming interface (API) at any given point in time. In traditional log record system, ensuring tamper-proof data and user's queries is crucial. Mytis et al. [105] suggested Blockchain guarantee the integrity and non-repudiation of retrieval information from the conventional biomedical database. The system comprises three components: a) a data user front-end interface used by third parties to make queries b) an interface for interacting with biomedical interface c) smart contract in between user-interface and database interface to record all user's queries in the Blockchain. The smart contract was developed on the Ethereum Blockchain using Solidity language. MongoDB database is deployed to store biomedical data.

3.1.9. Lightweight BC in eHealth

Blockchain implementation requires immense computational power thanks to its mathematical principles such as cryptographic key systems, the Merkle Hash Tree and Proof of Work (PoW)[197]. Most importantly, IoT devices are typically inadequate in performance. Researchers[198, 199, 12, 200, 19, 201] have proposed a variety of ideas to optimize current BC technology.

Ismail et al.[198] proposed a healthcare architecture using a lightweight Blockchain. The authors geographically divided the Blockchain network and defined different roles of BC nodes. The cluster head called Head Blockchain Manager (HBCM) handles transactions and make Blocks. The HBCM maintains a single copy of ledgers for its members, thus avoiding fork. The customized Blockchain can reduce computational and communication delay but can not guarantee the tamper-proof of the ledger. The proposed scheme was simulated on NS3 and was compared with Bitcoin Blockchain in terms of efficiency and computational cost. Srivastava et al.[199] optimized the power consumption of the BC-based healthcare using lightweight cryptographic techniques such as ARX encryption scheme. The Ring Signatures was used to enhance the privacy properties including the singer's anonymity.

Ray et al.[12] also launched an improved IoT-based eHealthcare Blockchain framework, called IoBHealth where the IoT-based Blockchain network for accessing and managing EHR data in eHealthcare is more robust, secure, open and effective. Attia et al. [200] implemented an IoT-Blockchain healthcare architecture to track patients via connected devices. The authors used Hyperledger fabric as Blockchain and implemented a Graphical User Interface (GUI) that enables a network user to display data ledger in clear visualizations and dashboards. Further, the system adopted Naming Data Networking protocol instead of using device identifiers which allows data mobility between different entities.

In chain structured Blockchain, a Block is propagated throughout the network after a miner completes Proof of Work for the Block. This brings its problem with scalability and high network overhead. Srivastava et al.[202] advanced a scalable Blockchain for remote patient monitoring by incorporating GHOSTDAG protocol which is transaction confirmation protocol. GOSTDAGE mechanism considers each transaction as a node rather than a single large chain of Blocks.

Dwivedi et al.[19] attempted to address the challenges of integrating Blockchain with wearable sensors. The system includes different entities including the Blockchain network, Cloud storage, healthcare providers, smart contracts and patients equipped with wearable IoT devices for healthcare purposes. Blockchain algorithms are run on a hierarchical topology of network nodes where a node with high computational power is nominated as a cluster head for a group of nodes to examine and process Blocks as a representative of its members. Although this approach might address the problem of poor scalability, traffic overhead and power consumption, the avoidance of global consensus mechanism are vulnerable to cyberattacks and sustainability.

Yang et al.[201] proposed a novel consensus mechanism for executing on the eHealth BC. The proposed consensus protocol was called Proof of Familiarity (PoF) that entails a collaborative medical decision making for offering medical services to a patient. In this process, the system enables a new patient to ask for experience of a cured patient given with their similar symptoms and diseases, the medical verdict from several physicians, and the strategic policies from insurance providers. The feedback from every party including healthcare providers, and previously cured patients are used to constitute a favourable joint medical decision. This decision and the hash of the medical data are stored on-chain, and medical data is stored in a local database off-chain. The shortcoming of the paper is that prototype is yet to be implemented to study the feasibility of the proposed consensus mechanism.

3.1.10. BC leveraged searchable encryption in eHealth

With the rapid development of Cloud computing, the original storage way of health data has been changed[96]. In general, health data are sensitive and need protection against unauthorised access. Health data is typically encrypted before uploading to the Cloud storage. The efficiency of accessing these data on the Cloud depends on the mechanism of encryption approach[203]. Searchable encryption (SE) which is a promising encryption technique guarantees data security, without compromising data searchability[96]. However, most current such schemes, particularly the searchable public-key encryption schemes (SPE) are vulnerable to the adaptive leakage-exploiting attacks or unable to meet the efficiency requirements of realistic applications[96]. To achieve a secure and efficient keyword search in the healthcare system, researchers have suggested merging Blockchain technology with a traditional Cloud storage system.

Chen et al. in [96] advanced searchable encryption supported healthcare framework using Blockchain technology. The system saves the search index on the Blockchain while the data is stored in the public Cloud. The consumers are required to obtain permission and encryption key from the owner to access the data. The system utilized the complex Boolean expression to extract the index-building EHRs and supported complex queries that allow different healthcare agents to request permission to access and interact with the medical records, which differs from the previous studies in [204]. Smart contract on the Ethereum Blockchain was designed to trace monetary rewards, including transaction fees, in multi-user setting between the parties involved.

Wang et al.[205] contrived a Cloud assisted consortium Blockchain-based framework for storing and sharing electronic health data. The Blockchain stores encrypted keywords for facilitating the quick search of health data uploaded in the Cloud. They defined the structure of Blocks and transactions and implemented primitive cryptographic protocols to store data securely. The Cloud database support re-encryption of the ciphertext and sends the re-encrypted ciphertext to the specified data requester when the patient has agreed with the data owner. The authors[206] also presented a Blockchain assisted searchable EHR storage system. The Cloud server stores the health data using attribute-based encryption to ensure fine-grained access control of EHRs. The Blockchain stores keywords of the EHR data, which is used to build indexes to enable data visitors to find data content on the Cloud storage. Noh et al.[207] recommended Blockchain to record access logs of medical record managed by Cloud service providers. The paper also included a proxy re-encryption scheme for securely sharing patient data.

3.1.11. BC enabled eHealth architecture

Fog computing has many benefits and is suited for applications that require fast response time, low latency, and real-time processing, for specially healthcare[47] [208]. However, Fog computing brings concerns regarding heterogeneous platform, security, privacy, trust, and resource management [209]. To answer these issues, Blockchain technology has been adapted in Fog enabled healthcare systems. In the context of video stream processing, Islam et al. [208] uploads the data to the Fog server deployed within the vicinity of the video camera instead of Cloud. The authors developed a human activity recognition platform that included Blockchain-based Fog-Cloud computing. They identified important features from video stream before applying data to a multiclass SVM classifier with error-correction out code framework. The strength of the paper is to analyse the accuracy of the activity recognition system using different datasets. However, the authors did not describe how Blockchain has been utilized in the proposed framework and no performance analysis has been conducted regarding Blockchain, Fog and Cloud platform.

Akkaoui et al. [84] proposed a hybrid Edge Blockchain-based eHealth architecture. The architecture consists of four layers: 1) end-user 2) Edge pool 3) global Blockchain 4) off-chain storage. The idea is like the work in [47] in the context of running mining process on the Edge pool to increase the throughput and transactions processing latency. The Edge pool consists of several Edge devices to check the validity of the transactions and classify the data as normal or abnormal. The global Blockchain Ethereum stores the Block containing metadata of EMR and body area sensors data whereas [47] suggested to run the mining process on the Edge networks and store the Block containing metadata

on the Edge network. [84] used an extra global Blockchain that can increase the latency of processing Blocks. The authors [84] also developed several smart contracts to establish role-based access to patient data.

The Blockchain-based healthcare studies covered in this paper is briefly described in Table 8, 9, and 10 with respect to diverse attributes. The acronym used in analyzing literature is explained in Table 5 and 7 respectively.

Table 8
The breakdown of BC based eHealth studies

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
BC for hospital & drug management	Jamil et al.[81]	EHF	SC	✓	⋆	OfC	REST API, couch database, Hyperledger Fabric, Hyperledger Caliper	Cloud front-end Interface was developed to access the BC. Smart contract was designed for defining access policies to patient vital signs for the healthcare professionals.	Security and privacy concerns while transmitting vital signs to Blockchain have not been highlighted.
	Rathee et al.[167]	CPrB	CCM	⋆	✓	NM	NS2 simulator	Blockchain nodes are divided into two types: miner nodes and executing nodes. The executing nodes check the legitimacy of the Blocks	The configuration parameters and implementation procedures of BC on NS2 were not described
	Nguyen et al.[169]	EEB	SCM	⋆	✓	OfC	Ethereum Blockchain network on the Amazon Cloud	Cloud Blockchain was introduced to integrate EHRs to share data between healthcare professionals and patients.	How continuous health data can be handled on the Blockchain has not been covered.
BC for mHealth	Liang et al.[173]	PrPB	ECM	⋆	⋆	OfC/ OnC	Hyperledger Fabric	Blockchain was utilized to validate and preserve patient's data while sharing these with different stakeholders.	Real prototype was not implemented and privacy and security of IoT devices were ignored.
	Nguyen et al.[82]	ClB	SC	✓	⋆	OfC	Amazon web service, mobile android application.	Smart contracts based EHRs trustworthy control mechanism and data exchange protocol on Cloud Blockchain platform was developed.	Security and privacy analysis of the proposed system were missed
	Nguyen et al.[210]	NM	SC	✓	⋆	OfC	Not implemented yet	A mobile Blockchain was developed for clinical assessments and controlling.	Scalability and communication cost issues of the Blockchain have been not investigated
	Ni et al.[174]	NM	CCM	⋆	⋆	NM	Performance evaluation has not been carried out.	The authors developed an optimal decision-making process to keep BC mining cost effective.	Simulation has not been done to analyse its performance.
	Ichikawa et al.[175]	EHF	ECM	⋆	⋆	OnC	Hyperledger Fabric, JavaScript	The authors developed a mobile app to capture wearable sensor data to store those in private Hyperledger Blockchain	Performance has not been analysed in terms of throughput and energy consumption. The security issues between sensors, mobile App have not been addressed.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, ✓= Yes, ⋆ = No

Table 9
The breakdown of BC based eHealth studies

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
BC leveraged access control for eHealth	Tanwar et al.[143]	EHF	SCM	✓	⋆	OfC	Composer, Docker Container, Hyperledger Caliper, and the Wireshark	Access policies for healthcare entities were stored on the Blockchain. Algorithms defining access policy were designed.	Security issues such as malicious attacks and authentication were not addressed.
	Wang et al.[83]	CoB	SCM	⋆	⋆	OfC	Ethereum Blockchain	ABE(Attribute Based Encryption) was implemented using smart contract on Ethereum Blockchain.	The delay caused by ABE has not been addressed.
Storage of eHealth data	Liu et al.[185]	PuB	SC	⋆	✓	OfC	Prototype has not been developed.	EHRs were stored in the Cloud and index of EHRs were maintained on the Blockchain	Performance analysis has not been done.
BC based data sharing in eHealth	Xia et al.[85]	PrB	SC	✓	⋆	OfC	Simulation tools are not mentioned	An access management architecture that exploited smart contracts was designed to monitor access pattern of data users.	Extensive performance analysis has not been carried out.
	Dwivedi et al.[91]	CuB	NM	⋆	✓	OfC	Not implemented yet	The authors introduced overlay network for running Blockchain.	Simulation of the system was not done to analyze performances.
	Shen et al.[188]	NM	SCM	⋆	✓	OfC	WANem	Two separate networks named Blockchain and normal P2P network were designed. A session for packaging and removal of health data while sharing was also introduced.	Settings and configuration about Blockchain have not been described.
	Fan et al.[189]	NM	SCM	✓	✓	OfC/ OnC	breadcrumbs	The authors introduced Blockchain-based data sharing for hospital. The provincial hospital collects data from the community centres and participates in making Blocks.	Blockchain configurations are not discussed.
	Hang et al.[211]	EHF	SC	✓	✓	OfC /OnC	Hyperledger Fabric	The proposed scheme manages EMRs across different hospitals using Blockchain. Smart contract was designed to store data, logs and regulate access to data.	The implementation demonstrated the feasibility of the method.
	Zheng et al.[212]	NM	NM	⋆	✓	OfC	Not implemented yet	A conceptual model was outlined for sharing health data where the hash value of the data was stored on the Blockchain.	The real prototype of the framework is yet to be developed.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned ✓= Yes, ⋆ = No

Table 10
The breakdown of BC based eHealth studies

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
BC leveraged outsourcing in eHealth	Park et al.[94]	NM	NM	✓	⋆	OfC	Not implemented yet	A Blockchain based crowdsourcing platform was designed to provide data owner with incentives.	Performance of the proposed scheme has not been experimented.
BC smart contract for eHealth	Daraghmi et al.[95]	EEB	CCM	✓	✓	OfC	Ethereum, Smart contract using Solidity language.	The authors developed a timed smart contract-based medical record access and permission management architecture. An incentive-based mining process was proposed to eliminate the need for digital currency.	The model was not designed for continuous patient monitoring data.
	Kazmi et al.[100]	EEB	SC	✓	⋆	OfC	Ethereum, Remix	Smart control manages and controls the enrolment of healthcare professionals and devices license in remote patient monitoring.	The security and privacy issues while retrieving data from wearable sensors were ignored.
	Malamas et al.[101]	NM	SC	✓	⋆	OfC	Not implemented yet	A medical forensic framework was proposed using Blockchain to save digital evidence and logs.	The prototype of the proposal was not implemented.
	Mytis et al.[105]	EEB	SC	⋆	⋆	OfC	Ethereum, MongoDB	The proposed system protects biomedical database queries using Blockchain technology	Different Blockchain related security attacks were not discussed.
Lightweight BC for eHealth	Ismail et al.[198]	CPuB	CCM	⋆	✓	OfC	NS3	A lightweight Blockchain was devised where only cluster head maintains Blockchain ledger.	The proposal cannot guarantee the tamper-proof of the data.
	Yang et al.[201]	CPuB	CCM	⋆	⋆	OfC	Not implemented yet	A novel context-aware consensus process called Proof of Familiarity was described to make a medical decision by gathering information from healthcare professionals and cured patients.	High-level performance analysis was done but the prototype of the proposal is yet to be implemented

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, ✓= Yes, ⋆ = No

Table 11
The breakdown of BC based eHealth studies

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
BC leveraged searchable encryption for eHealth	Chen et al.[96]	EEB	ECM	✓	✓	OfC	Ethereum platform	A searchable encryption supported healthcare system using Blockchain was developed. The Blockchain contains the search index.	How BC based searchable encryption improved over the conventional was not demonstrated.
BC for eHealth architecture	Islam et al.[208]	NM	NM	⋆	✓	OfC	Not implemented yet	The authors developed a human activity recognition platform including Blockchain based Fog-Cloud computing.	The authors did not describe how Blockchain has been utilized in the proposed framework and no performance analysis has been conducted regarding Blockchain, fog and Cloud platform.
	Akkaoui et al.[84]	EEB	CCM	✓	✓	OfC	Go-Ethereum	A hybrid Edge Blockchain-based healthcare system has schemed where edge nodes certify the transactions and a separate global Blockchain stores metadata.	Using extra global Blockchain can increase the latency of processing Blocks.
	Calvaresi et al.[213]	EHF	ECM	⋆	⋆	NM	JADE-Java Agent, Hyperledger Fabric	Blockchain technologies (BCT) and MAS were combined to manage reputation for the Agents.	The performance of the Blockchain was not covered in the article.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, ✓= Yes, ⋆ = No

3.2. BC assisted smart cities/home management

The convergence of Internet of Things, Fog and Cloud computing has accelerated the advent of many sophisticated applications including eHealth, agriculture, supply chain, an automatic vehicle with the benefits of enhanced quality of services(QoS). This model can also increase resource utilization, and reduce operating costs.

With the advent of Fog, Cloud and IoT technology, a new business paradigm has evolved that enables customers to use cities/home's resources optimally to provide them with a wide range of services. Smart cities have a range of components including IoT systems, heterogeneous networks, large data storage and efficient information processing centres such as Fog, and Cloud server. Despite having such a vision of smart cities, ensuring high quality and security for smart city services has appeared to be difficult. However, the Blockchain with attractive technological features, Cloud, and Fog computing can be a promising paradigm to opt smart cities/home services. Many recent studies indicate that Blockchain architectures can provide seamless connectivity between clients and industrial applications in smart cities. Recent studies pertaining to deploying Blockchain in smart cities has been summarized with respect to smart city and smart home service. Many of the current smart homes depend on third parties to provide different services to the resident, and in these systems, the resident has little control over his data. Cloud third parties store, process and manage the home data, which is often vulnerable to one single point of failure[214, 215].

Although the existing systems can provide smart home devices with fast connectivity and safe communication, those are centralised and have problems with scalability. Decentralized systems such as Blockchain and smart contracts have been regarded as a potential means of addressing these problems. A smart city is referred to as an interconnected network consisting of computer servers, system administrations and other ubiquitous equipment such as IoT devices for capturing and processing all forms of data generated by city dwellers. Thanks to the distinctive nature of IoT devices, the design of smart cities infrastructure remains challenges, including ensuring anonymity, completeness, and bottleneck issues[216].

A collaborative framework for smart cities to ensure data integrity in the Cloud ecosystem was implemented in [106]. The architecture has two key entities: data owners and Cloud service providers (CSPs). To check the validity of data stored by different CPSs, they introduced a Blockchain-based auditing framework for users. In this context, Blockchain is used to develop a decentralised audit infrastructure which makes the overall system very stable and efficient without the need for third-party auditors. However, the implementation of smart contract and security assessment has not been done. The study in [106] discussed an authorization architecture and IoT delegation in a Cloud-centric Blockchain project. The process is carried out using a smart contract that enables access control functions to ensure trust and auditing for network operations of users in IoT, and Cloud ecosystems.

In addition, a Blockchain was implemented in [217] to develop an IoT-based smart city infrastructure with three key components: smart node, P2P network and Cloud. Blockchain is unstable on IoT devices due to its resource constraints. The authors designed a lightweight Blockchain that requires low computational costs for smart city infrastructure. All IoT devices' communications on a P2P Blockchain networks are tagged as transactions and securely stored in Cloud storage. The architecture for smart cities retains five key cryptographic primitives, including authenticity and entry, confidentiality, and non-repudiation. However, a limitation of the work is that no access control has been designed for Cloud storage.

Meanwhile, Rahman et al.[97] has recommended a Blockchain smart contract-based shared economy applications in the context of smart cities. The multimedia payload from the IoT ecosystem is uploaded and securely stored in IPFS distributed storage repositories as unchangeable headings. In particular, the system also provides a sustainable incentive mechanism that guarantees a secure cyber-physical sharing of IoT data. Smart contracts were implemented without the oversight of central authentication authority that ensures space-temporal services.

The smart home is a network of IoT devices with automated equipment, smart sensors, and detectors that capture environmental information from IoT devices to be stored on a Control server, particularly Cloud storage platform. While smart homes can provide residents with several advantages, there remain several challenges including malicious attacks and privacy issues to be resolved. Cloud computing powered by a Blockchain with distributed, secured and private properties[218] can provide a promising solution to these concerns.

Dorri et al. [219] suggested a smart home architecture that has three main levels: Cloud storage, overlay network, and smart home network. Intelligent tools were designed to handle transactions within the smart home and to preserve confidentiality, fairness and availability of IoT data. Data storage for the smart home network is managed via Blockchain-based Cloud service providers to provide high security for smart home operations. However, the shortcoming of the proposed scheme is that Blockchain for the system has not been implemented.

In [220], the integration of Cloud computing and Blockchain technologies provides a secure and efficient IoT

smart home system. The system is composed of four general components: 1) smart home network, 2) Blockchain network, 3) Cloud infrastructure, and 4) application platform. Blockchain facilitated data traceability and Cloud server was exploited for distributed data storage. In addition, the system also offered recovery and trading facilities of the consumer data generated from the smart home network. Shared key policies were implemented on the Blockchain in order to guarantee smart home authorization and the availability of transactions between IoT devices and Blockchain miners.

In addition, Xue et al. [221] proposed a hypothetical access control system for home automation system, which includes a proprietary Blockchain to hold records of user transactions and store large-scale access data in off-chain storage, such as Cloud server. Singh et al. [222] proposed a smart home appliance management and controlling system utilizing Proof of Authority consensus mechanism of the Blockchain.

Ali et al. [223] implemented a Blockchain-based behavioural verification system for smart-IoT. The system demonstrated a degree of trust level for the external devices that want to join the smart home network. Blockchain was deployed in the IoT behaviour controller system to store, track, and identify IoT devices to safeguard IoT devices from malicious attacks. Sensor level filter has been utilized to prevent the malicious or faulty sensor from joining the network. Lee et al.[224] developed a Blockchain-based smart home architecture to solve the limitations of the existing centralised smart home network and combat future attacks against the smart Gateway. They used Ethereum Blockchain to make sure the smart home data was authenticated and confidential. The summary of some recent research in this field is illustrated in Table 12.

Table 12
The breakdown of BC based smart cities/home studies

Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
Ali et al.[223]	PrB	CCM	⋆	⋆	OfC/ OnC	Tensorflow and Keras libraries	A behaviour capturing, and verification procedures in Blockchain supported smart-IoT system were introduced. Blockchain was deployed in the IoT behaviour controller system to store, track, and identify IoT devices to safeguard IoT devices from malicious attacks.	Performance on the Blockchain has not been conducted.
Lee et al.[224]	PrB	CCM	⋆	✓	OfC	Mininet, Amazon EC2, Ethereum Bridge, Truffle development suite	A Blockchain-based smart home Gateway network architecture was proposed to overcome recent problems in current centralised security network architecture and combat future attacks on the smart homes Gateway.	The Gateway is vulnerable to a single point of failure and no approach was designed to tackle this problem.
Rahman et al.[97]	PrPB	CCM	⋆	✓	OfC	Amazon AWS platform, private Ethereum and Hyperledger Blockchain along with IPFS	The infrastructure leverage cognitive Fog nodes at the Edge to host and process offloaded geo-tagged multimedia payload and transactions. All result for AI processing is saved on the Blockchain and decentralised Cloud repositories to promote shared economy services.	The security and privacy issues of the offloaded tasks were not considered.
Singh et al.[222]	CoB	CCM	✓	✓	OfC	Cooja and Netsim, Amazon EC2	The Blockchain technology was used in a smart home network to manage system transactions and adopted green Cloud computing, which hosts a green broker to minimise the environmental impact of the model.	Blockchain configuration and settings for the simulators have not described in detail.
Yu et al.[106]	CuB	CCM	⋆	✓	OfC	Java Pairing-Based Cryptography Library (JPBC)	An automated blockchain platform called the blockchain data auditing (DAB) method, which gathers audit evidence was proposed. The DAB utilized a customized consensus algorithm based on the Practical Byzantine Fault Tolerance (pBFT) algorithm.	The authors did not describe how the optimized Blockchain was implemented.
Paul et al.[217]	CuB	CCM	⋆	✓	OfC	Ethereum, MySQL, DHT11 sensor	The authors adopted lightweight encryption for smart Blocks, such as symmetric key cryptography, which makes the smart Block more effective in terms of latency.	No access control has been designed for the Cloud storage.
Xue et al.[221]	PrB	CCM	✓	⋆	OfC	C language based on paired cryptographic library	A secure and auditable access control system for smart home using a private Blockchain was proposed	Full featured Blockchain was not designed.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, NA = Not applicable, ✓= Yes, ⋆ = No

3.3. BC assisted IoT vehicular network

The recent development of sophisticated sensing, and computing devices, and information technology has resulted in significant growth in smart transportation services which have significant impacts on various aspects of our lives. Blockchain with Cloud, Fog and IoT can build a stable, reliable, and decentralised intelligent transport ecosystem. The integration of Cloud with virtually unlimited storage, Fog computing with processing capabilities and Blockchain with high-security feature revamps smart transport security and service quality. We reviewed smart transport applications into two main categories : vehicle communication management and secure vehicle operation.

The incorporation of Cloud, Fog computing, and Blockchain can achieve efficient and secure connectivity in automated vehicular networks. Yin et al. [225] recommended a Blockchain-based multi-vehicle Cloud communication network to implement a structured framework. The private Cloud of vehicles from various manufacturers form a V2V(vehicle to vehicle) interconnected infrastructure using Blockchain decentralized system. Thus, the system facilitated various car services including asset management, sharing of ownership, co-operation and collaboration among private Cloud.

Liu et al. [226] implemented a layered architecture that comprises electric vehicles, Cloud and Edge network. The system created a pool of shared resources by facilitating collaboration among the heterogeneously-dispatched electric vehicles in order to provide seamless communications between heterogeneous entities. A Blockchain was used to achieve robust security in sharing information and energy. In this context, a new Blockchain cryptocurrency for vehicular applications was proposed in which two kinds of the coin were introduced data coin and energy. The transactions generated in exchanging information and energy of the vehicular network are encrypted and added to a consortium Blockchain through a consensus mechanism.

Nadeem et al. [227] proposed a Blockchain Cloud-based vehicular distributed Ad-hoc (VANET) system to maintain the private lives of vehicle drivers with on-demand and low-cost access. The three interconnected components named 1) vehicle Cloud, 2) roadside Cloud(RSC) and 3) central Cloud form a Cloud hierarchical architecture to address the problems associated with VANET's storage, computation and broadband bandwidth constraints. The joint Cloud network securely links cars, service providers through a Blockchain regulated P2P network that can withstand cyberattacks and tackle bottlenecks issue in the car ecosystem.

Xie et al.[228] designed a Blockchain-based integrity management system for SDN-enabled 5G vehicular networks. In this system, each vehicle shares a tag containing road information with other vehicles. Other vehicles nearby this sender offer it scores regarding the veracity of the shared information so that false or incorrect information cannot impact destination vehicles. The score providing vehicle determines the trust value based on their distance with the sender vehicle and puts the value in the Blocks. Proof of Work and Proof of Stake consensus mechanisms were used to confirm the Blocks on the Blockchain. The simulation for the proposed scheme was carried out in OMNET++.

Michelin et al. [7] proposed SpeedyChain that decoupled Block headers from the Block's contents. The Blockchain for managing smart cities processes Blocks' headers on-chain. The authors set an expiration time while forming a Block to reduce its size and recommended the key update of the algorithms to minimize transactions' traceability. Further, they incorporated the level of access to control vehicles' permission. The experiment of the system was undertaken in an emulation environment using Common Open Research Emulator (CORE) to assess the performance of the SpeedyChain.

Meanwhile, Baza et al.[108] suggested Blockchain technology for providing autonomous vehicle (AV) with a firmware update on a regular basis. The manufacturers of AV inserted proofs into the on-board unit (OBU) of their AVs using ABE (attribute-based encryption) mechanism. The smart contracts were designed to hold policies about who has the right to download and use the firmware update. The authors proposed a Zero-Knowledge Proof in which each distributor exchanges an encrypted version of the firmware update with their AVs. The smart contract delivers the decryption key if the AVs can display the proofs obtained from the distributors.

The future transport system is going to accommodate driverless automatic vehicles that will carry freight and people. The human-driven gas station will be replaced with full autonomous electric charge station. In this scenario, transactions will be committed between machine to machine(M2M), and the present credit-based system is not adequate to facilitate transactions for such autonomous intelligent transport system. Pedrosa et al.[229] emphasized that the Blockchain technology can provide flexible and scalable facilities for M2M transactions targeting the use case of a driverless vehicle to be charged in electric stations. The shortcoming of the article is that the feasibility of the proposal was not studied.

Li et al.[230] proposed a Blockchain assisted vehicular Fog computing for carpooling services. Carpooling refers to the act of sharing a single vehicle with one or many passengers travelling in the same direction. Malicious users

or drivers can falsely report their locations in such a system. To preserve passenger privacy and security, the authors applied conditional privacy, one-to-many proximity matching, destination matching, and data audibility in the car-pooling scheme. The authors suggested Blockchain on RSU (roadside unit) that was deployed in the Fog layer. The Blockchain stores the hash of the data transactions generated from user's queries and the Cloud server stores those data. The queries, and report regarding car locations, route plan were passed to Cloud server via the RSU Blockchain so that malicious users cannot alter information. The experiment was conducted on a private Blockchain.

Yao et al.[231] suggested a Blockchain assisted authentication approach for distributed vehicular Fog network. The authentication process was completed following four phases: 1) registration phase, 2) authentication phase, 3) consensus phase and 4) service delivery phase. In the registration phase, the on-board unit (OBU) of vehicles asks partial public key from the audit department (AD). The authentication phase involves the communications among OBU, vehicular Fog service (as known as RSU) and service manager (SM) for granting OBU access to resources. Next, the SM and WP (witness peer) run consensus protocol to insert the transactions of the authentication process into the Blockchain. The benefits of using Blockchain is that OBU does not require to initiate the authentication process next time when it moves to other data centre or Fog services.

Gao et al.[232] introduced a vehicular network which combined Blockchain, SDN and Fog computing. The vehicles equipped with OBU (on-board unit), RSU(roadside unit) and BS(base stations) perform the role of SDN data planes such as receiving packets, taking actions on these packets, updating counters and channel selection. On the other hand, the RSUH (roadside hub) was deployed in the Fog layer which acts as an SDN controller and decides the flow rules for the network. RSUH interconnects interzonal vehicular networks and runs Blockchain operations such as consensus mechanism. The Blockchain in the proposed scheme built a trust model by using information collated from peers to decide on messages to be sent from source vehicle to destination vehicle. The network parameter of the scheme was simulated on NS3 to analyse the performance in terms of packet delivery ratio and time. The Hyperledger Fabric was used to develop the Blockchain for the proposed 5G vehicular network.

In most recent research of dynamic car parking allotment; the researchers have suggested Vehicular Ad-hoc Network (VANETs) where vehicles serve as hops to exchange information regarding the saturation status of the parking lot[233]. This approach encounters several challenges including sustainability and security because there is no incentive mechanism to exchange information with other vehicles and there is no consensus mechanism that can increase users' level of trust. To address this research gap, Hassija et al. [234] proposed a system based on DTL and DAG for allocating parking lots where DTL forms a protected peer-to-peer network with users, owners of parking lots, garages and free space. In the DAG network, a time-stamped consensus system was designed to process transactions related to requests for parking reservations in order to give users the best possible services in a cost-optimal manner. The authors also developed an adaptive pricing model for each parking request with respect to multiple parameters to provide the users with the best available slots in less time and expense.

State-of-the-art works in the Blockchain proposed a variation of Proof of Work to overcome the limitations of the generic Blockchain. PoS, PoB (Proof of Burn), and PoET follow the similar principle of PoW. Further, to apply PoS in a new distributed application is challenging because nodes in the network do not own any stake or cryptocurrency to burn in the initial stage. To address this issue, Hassija et al.[235] proposed a DAG-based energy trading platform for V2G(Vehicles to Grid) and G2V (Grid to Vehicles) where all transactions are stored in a tangle data structure. Further, a tip selection algorithm was devised to enable buyers and sellers to add new transactions in ledger without the need for miners. A game theory-based optimization algorithm was designed for both buyers and sellers to have the best deals in trading energy. The game theory guarantees a nash equilibrium between buyers and sellers, thereby preserving the price of energy sales.

Bera et al.[236] proposed a Blockchain assisted secure framework for managing Internet of Drones (IoD). They presented the importance and applicability of BC technology in 5G enabled IoD and developed a Blockchain leveraged data delivery and collection scheme to create a secure communication channel between drones, geographic stations, and control centres. The comparative analysis of security and privacy demonstrated that the proposed scheme is able to resist several potential cyberattacks in IoD.

The traffic jam prediction model assists users' vehicles to avoid congestion on the road. Such prediction model requires live traffic data, users' location and participants' private details including their name, and phone number that are sensitive. Google maps use crowdsourcing for data pertaining to live traffic congestion. However, not all users might be motivated to share their sensitive information about routes and locations with crowdsourcing without sufficient incentives. To realize this, Hassija et al. [237] suggested a traffic jam estimation system based on Blockchain where the Ethereum smart contract was designed to verify and store information from participants. The BC peer to

peer network ensures safe sharing of confidential live traffic jam data from users. To estimate the probability of traffic jam at a specific location, an LSTM-based neural network was used. An incentive model provides a user token if the user shares live traffic data with other users willingly. The user will use the token in the future to access the same services. Most studies in IoT vehicular that are reviewed above are summarized in Table 13.

Table 13
The breakdown of Blockchain based IoT vehicular studies

Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
Yin et al.[225]	NM	SM	⋆	✓	OfC	NA	Blockchain technology was integrated into the shared service model of the JointCloud network. Authors developed a series of information and value exchange networks that facilitate decentralised peer-to-peer communication between the various clouds.	The proposal is conceptual and the Blockchain technology was not described.
Xie et al.[228]	CPrB	CCM	⋆	✓	OfC	OMNeT++, crypto++ library	SDN enabled 5G vehicular network was designed for trust management using Blockchain. A hybrid consensus mechanism based on PoS and PoW was also presented.	Setting parameters for Blockchain has not been discussed.
Nadeem et al.[227]	PrB	NM	⋆	✓	OfC	Not implemented yet	A Blockchain-based distributed Cloud architecture was proposed to safeguard the privacy of drivers.	The scheme was not implemented.
Baza et al.[108]	CoB	CCM	✓	✓	OfC	Python charm cryptographic library	Blockchain and smart contract-based firmware update scheme were proposed for AV's subsystem where a reward system was introduced to incentivize AVs to distribute the updates.	The authors did not describe how Blockchain was implemented.
Yao et al.[231]	CoB	CCM	⋆	✓	OfC	Java Runtime Environment	A Blockchain based lightweight anonymous authentication approach was proposed for distributed vehicular system.	The security protocol needs to be analyzed in enterprise BC.
Gao et al.[232]	PrB	SCM	⋆	✓	OfC	MATLAB, NS-3	The article highlighted the integration of Blockchain and SDN for the 5G enabled Fog vehicular network. A trust-based model is also provided to curb malicious attacks in the network	Integration of the three different technologies demonstrated a promising outcome.
Liu et al.[226]	CPrB	CCM	⋆	✓	OfC	Not implemented yet	A Proof of Work based on data contribution frequency and energy contribution amount was proposed in context-aware vehicular applications.	The context-aware Proof of Work has not been implemented.
Michelin et al.[7]	PrB	CCM	✓	✓	OfC	Common Open Research Emulator (CORE)	The Block header is decoupled from the Block contents and the Blockchain maintains Block header.	Performance analysis was done but how Blockchain was implemented in CORE was not described.
Pedrosa et al.[229]	EEB	SCM	⋆	✓	OfC	Not implemented yet	Refueling scenario for autonomous electric vehicles was described and an algorithm to ensure energy recharges was devised.	Prototype was not realized to analysis performance.
Li et al.[230]	PrB	CCM	✓	✓	OfC	Miracl cryptographic toolset	Privacy-preserving carpooling framework was devised using a Blockchain assisted vehicular Fog computing. The privacy of the users was guaranteed using on-to-many matching, destination matching and data auditability processes.	The privacy concerns in BC were addressed.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, ✓= Yes, ⋆ = No

3.4. State-of-the-art works in BC assisted miscellaneous IoTs

This section contains the state-of-the-art works related to the Internet of Things beyond IoT healthcare, smart home/cities and vehicular network that were reviewed in the above sections.

3.4.1. Agent managed BC in IoT

IoT devices cannot directly host Blockchain technology due to their limited processing and memory capacities. IoT devices produce vast numbers of transactions at a higher rate, but the current Blockchain cannot process those transactions at the same rate. Further, a large number of IoT transactions propagate in the Blockchain networks and cause higher energy consumption. To overcome these fundamental issues of integrating Blockchain into IoT ecosystem, Biswas et al. [238] proposed a scalable Blockchain framework that divides the Blockchain networks into two parts called local peer network and the global Blockchain network. The basic premise of this scheme and the scheme in [239] are similar. In both approaches, IoT systems are not be directly connected to the peer nodes of the Blockchain network. The proposed scheme in [239] described that the flow of transactions would be managed by using an intermediary agent between the devices and Blockchain peers as all IoT applications are usually affiliated with an organization. In [238], a local peer network is formed with devices from the IoT organizations to filter transactions and organize those in the Block. As a result, a lot of transactions remain within the local network that Blockchain would have to globally process. The approach in [239] differs from this scheme with respect to local agents' functionalities. Uddin et al.[239] proposed a local agent that dynamically determines storage repositories, governs the mining process of the Blockchain, maintains multiple Blockchain etc.

Calvaresi et al.[110] attempted to integrate Blockchain technology with multi-agent systems. A Hyperledger Fabric was utilized as permissioned Blockchain, and the Agent was developed using JADE-Java Agent Development framework. The smart contracts manage the reputation of the Agent to measure its credibility. The users have been provided with a GUI to interact with agents in the system.

With Multi-Agent System (MAS), a software agent working on half of IoT devices is an efficient way to promote social interactions among intelligent devices. IoT devices need to associate them with a secure software agent when switching from one area to another [240, 182]. However, IoT devices generally have no accurate information available regarding the agents of a new environment. Further, IoT devices are often unknown, and unreferenced and the traditional approach of asking other trusted agents for information is usually impracticable. The work in [241] suggested a reputation model of the software agent in which the consumer's feedback for its services is summed up. Ethereum Blockchain was used to preserve and certify the reputation of all the agents in the distributed IoT networks.

3.4.2. BC for SDN enabled IoT

Pourvahab et al.[242] proposed Blockchain leveraged forensic architecture in Software-Defined IoT network to collect evidence for the forensic experts to continue further analysis. The Blockchain was adopted into the control layer of the IoT SDN network to authenticate all the IoT devices for safe access. The SDN control layer runs a Neuro Multi-Fuzzy model to classify all kinds of packets into three categories based on six features. The features include the IP address of a source, IP address of a destination, length of flow, packet size, sequence number and type of operation. Finally, suspected evidence was stored in the Blockchain for future investigation.

El et al.[112] envisaged a Blockchain leveraged distributed Fog-Cloud architecture to provide IoT devices with secure, and on-demand access to the Cloud, and Fog. The Cloud-hosted Blockchain transactions and carried out Blockchain operations. The Fog layer incorporated Blockchain managed SDN-NFV technology to carry out computing resources for the IoT network. The SDN controller checked the availability of resources including computing, network, and storage pools at the request of NFV infrastructure servers. The SDN allocated the required resource and launched VNFs which is the basic block in NFVs architecture. The Gateway on the Fog layer provided the IoT devices with smart contract interfaces to place their requests and receive extra resources from the edge servers. The setbacks of the proposal are that the security concerns for the Edge servers were not addressed and the architecture was not implemented for analysing performance.

Talukder et al. [113] built a distributed database system using customized Blockchain technology to safeguard the system from malware attacks. Rathore et al.[114] also described a decentralized malicious attack detection and mitigation approach for IoT ecosystem with the aid of SDN, Edge, Fog, Cloud and Blockchain technology. The IoT devices are connected to SDN enabled Edge switch. The SDN-enabled switch records the information regarding dynamic traffic flow to assist the attack detection process executed at the Fog layer for finding suspicious traffic flows and blocking suspicious flows. The SDN controller at the Fog layer is connected to the SDN enabled switch. The

SDN controller includes four components: 1) traffic flow analyser, 2) traffic flow classifier, 3) Blockchain-based attack detection, and 4) attack mitigation module. The first two components identify anomalous traffic and prepare an individual attack detection model for the Fog node. The third component contributes to the dynamic updating of the attack detection model using Blockchain technology and deep learning algorithm. The attack detection model helps the attack mitigation module to prevent attacks at the Edge layer. They implemented the framework on the Ethereum Blockchain and the Mininet emulator was used to analyse the performance of attack detection and mitigation approach. The authors described the design and workflow of the framework in detail and extensive performance analysis has been done. The significant contribution of the paper is that the Cloud agent collects local detection model using Blockchain smart contract and form a fusion attack detection model with higher accuracy. However, how Blockchain collaborated with SDN enabled switch and controller in the Fog layer is unclear.

In Blockchain technology, all transactions generated in the P2P network is stored in a Transactions Pool. The miners select a certain number of unconfirmed transactions from the Pool in a random fashion or based on a fee in order to make a Block. The Block, in addition to transactions in the Block is verified and confirmed by the Blockchain nodes. However, this approach is not appropriate for transaction validation in time-sensitive service-oriented time tasks because the time-sensitive services might be impacted by long latency. Hosen et al. [243] advanced a context-aware selection process for transactions to be bundled into Blocks by the miners. The authors opted to add an extra field in the transactions to set a priority for the selection process. The priority methodology determined a transaction classification system based on a service's weight. The miner always picks the transactions with higher priority. An SDN-Gateway was introduced to bridge the lightweight IoT devices with Blockchain. The SDN-Gateway controls and collects transactions from the IoT devices. However, the challenge of this approach is to ensure that the weight on the service is honestly set because a client can falsely claim higher priority for its transactions. The author did not demonstrate how weight is measured for a transaction which has been left as future work. The performance of the proposed scheme was evaluated on a network emulator, called Common Open Research Emulator (CORE).

3.4.3. BC for securing SDN IoT

Current IoT networking is confronted with many challenges including security, huge traffic, high availability, high reliability, high bandwidth, and limited energy. The recent emerging technologies such as distributed MEC (Multi-access Edge Computing), Software Defined Network (SDN), Network Virtualization Functions (NVF) and Blockchain are thought to address the existing challenges of the current IoT networking[244]. These technologies can either combinedly or individually meet the major IoT network requirements with high performance. Gao et al.[245] incorporated proxy-encryption (PRE) with Blockchain to improve IoT devices' credibility and authenticity in software-defined networking. Several smart contracts were designed to search and update records on the Blockchain. Mininet with OpenDaylight SDN controller was used to simulate the proposal. Hyperledger with Fabric SDK runs smart contracts to perform registration and enrolment of users.

In the Fog layer, Misra et al.[246] deployed a pBC (private Blockchain) where the Block content contains flow rules that are open to all SDN controllers. In the event of defective flow rules, the pBC allows for easy retraction to a previously running set of rules. As user's reliance on the Internet rises, traditional network designs with static characteristics will eventually fail to meet all requirements. SDN flexibility carries many security threats including unavailability of routing information to forwarding devices when forwarding devices fail to communicate with SDN controller due to the programmable interface being used illegally, and hidden vulnerabilities of a new complex system. To address the security issues, the Blockchain technologies are adopted at the SDN controllers to record and scan network management information[247]. Distributed storage of Blockchain P2P enables the restoration of flow tables of a node during a network failure. To avoid unauthorized interference, Zhang et al.[247] suggested an information classification where the SDN controller's working process is managed by announcing the relationship of dependency between different type of information. However, how information classification was done has not been comprehensible.

Various network attacks are involved in SDN controllers, OpenFlow switches, and host interfaces. For instance, an infected controller can deliver misleading and deceptive instructions to OpenFlow switches by inserting and changing flow rules. Duy et al.[248] utilized Blockchain to record details about SDN events and actions in logs to perform digital forensics. To implement the SDN environment, the Floodlight controller as SDN control pane and Hyperledger Fabric Blockchain were integrated on Docker container.

Medhane et al.[249] proposed a security attack detection architecture for Software Defined Networking. The security architecture combined Blockchain, Edge, Cloud technologies for SDN enabled attack identification. The Cloud layer executes an algorithm to identify attack to reduce security attacks on the Edge layer. The SDN-enabled Gate-

way ensures dynamic monitoring of network traffic flows, which helps detect security attacks by determining dubious network traffic flows. The proposed security framework is implemented using Java programming and estimated performance in terms of network parameters including jitter, average energy consumption, packet delivery ratio, throughput, and delay.

Abou et al.[250] designed a Blockchain-enabled distributed DDoS attack mitigation framework. The framework utilized smart contracts on Ethereum Blockchain to pass attack information between SDN-based domains to promote attack collaboration securely and efficiently. The model is implemented on both private network (Ganache simulator) and the public network (Ropsten test network) of Ethereum to examine it in terms of versatility, efficiency, security, and cost-effectiveness. The smart contract written in Solidity language was deployed on the Ethereum Blockchain using the truffle platform. The smart contract was tested first on Ganache simulator before installing on Ropsten's official Ethereum test network.

3.4.4. BC for mobile IoT

With the exponential growth of mobile phones, the management of huge mobile data traffic requires a secure and fast network connection to boost QoS for consumers. However, network operators require heavy investment to constantly expand the capabilities of network infrastructure with the rapid rise of mobile devices. To cope with this issue, mobile data offloading to Fog or Cloud servers is a promising solution. The conventional algorithms for unloading mobile data do not have any mechanism to inspire or enable mobile devices or users to engage actively in the offloading process. Generic Blockchain was suggested to form a peer to peer network for facilitating mobile data offloading securely. However, the Blockchain with its conventional consensus mechanism lacks scalability and limit the performances of mobile data offloading process. Further, there involves a lot of microtransactions between the service providers and users in mobile data offloading. The users require to pay a certain amount to miner nodes for adding every microtransaction in the Blockchain which can demotivate them to participate in data offloading. To address this issue, Hassija et al. [251] suggested a lightweight framework based on Blockchain to enable mobile data offloading where the offloading is scheduled by a hashgraph consensus algorithm according to the minimum offloading time. The game-theoretical model was developed to negotiate and choose the best mobile devices in terms of computing power and processing time for data offloading. Their simulation results in the lowest cost of contact and suitable scheduling compared with other approaches to offloading.

Mobile devices can access the Edge servers to expand their computing capabilities. Edge computing has been seen as a promising solution for mobile Blockchain applications, which can bring several benefits. First, the robustness of the Blockchain network is enhanced, by adding more miners. Second, smartphone users can achieve a reward for executing a consensus mechanism of the Blockchain by utilizing Edge resources. To realize economical benefits on a mobile system, Edge providers need to set optimized pricing levels for the Edge computing services. For instance, Xiong et al. [252] suggested a pricing mechanism to buy Edge computing resources in mobile Blockchain network. The author in[252] introduced a mobile Blockchain network that allows mobile devices to invoke and access resources or computing services from the Edge network for running the mining process of the Blockchain. The mobile or IoT devices purchase computing resources from the Edge service providers using the two-stage Stackelberg game model. A prototype of the architecture was implemented to demonstrate important findings from the proposed pricing scheme.

Mobile and IoT devices are usually restricted to local computing resources. These devices require to offload computational tasks to the Cloud/Fog to perform Proof of Work. Jiao et al. [253] planned a Blockchain assisted auction mechanism for the resource-limited devices to utilize Cloud/Fog computing resources. The authors [253] suggested two bidding schemes: 1) the constant demand scheme in which each miner bids for a fixed quantity of resources, and 2) the multi-demand scheme in which the miners may apply their desired demands and bids. Further, they described an auction mechanism for the constant-demand bidding scheme which achieves the optimum total utility of the computation resources and the number of miners in the Blockchain network using an approximate algorithm. The authors designed their resource auction algorithm in a Cloud/Fog ecosystem to address several questions such as which miner can be offered the computing resources, what is the optimal number of miners because a small number of miners can diminish the credibility of the Blockchain network and a large number of miners can cause network latency, how fair pricing can be set for performing mining tasks. This model was implemented in a Go-Ethereum platform to analyze performance.

Mobile devices can discharge data traffic to a Fog layer to extend their network transmission bandwidths. The mobile devices can also discharge computing tasks to the Fog layer to release their workloads. Tang et al.[254] presented a Blockchain leveraged task offloading approach for the Fog-Vehicular environment. The Blockchain ledger saves the

transactions related to the computational load of Fog servers. A vehicle chooses a Fog server based on computational load and distance. The proposed scheme was simulated on NS3. The work in [47] also envisaged a Blockchain-based task offloading approach for eHealth in Fog-Cloud ecosystem. However, the approach in [47] is different from the existing schemes in several ways. In [47], the Patient Centric Agent assists in outsourcing patient's tasks to a remote Fog Agent considering the sensitivity of the tasks. The computational parameters of the Fog Agent were divided as dynamic and static. Static execution parameter of a Fog Agent (such as CPU processing capability) is stored in the Blockchain while the dynamic execution parameters such as computational queue latency are asked from a group of Fog Agents. Storing transactions related to dynamic execution parameters increases power consumption and throughput of the task offloading approach. If more than one Fog Agent is a candidate for outsourcing, the Hungarian algorithm was used to optimize energy consumption and processing time. The remote Fog Agents can lie about their static and dynamic execution parameters. To prevent them from doing so, the Proof of Stake consensus protocol was modified to record reputation for every Fog Agents. The miners verify the static execution parameter by assigning sample tasks to a Fog Agent when a Fog Agent wants to join the Blockchain.

Nguyen et al.[255] has suggested a novel Blockchain mobile network in which smartphones load complex computing tasks onto the Edge node to facilitate computationally intensive mining. The article presented a privacy-preserving task-offloading network by considering the complexities of the Blockchain transaction states and channel states between the miners and the Edger server. They proposed an optimal DRL-based algorithm for all miners by using a deep Q Network to achieve complete confidentiality and reduce the cost of latency and resources.

3.4.5. BC for wireless sensor networks

In wireless sensor networks, nodes remain unattended for an extended period and often fail to properly operate due to natural disastrous and malicious attacks. To recover the failed nodes, Noshad et al.[256] proposed a Blockchain-based node failure detection and recovery approach in a wireless sensor network. In this process, the hierarchical structure of the nodes was considered where a cluster head (CH) maintains the Blockchain ledgers. If a cluster head goes in an active state, a centralized entity requests the session history of the failed node from other CHs which degree of nodes is higher. The authors introduced a smart recovery contract (SC) to record the state of every CH.

Yazdinejad et al. [257] schemed a Blockchain-based decentralized authentication process for the Internet of Underwater Things. The cluster head chosen from IoUT devices forms a P2P network for running the Blockchain. If a node in a cluster is approved, the node can authorize other nodes and be trusted in other clusters. The node does not need to perform the authentication process again while communicating with other devices in another cluster. The Blockchain ledger contains a unique device and other information regarding IoUT nodes.

Uddin et al. [258] contributed to exploring a smart Agent's feasibility in tracking underwater IoT and IoT smart home or cities using a custom Blockchain. In Blockchain leveraged underwater IoT monitoring framework, they designed a secure light hierarchical routing protocol for the underwater sensors deployed at different depths and a lightweight consensus mechanism of the Blockchain for processing underwater IoT data. Java programming was used to implement the system. The architecture consists of three layers: Underwater IoT layer, the Edge layer and Cloud layer. The smart Agent residing in the Edge layer receives data from the surface nodes of the IoUT layer and selects a group of suitable Miners from Cloud Blockchain network using the TOPSIS method to process IoUT data. To analyse the efficiency of the proposed consensus protocol in detecting an anomaly, the authors used publicly available datasets called KDD Cup 1999 Data[259]. In addition, the performance of the Blockchain-based routing protocol is evaluated in terms of different metrics such as block time generation, energy consumption, remaining energy and reliability.

Goyat et al.[260] proposed a BC-based storage and authentication framework for WSN (Wireless Sensor Network). In this scheme, cluster heads forward the data sensed by regular sensors to a base station (BS). The BS accommodate a BC to manage security keys and transmits large data to Cloud storage. The BC on the BS removes and revoke certificates of malicious nodes.

Pop et al. [115] explored the Blockchain technology in a smart grid to manage demand response of energy. The smart contracts executing on the Blockchain defined the expected levels of energy demand, validated demand response agreements, and a balance between energy demand and production. The Ethereum Blockchain was used to implement a prototype of the smart grid based on UK building datasets. Cech et al.[261] investigated the full functionalities of Blockchain on the Fog network to share data emitted from IoT sensors. The authors used virtualized features of the Blockchain using docker container orchestration and management system with its Swarm mode and MultiChain framework. The prototype of the proposed scheme was designed on a Raspberry Pi SBC testbed to show the viability of the data sharing with higher security and integrity.

Zhu et al.[262] investigated Blockchain in the Fog layer to set up a social network which managed two main services: Identity management and relationship management services. They further outlined access policies based on the relationship of the users. The authors described the identity registration, update, and revocation process on the Blockchain-enabled Fog network. The prototype of the system was implemented using SELinux and a Raspberry PI as a Fog node. In IoT Fog computing ecosystem, the PoW consensus mechanism is not appropriate due to its high-power consumption and time. Kumar et al. [156] optimized PoW for the IoT-Fog network using statistical method. They used polynomial matrix factorization to reduce the number of iterations to find the solutions for PoW. The proposed scheme was implemented to demonstrate the power consumption and processing time.

Biswas et al. [68] presented a lightweight consensus mechanism called the Proof of Block Trade (PoBT) for validating diverse kinds of trades. The authors incorporated this consensus mechanism into the architecture of the Hyperledger Fabric to build a scalable local trading network. Samuel et al.[263] presented a Blockchain-based data-sharing model for the smart grid which also included a Proof of Authority(PoA) consensus mechanism using page rank algorithm to minimize gas consumption and computational cost. In addition, Huang et al. [10] proposed a self-adaptive PoW algorithm to reduce power consumption for the power restricted IoT devices. The authors suggested determining the difficulty level of PoW consensus mechanism considering the nodes' behaviour in which difficulty level was reduced for the honest node and was increased for malicious nodes. An access control scheme which uses a robust data authority management approach based on symmetric cryptography in a transparent Blockchain network was also explored in the work.

3.4.6. BC for IoT supply chain

Hassija et al. [264] presented a thorough analysis of security and privacy problems relevant to various supply chain management areas. Three technologies-Blockchain, machine learning, and PUFs have been identified as a way of resolving security threats and other problems prevalent in traditional supply chains. For prospective researchers, the possible scope of study and recommendations for the supply chain have been addressed.

Malik et al. [109] developed a TrustChain which is a Hyperledger Fabric Blockchain-based supply chain system. The research included reputation management at each level of the supply chain from the product to the consumption, including the role of supply chain entities. The authors leveraged the smart contract to automate the assessment of reputation based on the quality of the food product being traded, the trustworthy of the supply chain participants and penalized the participants that withdraw their roles and falsely circulate high ratings. Malik et al. [265] also devised a tiered architecture to maintain provenance in supply chain systems and facilitate a forum for collaborating between supply chain entities and administrative bodies. The framework included an Access Control List (ACL) for transactions' reading and writing access and managed a set of parallel Blockchains instead of one large Blockchain. A transaction vocabulary was introduced to link the final product with multiple raw ingredients.

Figorilli et al. in [266] presented the application of Blockchain technology to manage the wood supply chain. The authors adopted RFID technology on the wood to receive information from various stages of wood processing, including from standing trees to the final products, going through cutting, felling, harvesting and sawmilling process. They simulated the wood supply chain in the region of Calabria, Southern Italy.

Hang et al.[211] investigated Blockchain in the agricultural sector. The Blockchain algorithms such as consensus algorithm consume higher power consumption and cause high latency in confirming Blocks. The complete replacement of the legacy system using Blockchain requires to invest enormous resources. That's why the authors suggested a hybrid architecture for tracking fish from the production to consumption by combining the legacy system and Blockchain technology.

3.4.7. BC based authentication for IoT

Manzoor et al. [98] designed a hybrid architecture for IoT data sharing by integrating Blockchain, smart contracts and Cloud. The storage problem on the Blockchain was solved by using Cloud storage. The proxy-encryption scheme was used as the security mechanism to enable only the owner and individuals listed in the smart contracts to access the data. A testbed was implemented to check the feasibility of a platform with respect to scalability and performance metrics.

Martinez et al. [267] enhanced the authentication scheme proposed by Zhou et al.[268] to prove the legitimacy of a member in the network. The authors [267] added a new sub-phase called link in an attempt to identify the authenticity of the participant.

Xu et al.[102] recommended Blockchain in IoT ecosystem for authentication and verifying reliable services from

untrusted Edge entities. The Cloud service providers stores services or program code on off-chain and business security-related transactions on-chain. The Edge entities which are at one hop away from the lightweight client cache the services or program code for IoT devices. The lightweight client requests a service from the associated Edge entity and triggers a smart contract to verify the authenticity of the services on the Blockchain. They analysed the performance of the proposed work using Ethereum Blockchain.

Ma et al.[269] advanced a Blockchain-based distributed key management architecture which includes Fog, and Cloud computing for guaranteeing hierarchical IoT access controls. The Fog network containing a security access manager (SAM) is divided into different zones. They break the Blockchain into various side Blockchain to save storage for IoT applications. Each SAM manages a side Blockchain for its domain. The Cloud collects all side Blocks from every SAM and hosts multi-Blockchains to facilitate cross-domain interactions. The proposed scheme was implemented in OMNet++ to analysis security strength and transaction processing time.

Almadhoun et al. [103] sought Edge servers to perform authentication using a smart contract on the Blockchain on behalf of IoT devices. The Fog nodes have an interface with Ethereum Blockchain's smart contract to relieve the burden IoT devices from running an authentication process. User can access IoT devices via Blockchain-enabled Fog servers connected with Ethereum smart contracts.

Nguyen et al. in[104] utilized smart contracts to ensure that the authorized users can access data without the requirement of third parties. The authors also projected a firmware update scheme for the IoT devices by leveraging Blockchain to avoid fraudulent and data tampering.

In addition, Bao et al. [270] presented an IoTChain which is consisted of three layers: 1) authentication layer, 2) Blockchain layer and 3) application layer. The architecture provides several services such as identity authentication, access control, the integrity of storage without incurring high overheads and delays. They claimed that the architecture offers a lightweight feature, and fault tolerance to DoS attacks.

3.4.8. BC for IoT trust management

Kochovski et al.[116] developed a trust management system in an Edge-Cloud orchestrated network using a Blockchain. The system consists of four layers: 1) application layers, 2) Blockchain layers, 3) decision-making layers, and 4) Edge to Cloud orchestration layer. The devices from Edge to Cloud orchestrations need to register to the Ethereum Blockchain. The smart contract on the Blockchain manages the trust for each device based on the author's defined attributes. The decision-making layers select an Edge service or Cloud services using a Markov decision process considering QoS. The strength of the proposal is to develop a smart contract to measure the trust of IoT, Edge and Cloud devices based on user's subscription and several attributes. However, a performance analysis of the Markov decision process for selecting Edge-Cloud providers was partially completed. The Blockchain has been used for maintaining the trust of Edge-Cloud but other security requirements such as data integrity, confidentiality and availability have not been addressed.

Debe et al.[111] designed a decentralised trust model to ensure the credibility of Fog nodes while IoT devices request computing services from the Fog nodes. The reputation scores for a Fog node is computed based on the client's opinion about their previous interactions with public Fog nodes. The nodes that frequently provide ratings have more influence on the reputation of Fog nodes. A client is penalized if it provides false ratings to a Fog node. The Ethereum Blockchain stored the reputation for the Fog nodes. The proposed scheme was tested by developing different smart contracts on the Ethereum. The smart contracts for registration, computing reputation scores and credibility of Fog nodes are tested on a Remix IDE (https://remix.ethereum.org) using Solidity language. Remix IDE is an online tool to develop, debug and test code on a virtual Ethereum Blockchain. The front end of the Blockchain layer has been built on the Truffle Suite (https://www.trufflesuite.com). The work in [47] also incorporated a trust model using a modified page ranking algorithm. Further, the research in [47] included a reputation score in a modified Proof of Stake consensus algorithm in Fog-Cloud network.

Kim et al.[271] proposed a Blockhain leveraged privacy preserving framework for managing human resource records. They introduced a trust scoring system for both employees and employers on the BC so that both information about both parties is transparent and trustworthy. Further, records in the system are classified into different groups depending on their privacy level required for the users. The framework was implemented using BC smart contract technology and performances were analyzed using Hyperledger-caliper.

3.4.9. BC for IoT payment management

Customers need to pay Cloud service providers for outsourcing their tasks. In the traditional system, customers subscribe to Cloud services using different banks. In such a system, both clients and servers require to trust third parties for guaranteeing services and payment which causes bottleneck and distrust problems. Zhang et al.[212] proposed a Blockchain-based payment system (BCPay) for outsourcing resources from Cloud and Fog. The BCPay system includes clients, Cloud server and a Blockchain. The BCPay's operations are performed in five phases: 1) set up phase 2) service implementation phase 3) service checking phase 4) service payment phase 5) service demand phase. All these phases involve Blockchain for completing the payment process without the need for third-party trust. The strength of the proposal is to analysis the performance of the security protocols of the proposed payment system. However, Blockchain-based implementation has not been done and which kind of Blockchain used was not highlighted. Further, the BCPay was not investigated for Fog computing. Debe et al. [99] also designed Ethereum Blockchain-based monetization and automated payment for public Fog nodes. The IoT devices can pay to their connected public Fog nodes for the services via an automated dispute-free payment system controlled by using a smart contract. They tested the proposed scheme using the similar settings of their earlier research in [111].

Meanwhile, Pan et al.[86] developed an EdgeChain, a Blockchain and smart contracts leveraged framework for the Edge-IoT network. The system utilized an internal currency for purchasing IoT services from Edge and Cloud. IoT devices used credit-based coins to purchase Edge servers where smart contracts applied regulation enforcement mechanism to control the actions of the IoT devices. They implemented a prototype to test and evaluate the EdgeChain. Furthermore, Seitz et al.[272] described a case study of IoT marketplaces which included Blockchain and Fog computing to make IoT services available to clients. The customers can check an App on the Blockchain if it is available there. If so, the customer places an order on Fog node using smartphone interfaces and the Fog node brings the app from the storehouse.

The succinct analysis of miscellaneous IoT and Blockchain related studies are presented in Table14, 15, 16, and 17, respectively.

Table 14
The breakdown of BC assisted IoT works

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
Agent managed BC in IoT	Biswas et al.[238]	EHF	SCM	⋆	✓	OfC/ OnC	Hyperledger Fabric, kafka-Zookeeper, Configtxgen	The authors introduced a local peer network to connect IoT network with global Blockchain which can limit the number of transactions entering into global Blockchain.	Local peer is vulnerable to many cyberattacks including Ransomware, and DoS attacks
BC for SDN enabled IoT	Pourvahab et al.[242]	CPrB	CCM	⋆	✓	OfC/ OnC	NS3, Python, C++, OpenFlow switch	A forensics architecture that adopted Blockchain network on SDN controllers for implementing chain of custody.	The paper did not describe in details how different tools are integrated to implement the proposal.
	El et al.[112]	PrB	NM	⋆	⋆	OfC	Not yet implemented yet	An architecture combining Blockchain, Edge computing and IoT was described.	The conceptual model was proposed without performance analysis
	Rathore et al.[114]	EEB	SCM	⋆	✓	OfC	Mininet, Amazon EC2, Ethereum, Truffle development suite	SDN enabled Fog computing, Cloud and Blockchain technology were combined to detect attacks in the IoT network.	The authors did not describe how Cloud and Blockchain technology was integrated into Mininet tools.
	Hosen et al.[243]	CuB	CCM	⋆	⋆	NM	Common Open Research Emulator (CORE)	A context-aware transaction validation mechanism for the Blockchain's miners was proposed where the miners select transactions from the Pool with the priority of service.	The author did not demonstrate how weight is measured for a transaction which has been left as future work.
BC for mobile IoT	Xiong et al.[252]	PrB	SCM	✓	⋆	NM	Intel Xeon CPU E5-1630 as Edge node	A prototype of mobile Blockchain network was simulated where the mobile devices or users can access and utilizes computing resources from the Edge service providers using two-stage Stackelberg game theory to run PoW consensus mechanism.	PoW consensus mechanism demands high power consumption and causes a delay in the mining process. The author could investigate other consensus protocol such as PoS.
	Jiao et al.[253]	PrB/ EEB	SCM	✓	✓	OfC	Docker platform, Go-Ethereum	The authors proposed an auction-based market model to trade between the Cloud/Fog computing services and Blockchain miners regarding purchasing resources.	Although optimization of mining process improves network performances including bandwidth, power and storage, it makes the mining process less decentralized and vulnerable to cyberattacks.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, NA = Not applicable, ✓= Yes, ⋆ = No

Table 15
The breakdown of BC assisted IoT works

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
BC for mobile IoT	Tang et al.[254]	PuB	SCM	⋆	✓	OfC	NS3	The authors incorporated Blockchain in the Fog network to facilitate secure task offloading	The authors did not focus on privacy of offloading tasks.
	Nguyen et al.[255]	EEB	SCM	⋆	✓	OfC	Ethereum, Lambda Edge, Amazon cloud, Biokin sensors	The authors proposed a task offloading for Blockchain assisted mobile Edge computing network using Markov decision, reinforcement learning (RL) and deep RL Q-network where mobile users act as miners and outsource tasks to Edge server.	The authors performed an extensive experiment and evaluated different performances that showed the approach's feasibility.
BC for wireless sensor networks	Noshad et al.[256]	PuB	SC	⋆	✓	OnC	Remix IDE, MetaMask, Ganache, Rinkeby test network and MATLAB R2018a	The authors suggested a Blockchain-based node recovery method for WSN where failed node is recovered based on the node degree.	Security strength of the approach was not evaluated.
	Yazdinejad et al.[257]	PrB	SCM	⋆	⋆	OnC	NS2	A decentralized authentication using Blockchain for underwater sensor networks was proposed	The authentication protocol was not described well and the role of the Blockchain in this process has not been clear.
	Uddin et al.[258]	PrB	CCM	✓	✓	OnC	iFogSim, Java Programming	The authors designed an Blockchain based multilevel architecture for Internet of Underwater Things	Security analysis has not been carried out in the simulated environment. Instead, a high level security conceptual analysis has been done.
	Pop et al.[115]	EEB	SCM /SM	⋆	✓	OfC /OnC	Ethereum platform	The author exploited Blockchain to build a smart gird for handling energy demand response.	The customer's privacy was not addressed.
	Cech et al.[261]	PuB	CCM	✓	✓	OfC	Raspberry Pi SBCs	The authors built a Fog computing system called HCL-BaFog using Blockchain to collect and exchange sensor data safely.	Full featured Blockchain might not be supported by all kinds of low-profile Edge nodes.
	Zhu et al.[262]	PuB	SCM	✓	⋆	OfC	SELinux, Raspberry PI	Fog computing and Blockchain to build a trustless social network system was investigated.	User's privacy has been addressed using access control.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, ✓= Yes, ⋆ = No

Table 16
The breakdown of BC assisted IoT works

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
Optimization of BC consensus method	Kumar et al.[156]	CPuB	CCM	⋆	✓	NM	NM	The authors devised a modified PoW for Cloud and Edge computing using expectation maximization algorithm and polynomial matrix factorization.	Tools to implement for the Blockchain have not been mentioned.
	Biswas et al.[68]	PuB/ EHF	CCM	⋆	✓	NM	Hyperledger Fabric	The authors proposed a lightweight proof of block and trade (PoBT) consensus to optimize Proof of Work	The performance evaluation shows that without sacrificing security, the proposed consensus mechanism can reduce power consumption.
	Huang et al.[10]	CuB	CCM	⋆	✓	OfC	RESTful HTTP, RPC, IOTA Python API	A credit-based Proof of Work was proposed where the difficulty level is reduced for honest nodes and increased for malicious nodes.	Variations in the degree of complexity will increase the risk of Blocks in the ledger being manipulated.
BC for IoT supply chain	Malik et al.[265]	CoB	SCM	⋆	✓	OfC	Hyperledger Composer, Caliper	The authors built a consortium Blockchain trust management system for the supply chain where trust and reputation scores for the participants are determined based on their interactions	The sharding technique improved the performance of the system.
	Figorilli et al.[266]	CoB	SCM	⋆	⋆	OfC /OnC	Azure Blockchain Workbench, MySQL server, REST API, JSON	The authors implemented an electronic traceability system using Blockchain where RFID sensors and open source technology were used for info tracing.	Appropriate security and privacy methods are needed at every stage of the traceability system.
	Hang et al.[211]	EHF	SCM	✓	✓	OfC	Couch DB, Hyperledger Fabric, Docker engine, REST API, JSON	The combination of Blockchain and conventional system was investigated to store agriculture data from the fish farm in tampered proof way.	The conventional portion of the system is still vulnerable to cyberattacks.
BC based authentication for IoT	Manzoor et al.[98]	EEB	SCM	⋆	⋆	OfC	Ethereum	A Blockchain based proxy re-encryption scheme were presented. Experiment was done on Ethereum Blockchain	Details about settings and parameters are missing in the experiment.
	Ma et al.[269]	PrB	CCM	✓	✓	OnC	OMNeT++, ECIES, curve secp160r1	The authors proposed a novel multi Blockchain based Fog-Cloud architecture for managing security key.	Although multi Blockchain improves performances, a chain might be manipulated and recreated by malicious attackers

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, NA = Not applicable, ✓= Yes, ⋆ = No

Table 17
The breakdown of BC assisted IoT works

Category	Authors	1	2	3	4	5	Tools/Simulator	Contributions/Outcome	Weakness/Remarks
BC based authentication for IoT	Almadhoun et al.[103]	EEB	ESM	✓	⋆	OnC	Remix IDE, Solidity language, Ethereum	An authentication mechanism for Blockchain enabled Fog network where Edge servers facilitated interface to access IoT devices via smart contracts on the Blockchain	implementation of prototype is left as future work.
BC for IoT trust management	Kochovski et al.[116]	EEB	SCM	⋆	✓	OfC	Ethereum	A trust management architecture for Fog-Cloud was implemented using Smart Contracts.	The Blockchain has been used for only maintaining trust of Edge-Cloud but other security requirements such as data integrity, confidentiality and availability have not been addressed.
	Debe et al.[111]	EEB	SC	⋆	✓	OnC /OfC	Ethereum, Remix	The authors proposed a Blockchain reputation model for public Fog nodes-based user's opinion about their past interactions with the public Fog nodes.	The performance of the system was not analyzed with respect to power consumption, throughput and other parameters.
BC for IoT payment management	Zhang et al.[212]	EEB	SM	✓	✓	OnC	Ethereum	The author presented a Blockchain based payment system called BCPay with architecture, specifications and adversary model	Blockchain based implementation has not been done and which kind of Blockchain used was not highlighted. Further, the BCPay was not investigated for Fog computing.
	Debe et al.[99]	EEB	SC	⋆	✓	OnC	Ethereum, Solidity language, Remix web tools	The authors proposed a Blockchain-based monetization and payment system for the public Fog nodes for the services they provide.	The performance of the system has not been analyzed with respect to power consumption and throughput.
	Pan et al.[86]	EEB	SCM	⋆	⋆	OnC	OpenStack, Go-Ethereum, Truffle	The authors incorporated a permissioned Blockchain to link Edge Cloud resources with IoT devices using internal coin currency.	Trust module is yet to be included in the system to make it sustainable.
	Seitz et al.[272]	EHF	SCM	⋆	⋆	OfC	NA	The authors recommended an IoT Bazaar to trade Edge apps using Blockchain to enable the monitoring of app installations on Edge devices.	Performance analysis has not been conducted for the proposal.

1 = Blockchain type, 2 = Consensus protocol, 3 = Access control, 4 = Scalable, 5 = Storage, NM = Not mentioned, NA = Not applicable, ✓= Yes, ⋆ = No

4. Research Gap and Solutions

In the manufacturing field, IoT technologies have promoted industrial automation and digitization. Various recent developed IoT apps have improved the quality, flexibility and scalability of the manufacturing infrastructure and thus it has reduced error, saved cost, and enhanced performance, and security in the manufacturing and industrial process[8]. Most existing IoT architecture maintains a centralized data centre for storing and processing sensors' data, which can be at risk of breaching security, single-point failure and malicious attacks like DDoS, Sybil attack[8][10][273]. This results in unavailability of service and the deluge of sensor data and thus outweighs the important advantages of the IoT system. Further, the data interception can occur when IoT devices transfer data between them which questions the reliability of the collected data. The notion of integrating Blockchain and IoT has recently gained significant popularity among the researchers to exploit such hybrid architectures to address the aforementioned issues. However, the adoption of the Blockchain technology into IoT applications poses a couple of challenges outlined in Figure 21 such as different mining rate, and imbalanced resources capacity between IoT devices and the Blockchain nodes. To meet these issues,

Researchers[15, 213, 274, 275, 276] suggested autonomous agents adopt Blockchain technology in various IoT ecosystems including healthcare, smart cities, smart home and electric energy trading which are regulated and managed by the autonomous agents on behalf of users. An agent typically refers to an autonomous entity which can perform actions on sensors or IoT data as a substitute of users. Internet of Things ecosystem compromising a wide variety of devices including wearable sensors, smartphones, network devices and portable computers generate massive quantities of data at very high speed. Users are not always in a position to manage this influx of data[277]. Hence, autonomous entities are required to track and analyse data while streaming the data from different types of IoT devices. The autonomous agent is a proactive body, which can decide the appropriate sensor data actions and automatically trigger action without the human user's intervention[274]. Machine learning and artificially intelligent technology typically form a basis for the creation of an autonomous agent to process and automatically identify action on the data streaming from sensors or online sources[213]. For instance, Tom et al.[274] proposed an agent-based smart energy distribution system on the IoT Fog network. The agent is designed to negotiate energy demands based on prices and energy availability during peak periods with the home agent at the customer's end.

The convergence of Blockchain technologies and multi-agents such as an agent for environmental protection, energy trading and monitoring patients can handle sensitive data to advocate transparency and trustworthy interactions for consumers and service providers[213]. Luo et al.[276] proposed multi-agents controlled Blockchain-based decentralized electricity trading system. This system consists of two layers: the upper layer that contains multi-agents for negotiating the electricity trading contract, and lower layer that hosts Blockchain network for the settlement of the electricity contracts. Qayumi et al.[275] proposed multi-agent to solve the scalability issue of the Blockchain-based architecture but did not describe how this can be achieved. Norta et al.[278] presented smart contracts for cooperation across various organizations. They described the possibilities of the Blockchain smart contract in realising non-repudiating properties. However, these works are still at a preliminary stage and will be developed in future. With Multi-Agent System (MAS), a software agent working on half of IoT devices is an efficient way to promote social interactions between intelligent devices. IoT devices need to associate them with a secure software agent when switching from one area to another[182, 240]. However, IoT devices have no accurate information available about the agents in a new environment. Further, IoT devices are often unknown and not referenced, and the traditional approach of asking other trusted agents for information is usually impracticable. Fortino et al.[241] suggested a reputation model of the software agent in which the consumer's feedback for its services is summed up. Ethereum Blockchain was used to preserve and certify the reputation of all the agents in the distributed IoT networks.

Further, researchers[15][279] have attempted to design autonomous algorithms on smart Gateway to adopt Blockchain in IoT networks. Ozyilmaz et al.[15] utilized a smart Gateway as one of the Blockchain nodes to integrate Blockchain network with low-energy IoT devices. The Gateway facilitated a proof of concept and event-based messaging systems for resource constraint IoT devices to access Blockchain network. This research addressed the connectivity issue of IoT devices with Blockchain but high power and bandwidth consumption required for the Blockchain remain unsolved in the proposal. Cha et al. [279] has developed a privacy-preserving IoT framework, which includes a Blockchain connected Gateway (BC Gateway) to incorporate the Blockchain network as the underlying infrastructure for privacy management. The BC Gateway uses Blockchain technology to secure and track user privacy preferences. However, the research has been limited to address the user's privacy concerns.

Nonetheless, most of these proposals[15, 279] are at a conceptual level and the notion of an agent in continuously monitoring patient's health has not been still studied to optimize Blockchain algorithm and IoT eHealth data manage-

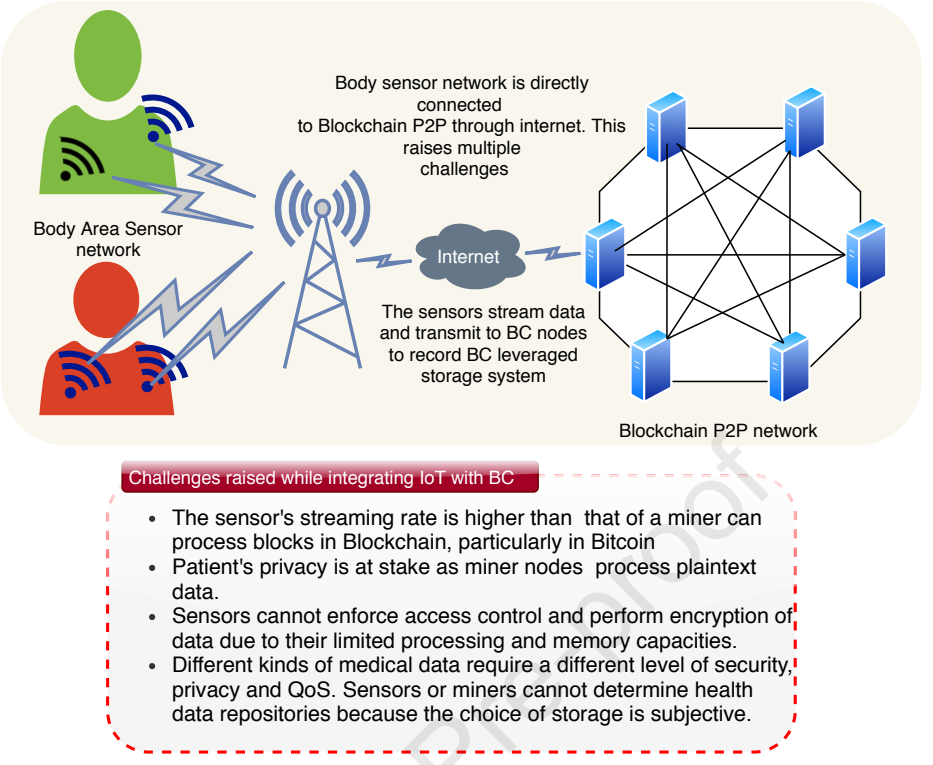


Figure 21: The challenges raised to connect Body Area Sensors with Blockchain

ment. Health data is always regarded as a lucrative target for hackers and researchers are highly motivated to exploit the secure transmission and storage of protected health information (PHI). Recent proposals of building secure eHealth system adopt smart agent in the form of smart Gateway and smart contract to integrate Blockchain technologies in Body Area Sensor Networks (BASN). For example, Griggs et al.[107] integrated WBAN (Wireless Body Area Sensor Network) with Blockchain network. Smart contract executed on the Blockchain can automatically analysis health data based on threshold values and record logs of transactions in an immutable ledger of the Blockchain for generating automatic reminders for caregivers. However, in the existing researches of IoT eHealth and Blockchain, little is known about the storage management of health data, mining management for the Blockchain and security and privacy of the patient end's devices. To bridge this research gap, Uddin et al.[239] proposed a Patient Agent assisted End to End decentralized Blockchain leveraged eHealth framework. The patient agent can provide high performance by integrating Blockchain, artificial intelligence and machine learning technology. The agent can address the challenges(as illustrated in Figure 21) raised while merging body area sensors with Blockchain. Table 18 provides the summary of challenges raised in the integration of BC and IoT and their prospective solutions.

4.1. To balance between power consumption, performance, and security

IoT devices are manufactured with limited computational power and memory capacities, while Blockchain technology requires an excessive level of storage and power[285]. The resource requirements for mining Blocks on the P2P Blockchain network outweigh the capabilities of resource-constrained IoT devices. The Patient Centric Agent introduced in [47][239] running on Edge and Cloud server can handle Blockchain operations on behalf of the IoT devices. The Patient Centric Agent in [239] runs a consensus mechanism and manages multiple Blockchains for IoT data.

[239] contributed to dealing with the challenges of implementing a Blockchain for EHR that can accommodate RPM. This proposal designed a Patient Centric Agent (PCA) to connect Blockchain with the RPM data stream. The PCA is an artificially intelligent software agent that executes on a patient's personal computer. However, implementing a software agent on the smartphone or Gateway devices is hard as these devices may be linked to multiple IoT devices and sensors. If the Gateway device containing the agent is stolen or hacked, operations of multiple IoT devices attached

Table 18
The summary of challenges and their solutions

SL No	Challenges	Prospective Solutions
1	Resource limitations of IoT to accommodate BC technology	Researchers[47, 280] have suggested smart Agent or Gateway converge IoT devices with Blockchain where the smart Agent performs computations, provide network and storage resources required to accommodate BC on behalf of IoT devices. Other kinds of solutions include 1) optimization of Blockchain's algorithms including consensus protocol, security protocol 2) DAG-based BC[235] technology that can obviate the need of miners 3) Sharding that refers to partition of BC network[75].
2	Higher bandwidth consumption in BC	Sharding[75] is a method of splitting BC peer to peer network into the different clusters. The members of a sharding are responsible for processing and verifying transactions generated in that sharding. This results in avoiding the propagation of a transaction across the entire network and hence can save bandwidth. An Edge-based personalized Agent can be appointed for each sharding where the agent collects transactions from IoT devices and make Blocks to further reduce high bandwidth requirements of the BC.
3	Connectivity challenges of IoT with BC	Sidechain[121] is a distinct BC that operates parallel to any enterprise public or private BC also called mainchain. To address the connectivity issue of IoT with BC, the MEC (Multi-access Edge Computing) can host sidechain which is close to the IoT network and enables the IoT devices to communicate with mainchain via the sidechain. Consequently, IoT devices can interact with the sidechain on the Edge network using their low bandwidth.
4	Accommodation of huge volume of IoT data in BC	Many researches have suggested off-chain strategies to handle big data in IoT where conventional Cloud storage is integrated with Blockchain storage. To deal with IoT big data, another approach is to distribute IoT data across multiple repositories including different Cloud service providing repositories, local computer, and on-chain of Blockchain based on the characteristics and diverse contexts of the data [281, 35].
5	Challenges of maintaining privacy in BC	Homomorphic encryption[282] and proxy re-encryption technique [245] have been investigated by several studies of BC and IoT to resolve the issue of user's privacy on the BC network. In addition, Federated learning[283] can be integrated with Blockchain technology to ensure the privacy-preserving computation on users' data. Federated learning allows a machine-learning algorithm to be trained by the participants of the Blockchain without exchanging their data where the Blockchain can guarantee the security of the trained algorithm in the form of a smart contract.
6	Challenges of regulating IoT BC	Lessig [284] described four means: law, social norms, and economic means for governing any applications on the cyberspace. However, no effective legislation has yet been put in place to govern the existing BC-based IoT applications. Blockchain oriented IoT applications can be effectively regulated by combining the technology of four means proposed by Lessig. The integration of the autonomous agent with BC can assist in defining social norms and enacting law for regulating Blockchain.

to the Gateway may be affected and come under various potential malicious attacks[286]. Further, such software agent needs a platform that can facilitate virtualization, encryption, data storage and high computational power for running accurate Blockchain algorithms which smartphone or Gateway cannot support. Therefore, the software agent requires to be executed on Edge or Cloud servers that facilitate distributed environments[287]. The PCA developed in [239] performs the following roles:

- Ensure security and privacy at the patient ends.
- Determine the storage and security requirement of streamed data. For instance, some streams will need to be stored in Blockchains, others can be archived with a lower level of security.
- Manage Blockchain providers. This includes selecting a Blockchain provider and facilitating insertion into a Blockchain by nominating a miner based on parameters such as network latency, power consumption, availability, and trust.

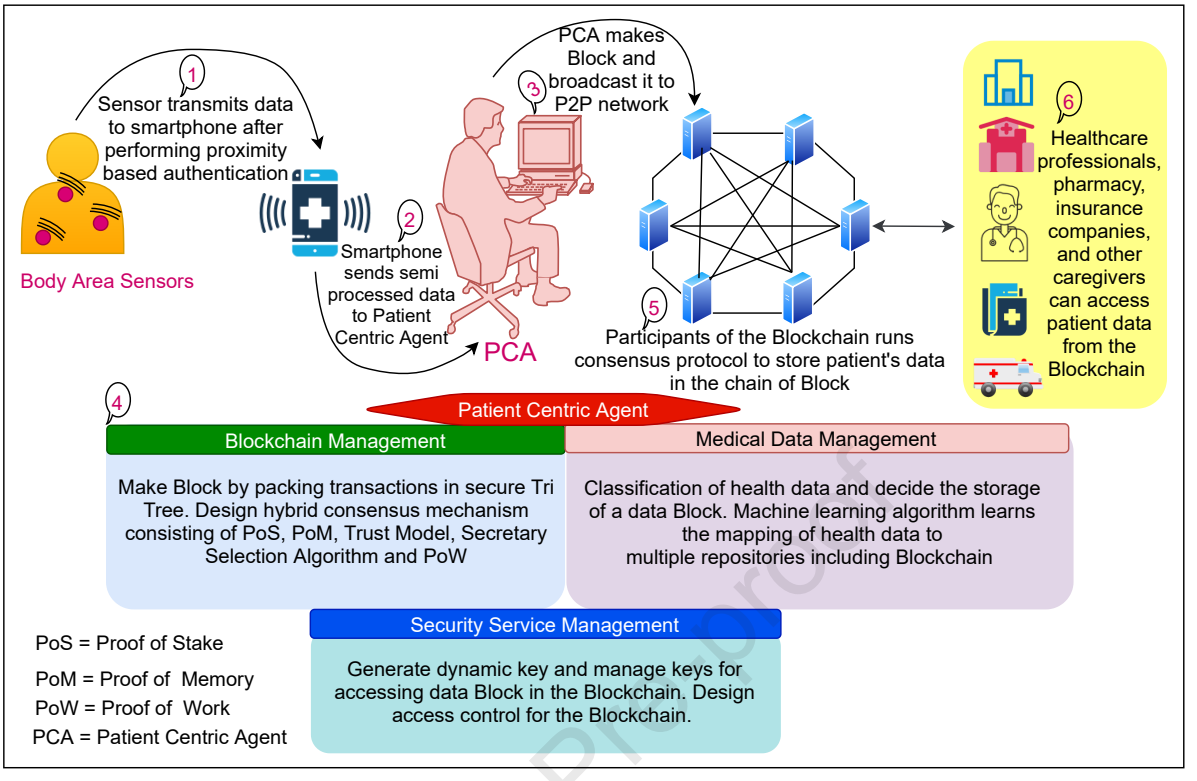


Figure 22: The basic operation of a Blockchain

- Liaise with Trust Centers for key management.

[239] designed a continuous patient monitoring system that includes the proposed Patient Centric Agent for connecting the Blockchain with Body Area Sensor Networks. The PCA depicted in Figure 22 in the framework administers a portion of Blockchain, such as access control, mining processing including a selection of the Miner and multiple Blockchain to protect privacy while streaming data from sensors. A lightweight communication protocol is introduced in the PCA-based architecture to improve data protection between different segments of the patient monitoring architecture in real-time. Figure 22 suggests that the Patient Centric Agent running on a patient's personal device is placed in between smartphone and a customized private Blockchain to bridge two different networks (body area sensor networks and peer-to-peer networks). The bottom part of Figure 22 presents the main activities of the Patient Centric Agent. A customized Blockchain was implemented using Java Programming to analysis the performance of the key algorithms designed in this proposal. The customized Blockchain was run several personal computers to analysis the performance using the NetBean. The high-level analysis of the proposed eHealth architecture was performed in terms of end to end consumption, delay and major cyberattacks.

4.2. To balance between data concurrency and throughput

Since Blockchain maintains a decentralized ledger on a P2P network, the participants require to broadcast Blocks throughout the network to include the Blocks in the distributed ledger and synchronizing it through executing a validation mechanism. IoT devices are equipped with limited bandwidth capabilities[288]. Recently, Edge-devices augmented with IoT devices might have sufficient bandwidth. However, the bandwidth required to operate Blockchain may exceed the upper thresholds of Edge servers. To tackle this aspect, the Patient Centric Agent[239] does not directly transmit transactions to the Blockchain network; instead, it creates Blocks by organizing a certain number of transactions. In this case, a significant number of transactions do not propagate throughout the P2P Blockchain network. Thus, the inclusion of Patient Centric Agent[239] with eHealth framework can reduce the bandwidth requirements. Further, the Patient Centric Agent can optimize the consensus mechanism to reduce the bandwidth in the Blockchain network.

The Patient Centric Agent in [239] operates on the patient's hardware at the end of the patient and creates collaboration between the Blockchain and the sensor networks in the patient's body[287]. However, the system has a centralised Blockchain controller at the end of the patient and decentralised Blockchain storage at the other end. As a result, the end of the patient is often vulnerable to significant cyberattacks such as single point failure and denial of service. The solution to this problem was proposed in [47]. The work in[47] decentralized the Patient Centric Agent through replicating the agent at Smartphone in Body Area Sensor Networks, NEAR processing layer (Fog level), and FAR processing layer (Cloud level). To process patient's records rapidly, a lightweight modified Proof of Stake consensus protocol for the Blockchain was constructed using the Fuzzy Inference Method. The consensus mechanism for data processing in remote patient management was incorporated at the Fog and Cloud levels.

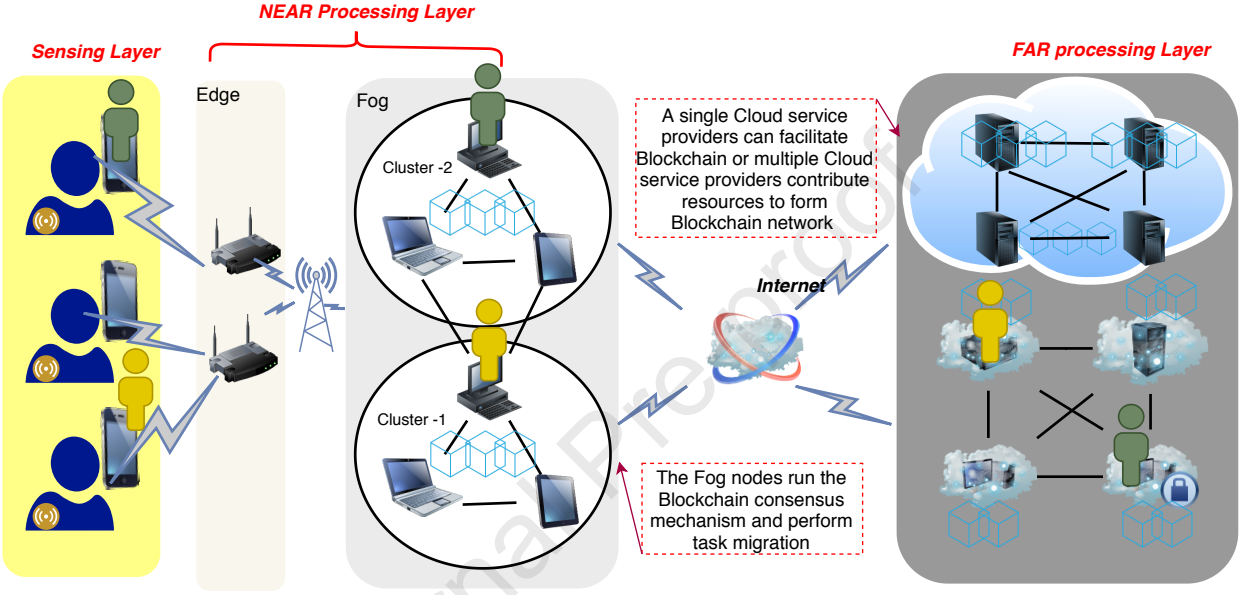


Figure 23: The decentralized Blockchain based eHealth System

The Patient Centric Agent in [47, 280] replicated at the three levels enables outsourcing patient's tasks to Edge and Cloud nodes while preserving privacy and security. Decentralizing Patient Agent in eHealth architecture results in software sustainability and allows the rapid and secure storage of medical data without the trusted authorities from third parties. The proposed decentralized eHealth architecture is presented in Figure 23. The left part of the figure includes various wearable sensors and smartphone to sense patient data. The next level of the sensing layer is NEAR processing layer shown as the middle part of Figure 23 consisting of Edge devices. The replicated Patient Agent in the Edge layer executes consensus mechanism for the Blockchain. The right part consisting of various Cloud service providers facilities high processing and storage for the Blockchain. The decentralized eHealth framework was simulated following the iFogSim. The proposed consensus mechanism and privacy-preserving task migration approach were implemented using Java Programming. The performances of key algorithms were analyzed in terms of Block generation time and energy consumption. The strength and reliability of the security protocols against major cyberattacks for the system were tested using Scyther [289, 35]. To demonstrate the viability of the approach in eHealth monitoring, the comparison of the proposed frameworks with other existing systems was provided with respect to different metrics.

4.3. To address connectivity challenges

In the P2P Blockchain network, all nodes remain connected to the network and autonomously operate through standard protocols. This nature of the Blockchain networks theoretically makes IoT devices higher susceptible to security attacks[2]. In [17]'s settings, the IoT devices are connected to Blockchain via the smart Agent [17] which implements a couple of security protocol to safeguard IoT devices from cyberattacks.

With the growing spread of IoT, the centralised IoT network structure poses the threat of numerous security vulner-

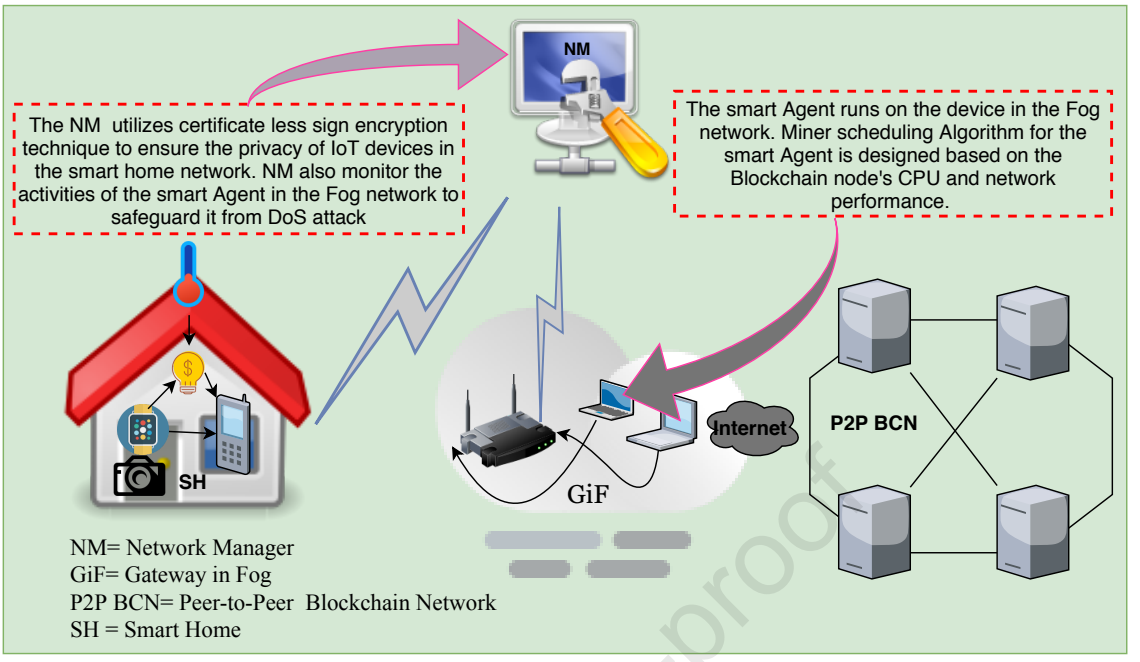


Figure 24: The Blockchain based smart home monitoring architecture

abilities including data forgery, manipulation, and unauthorised access to devices by targeting Gateway services[290]. The IoT devices in a smart home are usually connected to global internet and consumers via Gateway services. Therefore, smart home Gateway should be designed with centralised systems in an efficient and stable manner. [17] contributed to the creation of a system to track smart homes or cities securely using Blockchain technology. In this architecture depicted in Figure 24, along with the smart agent and the Blockchain component, the article [17] included an extra network manager module to encrypt user data using sign encryption that preserves user privacy. Like previous contributions in [47, 280], the work followed similar methodologies for implementing the framework. Few computers run the consensus protocol of a customized Blockchain. Jolinar [291] which is a Java software for estimating the power consumption of process level applications was used in the simulation.

4.4. Handling Big data on the Blockchain

The Blockchain technology has witnessed the most successful application in cryptocurrencies, where miners charge a fee for processing transactions without the requirement of third parties. However, eHealth applications significantly differ from cryptocurrencies in the level of storage requirements[292]. Patient monitoring system continuously streams health data and transactions are more frequently created in such applications. Storing all health data on the chain for many patients is challenged with Blockchain structure. To address these challenges, the Patient Agent in [281] has been provided with the knowledge of determining rapid repositories for every data blocks based on their characteristics and privacy requirements. The data blocks which processing demands the Blockchain-based secure storage are directed to the distributed ledger. For example, billing documents, healthcare provider's notes, medication summaries can be processed and stored in the Blockchain ledger. Other repositories such as Electronic Health Record, Electronic Medical record, Cloud eHealth can be recommended as per the requirements of various data blocks.

A broad variety of digital archives for health records has recently appeared. Those include government-controlled electronic health records, Electronic Medical Records (EMRs) maintained by health care providers, Personal Health Records (PHRs) operated directly by the patient, and modern Blockchain-based systems controlled mainly by technology. Health record repositories differ from each other in terms of protection, privacy, and service quality (QoS) that they provide. The health data contained in these archives often vary in sensitivity and importance from patient to patient, depending on medical, personal interest, and other factors. Decisions are complicated and nuanced about which digital record repository is most appropriate for the preservation of each data element at any point in time. The

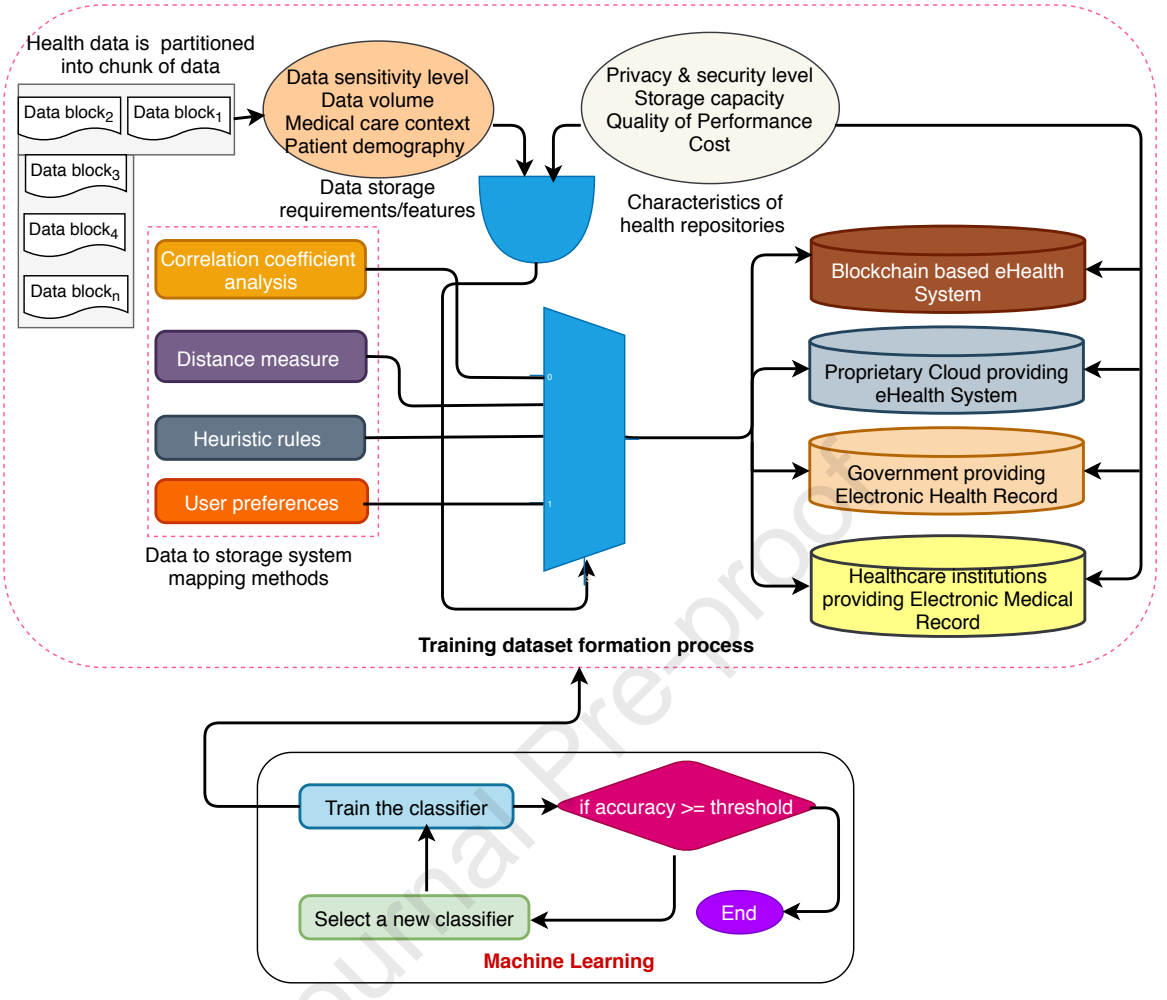


Figure 25: The machine learning based health data allocation systems

health data continuously streamed from wearable devices escalate the challenges. Here, the authors [281] contributed to enabling the Patient Centric Agent for building machine learning-based recommendation model for health data storage that can accommodate data storage requirements, and patient preferences and make storage decisions rapidly, in real-time, even with streamed data. The rapid storage allocation model for health data is presented in Figure 25. The model depicted in Figure 25 has two parts: the upper part involves the processing of inputs and methods to make a training dataset, and the bottom part involves the machine learning. The diverse data blocks with different features and health repositories with their performance measuring factors are fed to the upper portion of the model as input. Several processes such as correlation coefficient analysis, heuristics rules, distance measurements and user preferences are applied to determine the repository for each data block. The study generated a synthetic dataset having a variable number of instances. The dataset represents data storage requirements and user's preferences regarding the archive of their health data. The four datasets have been fed into five different classifiers to study the feasibility of a machine learning algorithm in selecting an appropriate storage medium. Five different classifiers trained here are Multilayered Perceptions (MLP), Random Forest (RF), J48, K-nearest neighbor (IBK) and Naive Bayes (NB). The classifiers are trained using a variable size of the synthetic dataset in Weka ToolKits. The performance was analyzed with respect to the accuracy, and root means square errors.

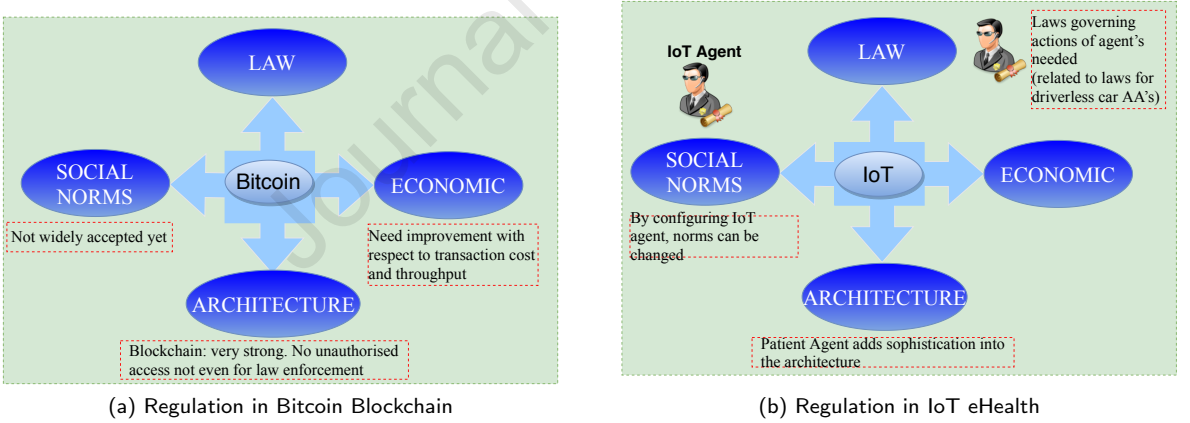
4.5. Maintaining both transparency and privacy

Information processing on the Blockchain nodes encounters the risk of leakage of data as plaintext data is shared and accessed with many nodes. In the BC computing model, the implementation of homomorphic encryption technology has promising potential to secure user data and can allow mining to preserve user's privacy[282]. Homomorphic encryption method allows any third-party service providers such as Cloud servers to conduct certain forms of operations on the ciphertext without first decrypting encrypted data while preserving data privacy at the same time. The integration of homomorphic encryption with Blockchain-based eHealth can potentially protect a patient's privacy in a decentralized model[282]. A consensus method that will be consistent with the technique of homomorphic encryption requires to be designed.

The current global health crisis due to COVID-19 involves tracking positive COVID-19 patients without the need for centralised authority, tamper-proof sharing of COVID-19 related data, and maintaining privacy, while collecting individual and healthcare centre COVID-19 datasets. In nature, the essence of the COVID-19 pandemic itself is distributed[293]. To cope with COVID-19 issues, distributed ledger technology, such as Blockchain, can be highly advantageous but this technology cannot guarantee users' privacy. However, the combination of Blockchain technology and federated machine learning [294] can facilitate decentralised COVID-19 tracing applications without the need of centralised authority that can collect and share user's information with privacy and security. Federated learning[295] is a technique of machine learning that trains an algorithm across several decentralized nodes or servers that do not exchange their local data samples with any centralized server.

4.6. To address regulation challenges of BC in IoT

The accuracy and security features of BC attract a wide variety of applications in the field of finance, economics and law. Further, a recent Ransom attack on the New York Times and BBC drew the attention of the US Congress that seeks BC technology as a potential solution of cyberattacks. Nonetheless, the abusive use of BC in shadowy trading sites has resulted in different scandals such as now-defunct Silk because currently, BC is largely unregulated[296].



(a) Regulation in Bitcoin Blockchain (b) Regulation in IoT eHealth

Figure 26: The dot regulation of BC IoT

Filippi et al. [297] presented the BC as a transformer from "Code is a law" to "Law is Code". Conventional law cannot regulate BC because of BC's decentralized properties. However, the smart contract technology that turns the law into code on the BC can enact laws. Law can be made a product using a smart contract of the BC. Pokrovskaia et al.[298] emphasized on having regulation mechanism for tax, finance and society within the knowledge-driven economy. They highlighted the need of efficient regulation framework for Blockchain and Fog computing. The sustainability and adaptability of BC technology depend on effective regulation and monitoring. Lessig[284] described four means: law, social norms, and economic means for appropriately regulating any applications on the cyberspace. Blockchain oriented IoT applications can be effectively regulated by combining these four means. No legislation is still enacted for governing the existing BC applications. To deal with tracking and regulating BC, IoT application oriented smart Agent can be adopted to configure social norms and implement laws for the BC applications. Figure 26 (b) shows that an agent enabled BC IoT architecture can define four norms of regulating technology including social norms and laws

that are absent in the current cryptocurrencies such as Bitcoin. Figure 26 (b) depicts that Bitcoin has a strong security architecture but other means of regulation have not been still developed.

5. Conclusion

We reviewed research from several domains including IoT eHealth, smart home, smart vehicular applications which incorporated Edge, Fog, Cloud computing and Blockchain technology to address security and privacy challenges. Nonetheless, a variety of technological and security issues in IoT remain unaddressed. In this review paper, several challenges in undertaking Blockchain technology in the IoT domain are identified and how those are being addressed is discussed. Existing Blockchain and IoT articles were scrutinized with respect to diverse attributes for demonstrating their strength and limitations. Further, the review includes a broad description of Blockchain components and several standard consensus mechanisms.

References

[1] Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. Integration of blockchain and cloud of things: Architecture, applications and challenges. *arXiv preprint arXiv:1908.09058*, 2019.

[2] Fatma Ellouze, Ghofrane Fersi, and Mohamed Jmaiel. Blockchain for internet of medical things: A technical review. In *International Conference on Smart Homes and Health Telematics*, pages 259–267. Springer, 2020.

[3] Muhammad Habib ur Rehman, Ibrar Yaqoob, Khaled Salah, Muhammad Imran, Prem Prakash Jayaraman, and Charith Perera. The role of big data analytics in industrial internet of things. *Future Generation Computer Systems*, 99:247–259, 2019.

[4] Soumyashree S Panda, Utkalika Satapathy, Bhabendu K Mohanta, Debasish Jena, and Debasis Gountia. A blockchain based decentralized authentication framework for resource constrained iot devices. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–6. IEEE, 2019.

[5] Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018.

[6] Nils Siegfried, Tobias Rosenthal, Alexander Benlian, et al. Blockchain and the industrial internet of things: A requirement taxonomy and systematic fit analysis. Technical report, Darmstadt Technical University, Department of Business Administration . . . , 2020.

[7] Regio A Michelin, Ali Dorri, Marco Steger, Roben C Lunardi, Salil S Kanhere, Raja Jurdak, and Avelino F Zorzo. Speedychain: A framework for decoupling data from blockchain for smart cities. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 145–154, 2018.

[8] Yong Yu, Yannan Li, Junfeng Tian, and Jianwei Liu. Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wireless Communications*, 25(6):12–18, 2018.

[9] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. Blockchain and iot integration: A systematic survey. *Sensors*, 18(8):2575, 2018.

[10] Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, 15(6):3680–3689, 2019.

[11] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to scalability of blockchain: A survey. *IEEE Access*, 8:16440–16455, 2020.

[12] Partha Pratim Ray, Dinesh Dash, Khaled Salah, and Neeraj Kumar. Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases. *IEEE Systems Journal*, 2020.

[13] Primavera De Filippi, Morshed Mannan, and Wessel Reijers. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, 62:101284, 2020.

[14] Andreas Antonopoulos. Bitcoin security model: trust by computation. *O'Reilly Radar. Retrieved October*, 4:2015, 2014.

[15] Kazım Rıfat Özyılmaz and Arda Yurdakul. Work-in-progress: integrating low-power iot devices to a blockchain-based infrastructure. In *2017 International Conference on Embedded Software (EMSOFT)*, pages 1–2. IEEE, 2017.

[16] Karl J O'Dwyer and David Malone. Bitcoin mining and its energy footprint. 2014.

[17] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring. In *ICIT*, pages 1135–1142, 2019.

[18] Pradip Kumar Sharma, Neeraj Kumar, and Jong Hyuk Park. Blockchain technology toward green iot: Opportunities and challenges. *IEEE Network*, 2020.

[19] Ashutosh Dhar Dwivedi, Lukas Malina, Petr Dzurenda, and Gautam Srivastava. Optimized blockchain model for internet of things based healthcare applications. In *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, pages 135–139. IEEE, 2019.

[20] Hany F Atlam and Gary B Wills. Technical aspects of blockchain and iot. In *Advances in Computers*, volume 115, pages 1–39. Elsevier, 2019.

[21] Elena Karafiloski and Anastas Mishev. Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, pages 763–768. IEEE, 2017.

[22] Kyle. Blockchain issues: 1: Data storage, Jun 2018.

[23] Tianqi Yu, Xianbin Wang, and Yongxu Zhu. Blockchain technology for the 5g-enabled internet of things systems: Principle, applications and challenges. *5G-Enabled Internet of Things*, 2019.

[24] Joshua Ellul, Jonathan Galea, Max Ganado, Stephen Mccarthy, and Gordon J Pace. Regulating blockchain, dlt and smart contracts: a technology regulator's perspective. In *ERA Forum*, volume 21, pages 209–220. Springer, 2020.

[25] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. *Future generation computer systems*, 88:173–190, 2018.

[26] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *Journal of Network and Computer Applications*, 149:102481, 2020.

[27] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58, 2019.

[28] Qingyi Zhu, Seng W Loke, Rolando Trujillo-Rasua, Frank Jiang, and Yong Xiang. Applications of distributed ledger technologies to the internet of things: A survey. *ACM Computing Surveys (CSUR)*, 52(6):1–34, 2019.

[29] Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, and Jun Zhao. A survey of blockchain applications in different domains. In *Proceedings of the 2018 International Conference on Blockchain Technology and Application*, pages 17–21, 2018.

[30] Arzoo Miglani, Neeraj Kumar, Vinay Chamola, and Sherali Zeadally. Blockchain for internet of energy management: Review, solutions, and challenges. *Computer Communications*, 151:395–418, 2020.

[31] Tejasvi Alladi, Vinay Chamola, Nishad Sahu, and Mohsen Guizani. Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, page 100249, 2020.

[32] Tejasvi Alladi, Vinay Chamola, Reza M Parizi, and Kim-Kwang Raymond Choo. Blockchain applications for industry 4.0 and industrial iot: A review. *IEEE Access*, 7:176935–176951, 2019.

[33] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.

[34] Anusha Vangala, Ashok Kumar Das, Neeraj Kumar, and Mamoun Alazab. Smart secure sensing for iot-based agriculture: Blockchain perspective. *IEEE Sensors Journal*, 2020.

[35] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Rapid health data repository allocation using predictive machine learning. *Health Informatics Journal*, page 1460458220957486, 2020.

[36] Jiawen Kang, Zehui Xiong, Dusit Niyato, Dongdong Ye, Dong In Kim, and Jun Zhao. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Transactions on Vehicular Technology*, 68(3):2906–2920, 2019.

[37] Avelino F Zorzo, Henry C Nunes, Roben C Lunardi, Regio A Michelin, and Salil S Kanhere. Dependable iot using blockchain-based technology. In *2018 Eighth Latin-American Symposium on Dependable Computing (LADC)*, pages 1–9. IEEE, 2018.

[38] Vivek Acharya, Anand Eswararao Yerrapati, and Nimesh Prakash. *Oracle Blockchain Quick Start Guide: A practical approach to implementing blockchain in your enterprise*. Packt Publishing Ltd, 2019.

[39] Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek. Performance evaluation of blockchain systems: A systematic survey. *IEEE Access*, 8:126927–126950, 2020.

[40] Rahul P Naik and Nicolas T Courtois. Optimising the sha256 hashing algorithm for faster and more efficient bitcoin mining. *MSc Information Security Department of Computer Science UCL*, pages 1–65, 2013.

[41] Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, 127:43–58, 2019.

[42] Dan Boneh. *Aggregate Signatures*, pages 27–27. Springer US, Boston, MA, 2011.

[43] Jae Cha Choon and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In *International workshop on public key cryptography*, pages 18–30. Springer, 2003.

[44] Weidong Fang, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao, and Guohui Wang. Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1):1–15, 2020.

[45] Avi Asayag, Gad Cohen, Ido Grayevsky, Maya Leshkowitz, Ori Rottenstreich, Ronen Tamari, and David Yakira. Helix: a scalable and fair consensus algorithm. Technical report, Technical Report. Technical report, Orbs Research, 2018.

[46] Ke Huang, Xiaosong Zhang, Yi Mu, Fatemeh Rezaeibagha, and Xiaojiang Du. Scalable and redactable blockchain with update and anonymity. *Information Sciences*, 546:25–41.

[47] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Blockchain leveraged decentralized iot ehealth framework. *Internet of Things*, 9:100159, 2020.

[48] Zuoxia Yu, Man Ho Au, Jiangshan Yu, Rupeng Yang, Qiuliang Xu, and Wang Fat Lau. New empirical traceability analysis of cryptonote-style blockchains. In *International Conference on Financial Cryptography and Data Security*, pages 133–149. Springer, 2019.

[49] Rebekah Mercer. Privacy on the blockchain: Unique ring signatures. *arXiv preprint arXiv:1612.01188*, 2016.

[50] R Yap. Understanding how zerocoin in zcoin works and how it compares to other anonymity solutions part 1, 2017.

[51] Chaoyang Li, Yuan Tian, Xiubo Chen, and Jian Li. An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. *Information Sciences*, 546:253–264, 2020.

[52] Jon M Peha and Ildar M Khamitov. Paycash: a secure efficient internet payment system. *Electronic Commerce Research and Applications*, 3(4):381–388, 2004.

[53] Ahsan Manzoor, An Braeken, Salil S Kanhere, Mika Ylianttila, and Madhsanka Liyanage. Proxy re-encryption enabled secure and anonymous iot data sharing platform based on blockchain. *Journal of Network and Computer Applications*, page 102917, 2020.

[54] Li Peng, Wei Feng, Zheng Yan, Yafeng Li, Xiaokang Zhou, and Shohei Shimizu. Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, 2020.

[55] Abdul Rahman Taleb and Damien Vergnaud. Speeding-up verification of digital signatures. *Journal of Computer and System Sciences*, 116:22–39, 2020.

[56] Ziyu Wang, Hui Yu, Zongyang Zhang, Jiaming Piao, and Jianwei Liu. Ecdsa weak randomness in bitcoin. *Future Generation Computer*

Systems, 102:507–513, 2020.
[57] Quanyu Zhao, Siyi Chen, Zheli Liu, Thar Baker, and Yuan Zhang. Blockchain-based privacy-preserving remote data integrity checking scheme for iot information systems. *Information Processing & Management*, 57(6):102355, 2020.
[58] Cheng-Fu Chou, William C Cheng, and Leana Golubchik. Performance study of online batch-based digital signature schemes. *Journal of Network and Computer Applications*, 33(2):98–114, 2010.
[59] Markus Michels, David Naccache, Holger Petersen, et al. Gost 34.10-a brief overview of russia's dsa. *Computers and Security*, 15(8):725–732, 1996.
[60] Hiraku Morita, Jacob CN Schuldt, Takahiro Matsuda, Goichiro Hanaoka, and Tetsu Iwata. On the security of the schnorr signature scheme and dsa against related-key attacks. In *ICISC 2015*, pages 20–35. Springer, 2015.
[61] Zhanna Lyasota. A guide to digital signature algorithms-dzone security, Aug 2018.
[62] Michele Elia, Matteo Piva, and Davide Schipani. The rabin cryptosystem revisited. *Applicable Algebra in Engineering, Communication and Computing*, 26(3):251–275, 2015.
[63] Ahmad Firdaus, Mohd Faizal Ab Razak, Ali Feizollah, Ibrahim Abaker Targio Hashem, Mohamad Hazim, and Nor Badrul Anuar. The rise of "blockchain": bibliometric analysis of blockchain study. *Scientometrics*, 120(3):1289–1331, 2019.
[64] Bin Yuan, Hai Jin, Deqing Zou, Laurence Tianruo Yang, and Shui Yu. A practical byzantine-based approach for faulty switch tolerance in software-defined networks. *IEEE Transactions on Network and Service Management*, 15(2):825–839, 2018.
[65] Leila Ismail and Huned Materwala. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, 11(10):1198, 2019.
[66] Vincent Gramoli. From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems*, 2017.
[67] Amie Corso. Performance analysis of proof-of-elapsed-time (poet) consensus in the sawtooth blockchain framework. 2019.
[68] Sujit Biswas, Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P Mohanty, and Yu Wang. Pobt: A lightweight consensus algorithm for scalable iot business blockchain. *IEEE Internet of Things Journal*, 7(3):2343–2355, 2019.
[69] Saqib Hakak, Wazir Zada Khan, Gulshan Amin Gilkar, Muhammad Imran, and Nadra Guizani. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network*, 34(1):8–14, 2020.
[70] Fan Yang, Wei Zhou, QingQing Wu, Rui Long, Neal N Xiong, and Meiqi Zhou. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 7:118541–118555, 2019.
[71] Mainak Ghosh, Miles Richardson, Bryan Ford, and Rob Jansen. A torpath to torcoin: Proof-of-bandwidth altcoins for compensating relays. Technical report, NAVAL RESEARCH LAB WASHINGTON DC, 2014.
[72] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. 2018.
[73] Deepak Puthal and Saraju P Mohanty. Proof of authentication: Iot-friendly blockchains. *IEEE Potentials*, 38(1):26–29, 2018.
[74] Deepak Puthal, Saraju P Mohanty, Priyadarsi Nanda, Elias Kougianos, and Gautam Das. Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–5. IEEE, 2019.
[75] Guangsheng Yu, Xu Wang, Kan Yu, Wei Ni, J Andrew Zhang, and Ren Ping Liu. Survey: Sharding in blockchains. *IEEE Access*, 8:14155–14181, 2020.
[76] Abdelatif Hafid, Abdelhakim Senhaji Hafid, and Mustapha Samih. Scaling blockchains: A comprehensive survey. *IEEE Access*, 8:125244–125262, 2020.
[77] Huan Chen and Yijie Wang. Sschain: A full sharding protocol for public blockchain without data migration overhead. *Pervasive and Mobile Computing*, 59:101055, 2019.
[78] Shubhani Aggarwal and Neeraj Kumar. Blockchain 2.0: Smart contracts. *Advances in Computers*.
[79] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference*, pages 1–15, 2018.
[80] Tharaka Hewa, Mika Ylianttila, and Madhusanka Liyanage. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, page 102857, 2020.
[81] Faisal Jamil, Shabir Ahmad, Naeem Iqbal, and Do-Hyeun Kim. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors*, 20(8):2195, 2020.
[82] Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access*, 7:66792–66806, 2019.
[83] Shangping Wang, Yinglong Zhang, and Yaling Zhang. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access*, 6:38437–38450, 2018.
[84] Raifa Akkaoui, Xiaojun Hei, and Wenqing Cheng. Edgemedichain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access*, 8:113467–113486, 2020.
[85] QI Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.
[86] Jianli Pan, Jianyu Wang, Austin Hester, Ismail Alqerm, Yuanni Liu, and Ying Zhao. Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*, 6(3):4719–4732, 2018.
[87] Rodrigo Cubas Celiz, Yasmin Escriba De La Cruz, and David Mauricio Sanchez. Cloud model for purchase management in health sector of peru based on iot and blockchain. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 328–334. IEEE, 2018.
[88] Jingwei Liu, Xiaolu Li, Lin Ye, Hongli Zhang, Xiaojiang Du, and Mohsen Guizani. Bpds: A blockchain based privacy-preserving data sharing for electronic medical records. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.
[89] Harleen Kaur, M Afshar Alam, Roshan Jameel, Ashish Kumar Mourya, and Victor Chang. A proposed solution and future direction for

blockchain-based heterogeneous medicare data in cloud environment. *Journal of medical systems*, 42(8):156, 2018.

[90] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, 95:511–521, 2019.

[91] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):326, 2019.

[92] Lei Hang, Eunchang Choi, and Do-Hyeun Kim. A novel emr integrity management based on a medical blockchain platform in hospital. *Electronics*, 8(4):467, 2019.

[93] Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and Ferrante Neri. Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain. *Information Sciences*, 485:427–440, 2019.

[94] Junseok Park, Seongkuk Park, Kwangmin Kim, and Doheon Lee. Corus: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies. In *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 181–184. IEEE, 2018.

[95] Eman-Yasser Daraghmi, Yousef-Awwad Daraghmi, and Shyan-Ming Yuan. Medchain: a design of blockchain-based system for medical records access and permissions management. *IEEE Access*, 7:164595–164613, 2019.

[96] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, and Nan Zhang. Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 95:420–429, 2019.

[97] Md Abdur Rahman, Md Mamunur Rashid, M Shamim Hossain, Elham Hassanain, Mohammed F Alhamid, and Mohsen Guizani. Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, 7:18611–18621, 2019.

[98] Ahsan Manzoor, Madhsanka Liyanage, An Braeke, Salil S Kanhere, and Mika Ylianttila. Blockchain based proxy re-encryption scheme for secure iot data sharing. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 99–103. IEEE, 2019.

[99] Mazin Debe, Khaled Salah, Muhammad Habib Ur Rehman, and Davor Svetinovic. Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access*, 8:20118–20128, 2020.

[100] Hafiza Syeda Zainab Kazmi, Faiza Nazeer, Sahrish Mubarak, Seemab Hameed, Aliza Basharat, and Nadeem Javaid. Trusted remote patient monitoring using blockchain-based smart contracts. In *International Conference on Broadband and Wireless Computing, Communication and Applications*, pages 765–776. Springer, 2019.

[101] Vaggelis Malamas, Thomas Dasaklis, Panayiotis Kotzanikolaou, Mike Burmester, and Sokratis Katsikas. A forensics-by-design management framework for medical devices based on blockchain. In *2019 IEEE World Congress on Services (SERVICES)*, volume 2642, pages 35–40. IEEE, 2019.

[102] Yang Xu, Guojun Wang, Jidian Yang, Ju Ren, Yaoxue Zhang, and Cheng Zhang. Towards secure network computing services for lightweight clients using blockchain. *Wireless Communications and Mobile Computing*, 2018, 2018.

[103] Randa Almadhoun, Maha Kadadha, Maya Alhemeiri, Maryam Alshehhi, and Khaled Salah. A user authentication scheme of iot devices using blockchain-enabled fog nodes. In *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*, pages 1–8. IEEE, 2018.

[104] Truc DT Nguyen, Hoang-Anh Pham, and My T Thai. Leveraging blockchain to enhance data privacy in iot-based applications. In *International Conference on Computational Social Networks*, pages 211–221. Springer, 2018.

[105] P Mytis-Gkometh, G Drosatos, PS Efraimidis, and E Kaldoudi. Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In *International Conference on Biomedical and Health Informatics*, pages 69–73. Springer, 2017.

[106] Haiyang Yu, Zhen Yang, and Richard O Sinnott. Decentralized big data auditing for smart city environments leveraging blockchain technology. *IEEE Access*, 7:6288–6296, 2018.

[107] Kristen N Griggs, Olya Ossipova, Christopher P Kohlios, Alessandro N Baccarini, Emily A Howson, and Thaier Hayajneh. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42(7):130, 2018.

[108] Mohamed Baza, Mahmoud Nabil, Noureddine Lasla, Kemal Fidan, Mohamed Mahmoud, and Mohamed Abdallah. Blockchain-based firmware update scheme tailored for autonomous vehicles. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–7. IEEE, 2019.

[109] Sidra Malik, Volkan Dedeoglu, Salil S Kanhere, and Raja Jurdak. Trustchain: Trust management in blockchain and iot supported supply chains. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 184–193. IEEE, 2019.

[110] Davide Calvaresi, Valerio Mattioli, Alevtina Dubovitskaya, Aldo Franco Dragoni, and Michael Schumacher. Reputation management in multi-agent systems using permissioned blockchain technology. In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, pages 719–725. IEEE, 2018.

[111] Mazin Debe, Khaled Salah, Muhammad Habib Ur Rehman, and Davor Svetinovic. Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain. *IEEE Access*, 7:178082–178093, 2019.

[112] Said El Kafhali, Chorouk Chahir, Mohamed Hanini, and Khaled Salah. Architecture to manage internet of things data using blockchain and fog computing. In *Proceedings of the 4th International Conference on Big Data and Internet of Things*, pages 1–8, 2019.

[113] Suranjan Talukder, Shanto Roy, and Tamim Al Mahmud. A distributed anti-malware database management system using blockchain.

[114] Shailendra Rathore, Byung Wook Kwon, and Jong Hyuk Park. Blockseciotnet: Blockchain-based decentralized security architecture for iot network. *Journal of Network and Computer Applications*, 143:167–177, 2019.

[115] Claudia Pop, Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie, and Massimo Bertoncini. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors*, 18(1):162, 2018.

[116] Petar Kochovski, Sandi Gec, Vlado Stankovski, Marko Bajec, and Pavel D Drobintsev. Trust management in a blockchain based fog computing platform with trustless smart oracles. *Future Generation Computer Systems*, 101:747–759, 2019.

[117] Federico Matteo Benčić and Ivana Podnar Žarko. Distributed ledger technology: Blockchain compared to directed acyclic graph. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 1569–1570. IEEE, 2018.

[118] Vida J Morkunas, Jeannette Paschen, and Edward Boon. How blockchain technologies impact your business model. *Business Horizons*,

62(3):295–306, 2019.

[119] Rebecca Yang, Ron Wakefield, Sainan Lyu, Sajani Jayasuriya, Fengling Han, Xun Yi, Xuechao Yang, Gayashan Amarasinghe, and Shiping Chen. Public and private blockchain in construction business process and information integration. *Automation in Construction*, 118:103276, 2020.

[120] Paul Rimba, An Binh Tran, Ingo Weber, Mark Staples, Alexander Ponomarev, and Xiwei Xu. Quantifying the cost of distrust: Comparing blockchain and cloud services for business process execution. *Information Systems Frontiers*, 22(2):489–507, 2020.

[121] Amritraj Singh, Kelly Click, Reza M Parizi, Qi Zhang, Ali Dehghantanha, and Kim-Kwang Raymond Choo. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149:102471, 2020.

[122] Peilin Zheng, Zibin Zheng, Xiapu Luo, Xiangping Chen, and Xuanzhe Liu. A detailed and real-time performance monitoring framework for blockchain systems. In *2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP)*, pages 134–143. IEEE, 2018.

[123] Sergey Smetanin, Aleksandr Ometov, Mikhail Komarov, Pavel Masek, and Yevgeni Koucheryavy. Blockchain evaluation approaches: State-of-the-art and future perspective. *Sensors*, 20(12):3358, 2020.

[124] Harish Sukhwani, Nan Wang, Kishor S Trivedi, and Andy Rindos. Performance modeling of hyperledger fabric (permissioned blockchain network). In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–8. IEEE, 2018.

[125] Tien Tuan Anh Dinh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. Blockbench: A framework for analyzing private blockchains. In *Proceedings of the 2017 ACM International Conference on Management of Data*, pages 1085–1100, 2017.

[126] Sara Rouhani and Ralph Deters. Performance analysis of ethereum transactions in private blockchain. In *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pages 70–74. IEEE, 2017.

[127] Parth Thakkar, Senthil Nathan, and Balaji Viswanathan. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pages 264–276. IEEE, 2018.

[128] Arati Baliga, I Subhod, Pandurang Kamat, and Siddhartha Chatterjee. Performance evaluation of the quorum blockchain platform. *arXiv preprint arXiv:1809.03421*, 2018.

[129] Hyperledger Caliper. Hyperledger caliper architecture. *Electronic Article. url: https://hyperledger. github. io/caliper/docs/2_Architecture. html (visited on 03/10/2019)*, 2019.

[130] Benjamin Ampel, Mark Patton, and Hsinchun Chen. Performance modeling of hyperledger sawtooth blockchain. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 59–61. IEEE, 2019.

[131] Hyperledger. hyperledger/iroha.

[132] Nicholas Lee Hickson-Brown. *Prototyping und Evaluierung des Hyperledger Burrow Frameworks unter Gesichtspunkten der Usability*. PhD thesis, Universität Hamburg, 2019.

[133] Zhongli Dong, Emma Zheng, Young Choon, and Albert Y Zomaya. Dagbench: A performance evaluation framework for dag distributed ledgers. In *2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*, pages 264–271. IEEE, 2019.

[134] M Divya and Nagaveni B Biradar. Iota-next generation block chain. *International journal of engineering and computer science*, 7(04):23823–23826, 2018.

[135] Anton Churyumov. Byteball: A decentralized system for storage and transfer of value. *URL https://byteball. org/Byteball. pdf*, 2016.

[136] Maher Alharby and Aad van Moorsel. Blocksim: a simulation framework for blockchain systems. *ACM SIGMETRICS Performance Evaluation Review*, 46(3):135–138, 2019.

[137] Santosh Pandey, Gopal Ojha, Bikesh Shrestha, and Rohit Kumar. Blocksim: A practical simulation tool for optimal network design, stability and planning. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 133–137. IEEE, 2019.

[138] Manuel Zander, Tom Waite, and Dominik Harz. Dagsim: Simulation of dag-based distributed ledger protocols. *ACM SIGMETRICS Performance Evaluation Review*, 46(3):118–121, 2019.

[139] Wellington Fernandes Silvano and Roderval Marcelino. Iota tangle: A cryptocurrency to communicate internet of things data. *Future Generation Computer Systems*, 2020.

[140] Julie Frizzo-Barker, Peter A Chow-White, Philippa R Adams, Jennifer Mentanko, Dung Ha, and Sandy Green. Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 2019.

[141] Yining Hu, Madhusanka Liyanage, Ahsan Mansoor, Kanchana Thilakarathna, Guillaume Jourjon, and Aruna Seneviratne. Blockchain-based smart contracts-applications and challenges. *arXiv preprint arXiv:1810.04699*, 2018.

[142] Umesh Bodkhe, Sudeep Tanwar, Karan Parekh, Pimal Khanpara, Sudhanshu Tyagi, Neeraj Kumar, and Mamoun Alazab. Blockchain for industry 4.0: A comprehensive review. *IEEE Access*, 8:79764–79800, 2020.

[143] Sudeep Tanwar, Karan Parekh, and Richard Evans. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50:102407, 2020.

[144] Fei Lin and Minqian Qiang. The challenges of existence, status, and value for improving blockchain. *IEEE Access*, 7:7747–7758, 2018.

[145] Soohyeong Kim, Yongseok Kwon, and Sunghyun Cho. A survey of scalability solutions on blockchain. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1204–1207. IEEE, 2018.

[146] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[147] Abdul Jabbar and Samir Dani. Investigating the link between transaction and computational costs in a blockchain environment. *International Journal of Production Research*, 58(11):3423–3436, 2020.

[148] Muhammad Kamran, Hikmat Ullah Khan, Wasif Nisar, Muhammad Farooq, and Saeed-Ur Rehman. Blockchain and internet of things: A bibliometric study. *Computers & Electrical Engineering*, 81:106525, 2020.

[149] Khaled Salah, M Habib Ur Rehman, Nishara Nizamuddin, and Ala Al-Fuqaha. Blockchain for ai: Review and open research challenges. *IEEE Access*, 7:10127–10149, 2019.

[150] Hao Jin, Yan Luo, Peilong Li, and Jomol Mathew. A review of secure and privacy-preserving medical data sharing. *IEEE Access*, 7:61656–

61669, 2019.

[151] Fondazione Bruno Kessler. Basic: Towards a blockchained agent-based simulator for cities. *Massively Multi-Agent Systems II*, page 144.

[152] Josh Constine. Former employees say lyft staffers spied on passengers, Jan 2018.

[153] Lingjun Fan, J Ramon Gil-Garcia, Derek Werthmuller, G Brian Burke, and Xuehai Hong. Investigating blockchain as a data management tool for iot devices in smart city initiatives. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pages 1–2, 2018.

[154] Parminder Singh, Anand Nayyar, Avinash Kaur, and Uttam Ghosh. Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet*, 12(4):61, 2020.

[155] Haoyu Wang, Lina Wang, Zhichao Zhou, Xueqiang Tao, Giovanni Pau, and Fabio Arena. Blockchain-based resource allocation model in fog computing. *Applied Sciences*, 9(24):5538, 2019.

[156] Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, Reji Thomas, and Tai-Hoon Kim. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. *IEEE Internet of Things Journal*, 6(4):6835–6842, 2019.

[157] Sibylle Schaller and Dave Hood. Software defined networking architecture standardization. *Computer standards & interfaces*, 54:197–202, 2017.

[158] Rajat Chaudhary, Anish Jindal, Gagangeet Singh Aujla, Shubhani Aggarwal, Neeraj Kumar, and Kim-Kwang Raymond Choo. Best: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system. *Computers & Security*, 85:288–299, 2019.

[159] Pradip Kumar Sharma, Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Communications Magazine*, 55(9):78–85, 2017.

[160] Pradip Kumar Sharma, Shailendra Rathore, Young-Sik Jeong, and Jong Hyuk Park. Softedgenet: Sdn based energy-efficient distributed network architecture for edge computing. *IEEE Communications magazine*, 56(12):104–111, 2018.

[161] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine, and Rachid Benlamri. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences*, 9(9):1736, 2019.

[162] Marko Hölbl, Marko Kompara, Aida Kamišalić, and Lili Nemec Zlatolas. A systematic review of the use of blockchain in healthcare. *Symmetry*, 10(10):470, 2018.

[163] Hai-Trieu Pham and Pubudu N Pathirana. Measurement and assessment of hand functionality via a cloud-based implementation. In *International Conference on Smart Homes and Health Telematics*, pages 289–294. Springer, 2015.

[164] Saiyi Li and Pubudu N Pathirana. Cloud-based non-invasive tele-rehabilitation exercise monitoring. In *2014 IEEE Conference on Biomedical Engineering and Sciences (IECBES)*, pages 385–390. IEEE, 2014.

[165] Hyperledger caliper, Apr 2020.

[166] Antonio Celesti, Armando Ruggeri, Maria Fazio, Antonino Galletta, Massimo Villari, and Agata Romano. Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital iot clouds. *Sensors*, 20(9):2590, 2020.

[167] Geetanjali Rathee, Ashutosh Sharma, Hemraj Saini, Rajiv Kumar, and Razi Iqbal. A hybrid framework for multimedia data processing in iot-healthcare using blockchain technology. *Multimedia Tools and Applications*, pages 1–23, 2019.

[168] Ijazul Haq and Olivier Museleme Esuka. Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. *Int. J. Comput. Appl.*, 180(25):8–12, 2018.

[169] Dinh C Nguyen, Khoa D Nguyen, and Pubudu N Pathirana. A mobile cloud based iomt framework for automated health assessment and management. In *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 6517–6520. IEEE, 2019.

[170] Minhee Kang, Eunkyoung Park, Baek Hwan Cho, and Kyu-Sung Lee. Recent patient health monitoring platforms incorporating internet of things-enabled smart devices. *International neurourology journal*, 22(Suppl 2):S76, 2018.

[171] Sharyl J Nass, Laura A Levit, Lawrence O Gostin, et al. The value and importance of health information privacy. In *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. National Academies Press (US), 2009.

[172] Yogachandran Rahulamathavan, Raphael C-W Phan, Muttukrishnan Rajarajan, Sudip Misra, and Ahmet Kondoz. Privacy-preserving blockchain based iot ecosystem using attribute-based encryption. In *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6. IEEE, 2017.

[173] Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, and Danyi Li. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–5. IEEE, 2017.

[174] Weiquan Ni, Xumin Huang, Junxing Zhang, and Rong Yu. Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In *2019 Chinese Control Conference (CCC)*, pages 6333–6338. IEEE, 2019.

[175] Daisuke Ichikawa, Makiko Kashiyama, and Taro Ueno. Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth*, 5(7):e111, 2017.

[176] Nafiseh Kahani, Khalid Elgazzar, and James R Cordy. Authentication and access control in e-health systems in the cloud. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pages 13–23. IEEE, 2016.

[177] Shuo Lu, Yuan Hong, Qian Liu, Lingyu Wang, and Rachida Dssouli. Access control in e-health portal systems. In *2007 Innovations in Information Technologies (IIT)*, pages 88–92. IEEE, 2007.

[178] SM Riazul Islam, Mahmud Hossain, Ragib Hasan, and Trung Q Duong. A conceptual framework for an iot-based health assistant and its authorization model. In *2018 IEEE 8th annual computing and communication workshop and conference (CCWC)*, pages 616–621. IEEE, 2018.

[179] Vidhya Ramani, Tanesh Kumar, An Bracken, Madhusanka Liyanage, and Mika Ylianttila. Secure and efficient data accessibility in blockchain based healthcare systems. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 206–212. IEEE, 2018.

[180] Hao Wang and Yujiao Song. Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, 42(8):152, 2018.

[181] Luca Marelli, Elisa Lievevrouw, and Ine Van Hoyweghen. Fit for purpose? the gdpr and the governance of european digital health. *Policy studies*, 41(5):447–467, 2020.

[182] Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. Blockchain-based personal health data sharing system using cloud storage. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6. IEEE, 2018.

[183] Thomas Hepp, Matthew Sharinghousen, Philip Ehret, Alexander Schoenhals, and Bela Gipp. On-chain vs. off-chain storage for supply-and blockchain integration. *it-Information Technology*, 60(5-6):283–291, 2018.

[184] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE International Conference on Software Architecture (ICSA)*, pages 243–252. IEEE, 2017.

[185] Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li, and Gaoping Li. A blockchain-based medical data sharing and protection scheme. *IEEE Access*, 7:118943–118953, 2019.

[186] Qi Xia, Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang. Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2):44, 2017.

[187] Yiwen Du, Jianwei Liu, Zhenyu Guan, and Hanwen Feng. A medical information service platform based on distributed cloud and blockchain. In *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, pages 34–39. IEEE, 2018.

[188] Bingqing Shen, Jingzhi Guo, and Yilong Yang. Medchain: efficient healthcare data sharing via blockchain. *Applied sciences*, 9(6):1207, 2019.

[189] Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li, and Yintang Yang. Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42(8):136, 2018.

[190] Zahra Kavosi, Hamed Rahimi, Saeideh Khanian, Payam Farhadi, and Erfan Kharazmi. Factors influencing decision making for healthcare services outsourcing: A review and delphi study. *Medical journal of the Islamic Republic of Iran*, 32:56, 2018.

[191] Heather Skipworth, Emanuela Delbufalo, and Carlos Mena. Logistics and procurement outsourcing in the healthcare sector: a comparative analysis. *European Management Journal*, 2020.

[192] Hanlin Zhang, Jia Yu, Chengliang Tian, Pu Zhao, Guobin Xu, and Jie Lin. Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing. *IEEE Access*, 6:40713–40722, 2018.

[193] Saide Zhu, Zhipeng Cai, Huafu Hu, Yingshu Li, and Wei Li. zkcrowd: a hybrid blockchain-based crowdsourcing platform. *IEEE Transactions on Industrial Informatics*, 16(6):4196–4205, 2019.

[194] Xiaolong Xu, Qingxiang Liu, Xuyun Zhang, Jie Zhang, Lianyong Qi, and Wanchun Dou. A blockchain-powered crowdsourcing method with privacy preservation in mobile environment. *IEEE Transactions on Computational Social Systems*, 6(6):1407–1419, 2019.

[195] Ming Li, Jian Weng, Anjia Yang, Wei Lu, Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, and Robert H Deng. Crowdbc: A blockchain-based decentralized framework for crowdsourcing. *IEEE Transactions on Parallel and Distributed Systems*, 30(6):1251–1266, 2018.

[196] Daniel Macrinici, Cristian Cartofeanu, and Shang Gao. Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35(8):2337–2354, 2018.

[197] Yinqiu Liu, Kun Wang, Yun Lin, and Wenyao Xu. A lightweight blockchain system for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 15(6):3571–3581, 2019.

[198] Leila Ismail, Huned Materwala, and Sherali Zeadally. Lightweight blockchain for healthcare. *IEEE Access*, 7:149935–149951, 2019.

[199] Gautam Srivastava, Jorge Crichigno, and Shalini Dhar. A light and secure healthcare blockchain for iot medical devices. In *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*, pages 1–5. IEEE, 2019.

[200] Oumaima Attia, Ines Khoufi, Anis Laouiti, and Cedric Adjih. An iot-blockchain architecture based on hyperledger framework for healthcare monitoring application. In *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2019.

[201] Jinhong Yang, Md Mehedi Hassan Onik, Nam-Yong Lee, Mohiuddin Ahmed, and Chul-Soo Kim. Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. *Applied Sciences*, 9(7):1370, 2019.

[202] Gautam Srivastava, Ashutosh Dhar Dwivedi, and Rajani Singh. Automated remote patient monitoring: data sharing and privacy using blockchain. *arXiv preprint arXiv:1811.03417*, 2018.

[203] Huige Li, Haibo Tian, Fangguo Zhang, and Jiejie He. Blockchain-based searchable symmetric encryption scheme. *Computers & Electrical Engineering*, 73:32–45, 2019.

[204] Shengshan Hu, Chengjun Cai, Qian Wang, Cong Wang, Xiangyang Luo, and Kui Ren. Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 792–800. IEEE, 2018.

[205] Yong Wang, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain. *IEEE Access*, 7:136704–136719, 2019.

[206] YANG Xiaodong, LI Ting, LIU Rui, and WANG Meiding. Blockchain-based secure and searchable ehr sharing scheme. In *2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, pages 822–8223. IEEE, 2019.

[207] Si-Wan Noh, Youngho Park, Chur Sur, Sang-Uk Shin, and Kyung-Hyune Rhee. Blockchain-based user-centric records management system. *Int J Control Autom*, 10(11):133–144, 2017.

[208] Naveed Islam, Yasir Faheem, Ikram Ud Din, Muhammad Talha, Mohsen Guizani, and Mudassir Khalil. A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services. *Future Generation Computer Systems*, 100:569–578, 2019.

[209] Ammar Awad Mutlag, Mohd Khanapi Abd Ghani, Net al Arunkumar, Mazin Abed Mohammed, and Othman Mohd. Enabling technologies for fog computing in healthcare iot systems. *Future Generation Computer Systems*, 90:62–78, 2019.

[210] Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. Privacy-preserved task offloading in mobile blockchain with deep

reinforcement learning. *arXiv preprint arXiv:1908.07467*, 2019.

[211] Lei Hang, Israr Ullah, and Do-Hyeun Kim. A secure fish farm platform based on blockchain for agriculture data integrity. *Computers and Electronics in Agriculture*, 170:105251, 2020.

[212] Yinghui Zhang, Robert H Deng, Ximeng Liu, and Dong Zheng. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Information Sciences*, 462:262–277, 2018.

[213] Davide Calvaresi, Alevtina Dubovitskaya, Jean Paul Calbimonte, Kuldar Taveter, and Michael Schumacher. Multi-agent systems and blockchain: Results from a systematic literature review. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pages 110–126. Springer, 2018.

[214] Botta Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. On the integration of cloud computing and internet of things. In *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on. IEEE*, 2014.

[215] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454–1464, 2017.

[216] Mehdi Sookhak, Helen Tang, Ying He, and F Richard Yu. Security and privacy of smart cities: a survey, research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(2):1718–1743, 2018.

[217] Rourab Paul, Paresh Baidya, Suman Sau, Krishanu Maity, Satyabrata Maity, and Sudhendu B Mandal. Iot based secure smart city architecture using blockchain. In *2018 2nd International Conference on Data Science and Business Analytics (ICDSBA)*, pages 215–220. IEEE, 2018.

[218] Maha AbuNaser and Ahmad AA 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)*, pages 58–62. IEEE, 2019.

[219] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen 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)*, pages 618–623. IEEE, 2017.

[220] Saurabh Singh, In-Ho Ra, Weizhi Meng, Maninder Kaur, and Gi Hwan 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*, 15(4):1550147719844159, 2019.

[221] Jingting Xue, Chunxiang Xu, and Yuan Zhang. Private blockchain-based secure access control for smart home systems. *KSII Transactions on Internet & Information Systems*, 12(12), 2018.

[222] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, and Sukumar Nandi. Managing smart home appliances with proof of authority and blockchain. In *International Conference on Innovations for Community Services*, pages 221–232. Springer, 2019.

[223] Jawad Ali, Ahmad Shahrafidz Khalid, Eiad Yafi, Shahrulniza Musa, and Waqas Ahmed. Towards a secure behavior modeling for iot networks using blockchain. *arXiv preprint arXiv:2001.01841*, 2020.

[224] Younghun Lee, Shailendra Rathore, Jin Ho Park, and Jong Hyuk Park. A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences*, 10(1):1–14, 2020.

[225] Bo Yin, Lishi Mei, Zexun Jiang, and Kai Wang. Joint cloud collaboration mechanism between vehicle clouds based on blockchain. In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, pages 227–2275. IEEE, 2019.

[226] Hong Liu, Yan Zhang, and Tao Yang. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Network*, 32(3):78–83, 2018.

[227] Sara Nadeem, Muhammad Rizwan, Fahad Ahmad, and Jaweria Manzoor. Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, 10(1):288–295, 2019.

[228] Lixia Xie, Ying Ding, Hongyu Yang, and Xinmu Wang. Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets. *IEEE Access*, 7:56656–56666, 2019.

[229] Alejandro Ranchal Pedrosa and Giovanni Pau. Chargeltup: On blockchain-based technologies for autonomous vehicles. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pages 87–92, 2018.

[230] Meng Li, Liehuang Zhu, and Xiaodong Lin. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet of Things Journal*, 6(3):4573–4584, 2018.

[231] Yingying Yao, Xiaolin Chang, Jelena Mišić, Vojislav B Mišić, and Lin Li. Bla: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. *IEEE Internet of Things Journal*, 6(2):3775–3784, 2019.

[232] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks. *IEEE Internet of Things Journal*, 7(5):4278–4291, 2019.

[233] Rasheed Hussain, Fatima Hussain, and Sherali Zeadally. Integration of vanet and 5g security: A review of design and implementation issues. *Future Generation Computer Systems*, 101:843–864, 2019.

[234] Vikas Hassija, Vikas Saxena, Vinay Chamola, and Richard Yu. A parking slot allocation framework based on virtual voting and adaptive pricing algorithm. *IEEE Transactions on Vehicular Technology*, 2020.

[235] Vikas Hassija, Vinay Chamola, Sahil Garg, Nanda Gopala Krishna Dara, Georges Kaddoum, and Dushantha Nalin K Jayakody. A blockchain-based framework for lightweight data sharing and energy trading in v2g network. *IEEE Transactions on Vehicular Technology*, 2020.

[236] Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and Mamoun Alazab. Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology*, 69(8):9097–9111, 2020.

[237] Vikas Hassija, Vatsal Gupta, Sahil Garg, and Vinay Chamola. Traffic jam probability estimation based on blockchain and deep neural networks. *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[238] Sujit Biswas, Kashif Sharif, Fan Li, Boubakr Nour, and Yu Wang. A scalable blockchain framework for secure transactions in iot. *IEEE Internet of Things Journal*, 6(3):4650–4659, 2018.

[239] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access*, 6:32700–32726, 2018.

[240] Pasquale De Meo, Fabrizio Messina, Domenico Rosaci, and Giuseppe ML Sarné. Recommending users in social networks by integrating local and global reputation. In *International Conference on Internet and Distributed Computing Systems*, pages 437–446. Springer, 2014.

[241] Giancarlo Fortino, Fabrizio Messina, Domenico Rosaci, and Giuseppe ML Sarne. Using blockchain in a reputation-based model for grouping agents in the internet of things. *IEEE Transactions on Engineering Management*, 2019.

[242] Mehran Pourvahab and Gholamhossein Ekbatanifard. An efficient forensics architecture in software-defined networking-iot using blockchain technology. *IEEE Access*, 7:99573–99588, 2019.

[243] ASM Sanwar Hosen, Saurabh Singh, Pradip Kumar Sharma, Uttam Ghosh, Jin Wang, In-Ho Ra, and Gi Hwan Cho. Blockchain-based transaction validation protocol for a secure distributed iot network. *IEEE Access*, 2020.

[244] Ammar Muthanna, Abdelhamied A Ateya, Abdukodir Khakimov, Irina Gudkova, Abdelrahman Abuarqoub, Konstantin Samouylov, and Andrey Koucheryavy. Secure iot network structure based on distributed fog computing, with sdn/blockchain. 2019.

[245] Ying Gao, Yijian Chen, Hongliang Lin, and Joel JPC Rodrigues. Blockchain based secure iot data sharing framework for sdn-enabled smart communities. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 514–519. IEEE, 2020.

[246] Sudip Misra, Pallav Kumar Deb, Nidhi Pathak, and Anandarup Mukherjee. Blockchain-enabled sdn for securing fog-based resource-constrained iot. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 490–495. IEEE, 2020.

[247] Peiying Zhang, Fanglin Liu, Neeraj Kumar, and Gagangeet Singh Aujla. Information classification strategy for blockchain-based secure sdn in iot scenario. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1081–1086. IEEE, 2020.

[248] Phan The Duy, Hien Do Hoang, Nguyen Ba Khanh, Van-Hau Pham, et al. Sdnlog-foren: Ensuring the integrity and tamper resistance of log files for sdn forensics using blockchain. In *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, pages 416–421. IEEE, 2019.

[249] Darshan Vishwasrao Medhane, Arun Kumar Sangaiah, M Shamim Hossain, Ghulam Muhammad, and Jin Wang. Blockchain-enabled distributed security framework for next generation iot: An edge-cloud and software defined network integrated approach. *IEEE Internet of Things Journal*, 2020.

[250] Zakaria Abou El Houda, Abdelhakim Hafid, and Lyes Khoukhi. Co-iot: A collaborative ddos mitigation scheme in iot environment based on blockchain using sdn. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[251] Vikas Hassija, Vikas Saxena, and Vinay Chamola. A mobile data offloading framework based on a combination of blockchain and virtual voting. *Software: Practice and Experience*, 2020.

[252] Zehui Xiong, Yang Zhang, Dusit Niyato, Ping Wang, and Zhu Han. When mobile blockchain meets edge computing. *IEEE Communications Magazine*, 56(8):33–39, 2018.

[253] Yutao Jiao, Ping Wang, Dusit Niyato, and Kongrath Suankaewmanee. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. *IEEE Transactions on Parallel and Distributed Systems*, 30(9):1975–1989, 2019.

[254] Wenda Tang, Xuan Zhao, Wajid Rafique, and Wanchun Dou. A blockchain-based offloading approach in fog computing environment. In *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, pages 308–315. IEEE, 2018.

[255] Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning. *IEEE Transactions on Network and Service Management*, 2020.

[256] Zainib Noshad, Atia Javaid, Maheen Zahid, Ishtiaq Ali, Nadeem Javaid, et al. Node recovery in wireless sensor networks via blockchain. In *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pages 94–105. Springer, 2019.

[257] Abbas Yazdinejad, Reza M Parizi, Gautam Srivastava, Ali Dehghantanha, and Kim-Kwang Raymond Choo. Energy efficient decentralized authentication in internet of underwater things using blockchain. In *2019 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2019.

[258] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasurbramanian. A lightweight blockchain based framework for underwater iot. *Electronics*, 8(12):1552, 2019.

[259] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. A detailed analysis of the kdd cup 99 data set. In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*, pages 1–6. IEEE, 2009.

[260] Rekha Goyat, Gulshan Kumar, Rahul Saha, Mauro Conti, Mritunjay Kumar Rai, Reji Thomas, Mamoun Alazab, and Tai Hoon-Kim. Blockchain-based data storage with privacy and authentication in internet-of-things. *IEEE Internet of Things Journal*, 2020.

[261] Hendrik L Cech, Marcel Großmann, and Udo R Krieger. A fog computing architecture to share sensor data by means of blockchain functionality. In *2019 IEEE International Conference on Fog Computing (ICFC)*, pages 31–40. IEEE, 2019.

[262] Xiaoyang Zhu and Youakim Badr. Fog computing security architecture for the internet of things using blockchain-based social networks. 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)*, pages 1361–1366. IEEE, 2018.

[263] Omaji Samuel, Nadeem Javaid, Muhammad Awais, Zeeshan Ahmed, Muhammad Imran, and Mohsen Guizani. A blockchain model for fair data sharing in deregulated smart grids. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2019.

[264] Vikas Hassija, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, 2020.

[265] Sidra Malik, Salil S Kanhere, and Raja Jurdak. Productchain: Scalable blockchain framework to support provenance in supply chains. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–10. IEEE, 2018.

[266] Simone Figorilli, Francesca Antonucci, Corrado Costa, Federico Pallottino, Luciano Raso, Marco Castiglione, Edoardo Pinci, Davide

Del Vecchio, Giacomo Colle, Andrea Rosario Proto, et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain. *Sensors*, 18(9):3133, 2018.

[267] Rafael Martínez-Peláez, Homero Toral-Cruz, Jorge R Parra-Michel, Vicente García, Luis J Mena, Vanessa G Félix, and Alberto Ochoa-Brust. An enhanced lightweight iot-based authentication scheme in cloud computing circumstances. *Sensors*, 19(9):2098, 2019.

[268] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, and Wayne Chiu. Lightweight iot-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, 91:244–251, 2019.

[269] Mingxin Ma, Guozhen Shi, and Fenghua Li. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. *IEEE Access*, 7:34045–34059, 2019.

[270] Zijian Bao, Wenbo Shi, Debiao He, and Kim-Kwang Raymond Chood. Iotchain: A three-tier blockchain-based iot security architecture. *arXiv preprint arXiv:1806.02008*, 2018.

[271] Tai-Hoon Kim, Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, William J Buchanan, Reji Thomas, and Mamoun Alazab. A privacy preserving distributed ledger framework for global human resource record management: The blockchain aspect. *IEEE Access*, 2020.

[272] Andreas Seitz, Dominic Henze, Daniel Miehle, Bernd Bruegge, Jochen Nickles, and Markus Sauer. Fog computing as enabler for blockchain-based iiot app marketplaces-a case study. In *2018 Fifth international conference on internet of things: systems, management and security*, pages 182–188. IEEE, 2018.

[273] Haifeng Yu, Phillip B Gibbons, Michael Kaminsky, and Feng Xiao. Sybillimit: A near-optimal social network defense against sybil attacks. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 3–17. IEEE, 2008.

[274] Rijo Jackson Tom, Suresh Sankaranarayanan, and Joel JPC Rodrigues. Agent negotiation in an iot-fog based power distribution system for demand reduction. *Sustainable Energy Technologies and Assessments*, 38:100653, 2020.

[275] Karima Qayumi. Multi-agent based intelligence generation from very large datasets. In *2015 IEEE International Conference on Cloud Engineering*, pages 502–504. IEEE, 2015.

[276] Fengji Luo, Zhao Yang Dong, Gaoqi Liang, Junichi Murata, and Zhao Xu. A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain. *IEEE Transactions on Power Systems*, 34(5):4097–4108, 2018.

[277] Jhim Kiel M Verame. *Helping users adopt and delegate agency to autonomous agents in everyday life*. PhD thesis, University of Southampton, 2018.

[278] Alex Norta, Anis Ben Othman, and Kuldar Taveter. Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration. In *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, pages 244–257, 2015.

[279] Shi-Cho Cha, Jyun-Fu Chen, Chunhua Su, and Kuo-Hui Yeh. A blockchain connected gateway for ble-based devices in the internet of things. *IEEE Access*, 6:24639–24649, 2018.

[280] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Blockchain leveraged task migration in body area sensor networks. In *2019 25th Asia-Pacific Conference on Communications (APCC)*, pages 177–184. IEEE, 2019.

[281] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. Dynamically recommending repositories for health data: a machine learning model. In *Proceedings of the Australasian Computer Science Week Multiconference*, pages 1–10, 2020.

[282] Rakesh Shrestha and Shiho Kim. Integration of iot with blockchain and homomorphic encryption: Challenging issues and opportunities. In *Advances in Computers*, volume 115, pages 293–331. Elsevier, 2019.

[283] Latif U Khan, Walid Saad, Zhu Han, Ekram Hossain, and Choong Seon Hong. Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *arXiv preprint arXiv:2009.13012*, 2020.

[284] Lawrence Lessig. The law of the horse: What cyberlaw might teach. *Harvard law review*, 113(2):501–549, 1999.

[285] Hany F Atlam, Ahmed Alenezi, Madini O Alassafi, and Gary Wills. Blockchain with internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications*, 10(6):40–48, 2018.

[286] Shreshth Tuli, Shikhar Tuli, Gurleen Wander, Praneet Wander, Sukhpal Singh Gill, Schahram Dustdar, Rizos Sakellariou, and Omer Rana. Next generation technologies for smart healthcare: Challenges, vision, model, trends and future directions. *Internet Technology Letters*, page e145, 2019.

[287] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. A decentralized patient agent controlled blockchain for remote patient monitoring. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–8. IEEE, 2019.

[288] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. Blockchain for internet of things: A survey. *IEEE Internet of Things Journal*, 6(5):8076–8094, 2019.

[289] Cas JF Cremers. The scyther tool: Verification, falsification, and analysis of security protocols. In *International Conference on Computer Aided Verification*, pages 414–418. Springer, 2008.

[290] Ke Gu, Lihao Yang, and Bo Yin. Location data record privacy protection based on differential privacy mechanism. In *ITC*, volume 47, pages 639–654, 2018.

[291] Adel Noureddine, Syed Islam, and Rabih Bashroush. Jolinar: analysing the energy footprint of software applications. In *Proceedings of the 25th International Symposium on Software Testing and Analysis*, pages 445–448. ACM, 2016.

[292] Saravanan Krishnan, Valentina Emilia Balas, Julie Golden, Y Harold Robinson, S Balaji, and Raghvendra Kumar. *Handbook of Research on Blockchain Technology*. Academic Press, 2020.

[293] Vinay Chamola, Vikas Hassija, Vatsal Gupta, and Mohsen Guizani. A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. *IEEE Access*, 8:90225–90265, 2020.

[294] Andrew Hard, Kanishka Rao, Rajiv Mathews, Swaroop Ramaswamy, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. Federated learning for mobile keyboard prediction. *arXiv preprint arXiv:1811.03604*, 2018.

[295] Junfeng Xie, F Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, Chenmeng Wang, and Yunjie Liu. A survey of machine learning techniques applied to software defined networking (sdn): Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(1):393–430,

2018.

[296] Peter Yeoh. Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, 2017.

[297] Samer Hassan and Primavera De Filippi. The expansion of algorithmic governance: from code is law to law is code. *Field Actions Science Reports. The journal of field actions*, (Special Issue 17):88–90, 2017.

[298] NN Pokrovskaia. Tax, financial and social regulatory mechanisms within the knowledge-driven economy. blockchain algorithms and fog computing for the efficient regulation. In *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*, pages 709–712. IEEE, 2017.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Md Ashraf Uddin

Internet Commerce Security Laboratory

Federation University Australia