International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 1, February 2023, pp. 718~735
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i1.pp718-735

Blockchain technology and internet of things: review, challenge and security concern

Mahmood Subhy Mahmood[1], Najla Badie Al Dabagh[2]
[1]College of Science, University of Mosul, Mosul, Iraq
[2]College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

Article Info

Article history:

Received Dec 8, 2021
Revised Jul 14, 2022
Accepted Aug 19, 2022

Keywords:

Blockchain
Blockchain attacks
Blockchain with internet of things
Consensus algorithms
Mining

ABSTRACT

Blockchain (BC) has received high attention from many researchers recently because it has decentralization, trusted auditability, and transparency as its main properties. BC has contributed fundamentally to the development of applications like cryptocurrencies, health care, the internet of things (IoT), and so on. The IoT is envisioned to include billions of pervasive and mission-critical sensors and actuators connected to the internet. This network of smart devices is expected to generate and have access to vast amounts of information, creating unique opportunities for new applications, but significant security and privacy issues emerge concurrently because it does not contain robust security systems. BC provides many services like privacy, security, and provenance to the systems that depends on. This research includes analyzing and a comprehensive review of BC technologies. Moreover, the proposed solutions in academia with the methodologies that used to integrate blockchain with IoT are presented. Also, the types of attacks on blockchain are collected and classified. Furthermore, the main contributions and challenges that are included in the literature are explored, then the relevant recommendations for solving the explored challenges are proposed. In conclusion, the integration of BC with IoT could produce promising results in enhancing the security and privacy of IoT environment.

Corresponding Author:

Mahmood Subhy Mahmood
College of Science, University of Mosul
Mosul, Iraq
Email: mahmoodsubhy1981@gmail.com

1. INTRODUCTION

Nowadays, cryptocurrency plays an important role in academia and industry domains. Bitcoin considers one of the most common cryptocurrencies which has gained a substantial success with its investment market represented by 220 billion dollars in 2020. It is estimated that it could reach 3 trillion market caps by 2025 as shown in Figure 1 [1].

With a special structure of data storing, transactions in Bitcoin could occur in a decentralized manner and the essential technology to create Bitcoin is the blockchain [2]. Blockchain technology is defined as "a distributed ledger technology (DLT), which secures and records transactions in a peer to peer (P2P) network instead of using single or numerous servers" [3]. When any malicious or hacker attempts to the delete or alter the data stored in a blockchain, this action can be detected because there are multiple replicas of the same ledger distributed over several locations [3]. Commonly, the blockchain has the following characteristics (persistency, decentralization, auditability, anonymity, and redundancy). With these characteristics, blockchain can really improve the efficiency and save the cost associated with developing the applications based on it [2], [3]. Blockchain use-cases tried to explore in different applications such as

financial services, legal services, health care, manufacturing, supply chain, retail services, transport and tourism, and governments [3], [4].

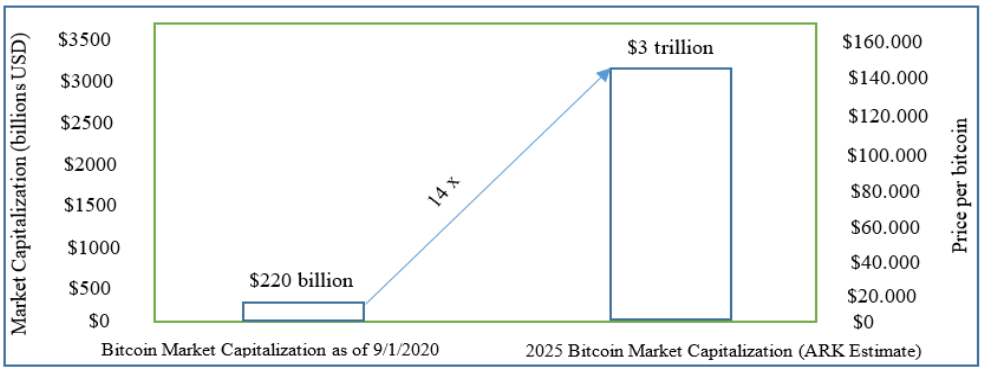

Figure 1. Sizing bitcoin's opportunity [5]

The blockchain provides several services to systems that depend on it like security, privacy, provenance and others. Currently, these services are provided to the internet of things (IoT) by reliable brokers or by using incompetent distributed methods. So, security and privacy are the highest challenge for existing IoT applications. Alternatively, the blockchain technology can offer security promises to resolve the traditional challenges that mentioned above. Furthermore, it is offering a provably secure, fully distributed and consensus solutions. Although, the blockchain has infinite potential for building the upcoming internet systems such as IoT, it is facing several technical challenges such as scalability, mining in restricted resource, blockchain operations which produce overhead traffic with limited-bandwidth in IoT devices [2].

Network of the IoT includes smart devices that produce, process, and interchange massive quantities of sensitive information. It will become attractive targets of many cyber-attacks [5]. The security and privacy hazards of IoT are exacerbated by the absence of fundamental security defenses in many of the first generation of IoT products. Various security vulnerabilities have been recognized in connected devices such as vehicles, smart locks [6] and smart home [7].

Several essential features of IoT increase its privacy and security challenges including: context-aware and situational nature of risks, heterogeneity, attacks, and scale [8]. Traditional blockchain is unsuitable for the IoT, because of IoT devices regularly want to operate with less bandwidth and computational power consumption. In addition to that, blockchain (BC) is considered the initial phase of development. Therefore, various researches in this domain are applied to enhance its efficiency [4]. Investigation of privacy and security for IoT by utilizing blockchain technology is getting a lot of attention in the research community as we will discuss later.

In this paper, the essential contributions are demonstrated: i) all the blockchain's fundamentals and architecture have been explained in details, ii) blockchain attacks have been listed and summarized, iii) the role of blockchain in IoT is to encounter security and privacy challenges and solutions have been discussed. The rest of this paper includes: section 2, which shows the blockchain's fundamentals that include (architecture, "pros and cons," challenges, types, attacks and applications of blockchain technology). Section 3 discusses the integration of blockchain with IoT. From the other hand, section 4 includes the conclusion and future works.

2. BLOCKCHAIN TECHNOLOGY

In this section, the architecture of blockchain is explained. Consensus algorithms, platforms and types are presented. Also, pros and cons, challenges and applications have been investigated.

2.1. Blockchain architecture

A blockchain technology consists of a network of nodes and a database, as shown in Figure 2. A blockchain database is a distributed ledger, shared, append-only, fault-tolerant which involve certain numbers of the transactions (i.e. transaction is a data unit on the BC) in blocks. While the blocks are shared by all nodes in the blockchain, users cannot be altered or deleted. Blocks that are verified are linked together in a chain by using cryptographic hash value and every block has a hash value of the previous block. Each block holds some of confirmed transactions. Moreover, each block includes a timestamp that signifies the time of

the block creation and (nonce) a random value for cryptographic tasks. The blockchain network includes nodes, which are distributed in a peer-to- peer manner [8].

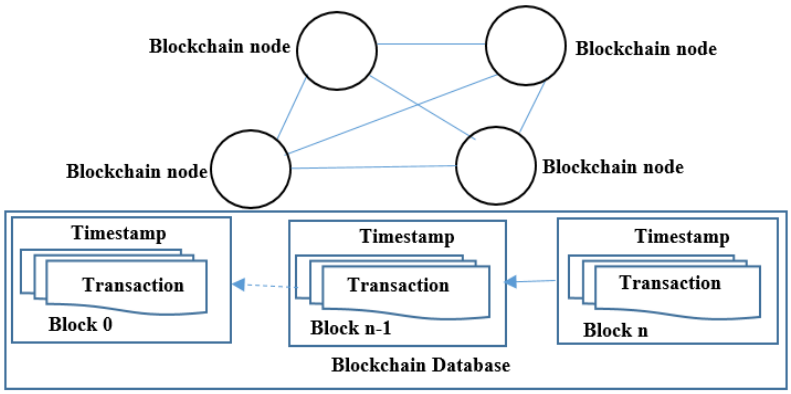

Figure 2. Blockchain network, database, blocks, and transactions [9]

2.1.1. Building blocks of blockchain

Many methods are used to build the blocks of blockchain. Asymmetric-key cryptography, digital signature, cryptographic hash function and others, are all explained. The following subsections include the details of these methods.

a. Asymmetric-key cryptography

Asymmetric-key cryptography utilizes a couples of keys: private and public keys that are related to each other mathematically. Asymmetric-key cryptography supports a trust links among users who do not trust or know one another, by using a 'digitally signed' to confirm the authenticity and integrity of transactions and to allow the transactions to remain public. A disadvantage of the asymmetric-key cryptography is slow to find hash value [10]. Each transaction has a unique digital signature, which is based on user's private key. Moreover, when a user receives the message, a digital signature and a public key of the sender, it will be easy to confirm if the digital signature is valid [4]. The signature must have the ability to offer non-repudiation, authenticity and integrity [11]. A process of applying a hash function to documents is called Hashing, which provides a unique outcome (digest) for any size of input of (i.e., image, text, and file). Many blockchain implementations are used an exact cryptographic hash function (secure hash algorithm (SHA-256)) with a 256 bits output size [10].

b. Peer-to-peer network

In a peer-to-peer (P2P) network, control and accountability disseminated for many various peers, which enhances the security of the network. BC uses a P2P distributed ledger to get rid of the hazards associated with the centralized database by saving the data in network and to allow the access of everyone (i.e. joining in an overlay network). When a node is connected to this network, it gets a full copy of the BC that can be utilized later on to check that everything is in order. A node might be an electronic device such as a computer, a smart printer, a smart phone, or even a TV, as long as it is connected to the internet. All the nodes on the BC are equally important. Moreover, each node has various tasks in constructing a BC. Nodes and the roles that play can be classified as the following [12]:

- Light node: It holds portion of the information, which is recorded on a BC.
- Full node: It stores an instance of the information recorded on a BC.
- Mining or forging node: It Processes the transactions, puts them in the current blocks, add blocks to a BC, approve and broadcast the block that was joined to the network. These nodes collaborate to administrate, secure and to expand the blockchain.

c. Block structure

Every block consists of a header and data. The header of block contains metadata. The data of the block contains a group of authentic and validated transactions, which are brought when they are submitted to the BC [10]. The block header includes many fields, which will be investigated in the following subsections [11]:

- Height: Every new block is assigned an order number. The height is calculated by subtracting the first block number from the last block number.

- Header hash: It is a basic block identifier. Hash function operates by means of using the header of the block as an input. It is not sent with the block but it is calculated upon receiving the new block.
- Previous block's hash: It allow the block to link with the preceding block, as we see in Figure 3.
- Nonce: A number is utilized to change the header hash value. By combining it with the difficulty field- which will be explained later – it is utilized to verify whether a miner has achieved a work.

$$digest = hash\ (data + nonce)$$

- Difficulty: It is a fractional hash value collision, and therefore, it based on the computational power of the mining node to compute the hash value that fulfills this fractional collision. The miner will modify the difficulty until reaching the fractional collision.
- Transactions: They mean the transmission of data (i.e. data unit of the blockchain).
- Merkle trees: It is a structure as binary tree that encapsulates the data and permits it to be tested securely and efficiently within a huge dataset. The transactions in Merkle trees are packed as shown in Figure 4 [13].

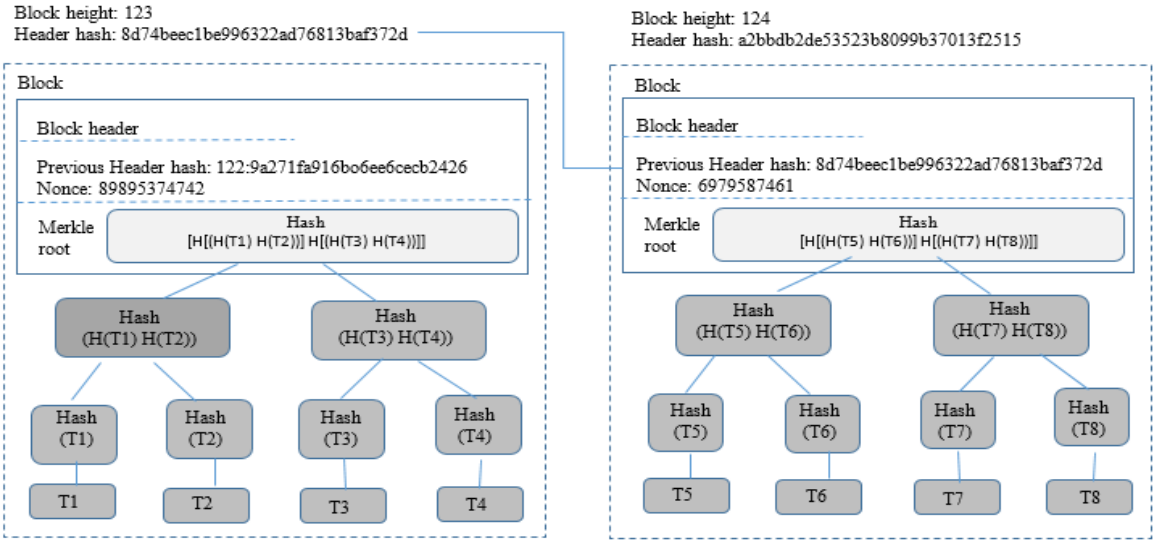

Figure 3. Simplified structure of the block [11]

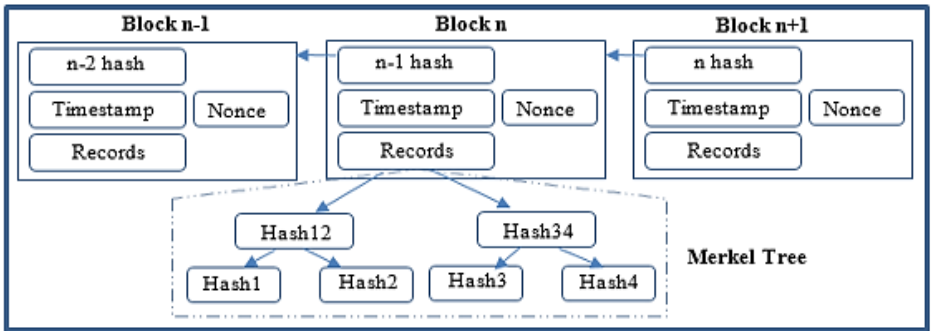

Figure 4. Blockchain structure example [13]

2.1.2. Mining

Mining is the process, which is responsible for updating the BC [11]. In a P2P network, the *mem_pool* is a space that is assigned in the full node memory, which saves and relays the transactions to other nodes. In order to update the status of the BC, certain nodes in the network, called the verifiers or miners, which verify the transactions and compute (cryptographic calculations that are very complicated and they need huge quantities of storage space and power) a block. The miners select certain transactions from

the *mem_pool* that will be put in the blocks. Transactions pay a fee of mining, which can be regarded as an impulse for the miners to so that the transaction can be mined by it. Normally, priority is given by the miner to the transaction that pays a higher fee. Transactions that are not chosen by the miners remain in the *mem_pool* till another one chooses them for a new block. Otherwise, transactions will be discarded [14].

2.1.3. Chaining of blocks

When the block is filled up, it is broadcasted across the network by the sender's node and then mining must be achieved. After that, the block becomes attached concurrently to the former block to make a ledger. This process goes on for a countless number of epochs to make a never-ending series of blocks [15], as shown in Figure 5.

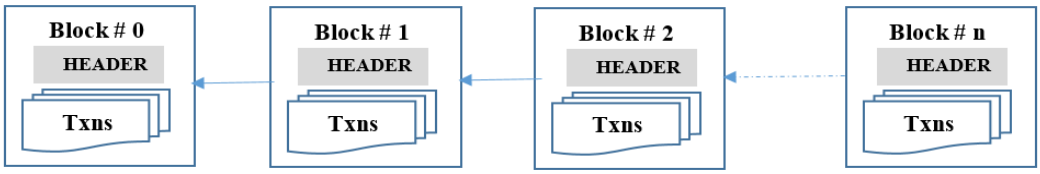

Figure 5. Block chain [15]

2.1.4. Addresses and address derivation

Each blockchain networks has an address, which is a short string of alphanumeric characters derived from the user's public key by a cryptographic hash function, along with certain additional information (i.e. checksums and version number) [10]. Most of the implementations of the BC make use of addresses as the "from" and "to" endpoints in a transaction. In general, addresses are shorter than the public keys and they are not secret. There is a method to generate an address, which is by creating a public key to which a cryptographic hash function is applied to it and the hash is converted to a text [10].

$$public\ key \rightarrow cryptographic\ hash\ function \rightarrow address$$

Each blockchain may implement a different method to derive the address. For public BC networks, which allow anonymous account creation, the user of the BC network can generate a considerable number of asymmetric-key pairs, and therefore addresses as desired. This allows a varying degree of pseudo-anonymity. Addresses could act as the public-facing identifier in the BC network for a user, and often an address will be converted into a QR code for the purpose of easier use by mobile devices [10].

2.2. Consensus algorithms

One of the key aspects of BC technology is determining which node publishes the next block. This is solved by implementing one algorithm amongst many possible consensus ones. For public BC networks, generally there are many publishing nodes, which compete at the same time to publish the next block. They usually do this to win cryptocurrency and/or transaction fees. They are generally distrusted nodes, who could recognize each other by their addresses [10].

When a node joins a BC network it should agree on the initial state of the system. This is recorded in the only pre-configured block, the genesis block (i.e. the first block in the blockchain). Every BC network has a published genesis block and every block must be added to the BC after it, based on the consensus algorithm agreed-upon. Regardless of the algorithm, however, each block must be valid and accordingly it can be validated in an independent way by each node of the BC. By combining the initial state and to verify every block, nodes can independently agree upon the current state of the BC. From the other hand, if there were two valid chains provided to a full node, the common mechanism almost all BC networks is that the 'longer' chain is regarded as the correct chain, which is to be depended; due to having been worked on more [10].

A major characteristic of the BC technology is that no third party is required to provide the status of the system. Each node in the system can test the integrity of the system. All nodes must be in a common agreement to add a new block to the BC. However, some temporary disagreement is sometimes permitted.

There are many consensus algorithms based on the BC implementations [3]. In Table 1, the basic consensus algorithms are briefly discussed. Every BC consensus attempts to achieved three important properties, which are (safety, liveness and fault tolerance) that can be implement efficiently [16].

Table 1. The basic consensus algorithms of the blockchain

Consensus algorithm	Description
Proof of work (PoW)	In 1999, Markus Jakobsson proposed the PoW. Mining nodes that utilize this algorithm requires to resolve a complex-mathematical processes that is altered repeatedly and should have been decided by all the miners. The decision here depends on a common consensus. The problematic with this algorithm is that it wasted a high power of computation [9]–[11], [14]. Furthermore, it is characterized with a great latency to confirm the present transactions [3].
Proof of stake (PoS)	PoS is essentially a generalized form of the PoW. The terms validators are used instead of miners, and they (the minors) are called to the nodes to confirm the transactions [3]. Unlike the PoW, the PoS does not need the mining to calculate the hash value. Instead, the next block creator is selected in a random manner. The chance of a node actually selected to build the new block is based on the stake of node [9], [10], [14], [17]. The PoS keeps great computational resources compared to the PoW [3].
Practical byzantine fault tolerance (PBFT)	PBFT is used widely in the private Blockchains, when the network has a higher trust model different from the PoS and PoW. In practical byzantine fault tolerance, the network is rearranged into a cluster of active and passive replicas. A primary replica is specified from active replicas. PBFT process includes four phases: (the pre- prepare, prepare, commit and the reply phases), as shown in Figure 6. Compared to PoW and PoS, the PBFT has a greater message density [11], [14].

Moreover, there are another consensus algorithms, which can be used in a specific application in the Blockchain such as proof of elapsed time (PoET) [11], proof of space [13], proof of importance [13], measure of trust, minimum block hash [9], leased proof of stake (LPoS) [13], delegated proof of stake (DPoS) [3], [13], proof of bandwidth [13], proof of authority (PoA) [13], [17], and round robin consensus model [10].

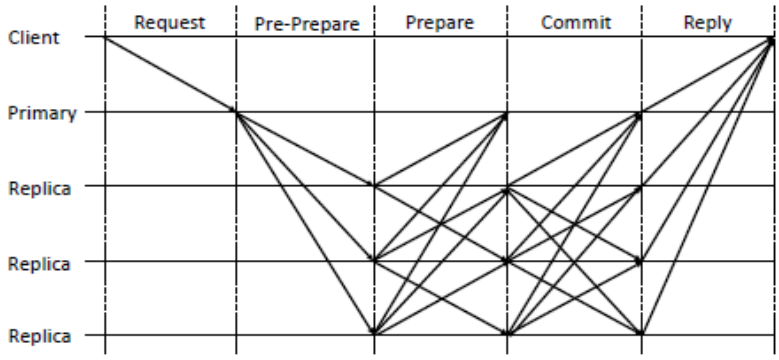

Figure 6. Overview of PBFT protocol [11]

2.3. Blockchain platforms

There are many platforms related to the BC technology that could be used as primary approaches to construct a wide variety of software such as [18]:

a. Bitcoin [19]: It was the leading BC that was theorized and applied and the cryptocurrency that works as a digital financial asset. The Bitcoin utilizes a P2P networking, public key cryptography and a PoW for the purpose of making transactions as well as verifying them. The system of the Bitcoin is programmed so that a fresh block can be created one time each ten minutes [18].
b. Ethereum [20]: It was proposed in 2013 by the developer of Bitcoin Vitalik Buterin. Ethereum [5] is an open-source, public, blockchain-based distributed computing platform featuring smart contract functionality. it utilizes the PoW as its consensus algorithm and mechanism, but it quickly switches to the PoS. The basic building of the proof of work algorithms is that the Ethereum currently used is a memory hard hashing algorithm called Dagger-Hashimoto. The time for creating the block is considerably less compared to the time consumed in several other systems and it is about 12 seconds. As the time of creating the lower block results in a higher rate of stale blocks, therefore the system uses the GHOST protocol to take the heaviest computational chain as the main blockchain. The heaviest chain in this case includes the stale blocks too [18]. As the main platform is a network, which is free for all, a software can be downloaded by anybody or use it in his/her computer. The incentive mechanism for running the software is represented by to getting ether (i.e. a digital currency). While the main platform of Ethereum is a free BC network, the software is an open-source and it permits the software developers to make the network a private one, where nodes participating are only those which were given permission [20].

c. Rootstock: it is a fresh open-source platform, which is like the Ethereum in terms of making a smart contract, except the fact that it uses the bitcoin. The benefits of this platform are that it occurs as a bitcoin and it is compatible with the Ethereum. So, all Ethereum contracts can simply run-on rootstock. The most important advantage, however, is the fact that they can be merged-mined with bitcoin and thereby making rootstock as secure as possible [18].
d. Hyperledger fabric [6]: it is the implementation of the private (permissioned) blockchain technology that is employed as a foundation for developing the BC applications that are hosted via the Linux for a wide variety of industries. Therefore, its architecture is modular, which allows components such as consensus and membership services to be plug-and-play. It leverages the container technology (docker) to enable smart contracts called "chaincode", which comprises the system application logic. The Hyperledger fabric is an open-source distributed ledger software, which is built and maintained by the Hyperledger community. It is a collaborative effort aimed at developing the cross-industry blockchain technologies [20]. Moreover, it is uses the PBFT as a consensus algorithm instead of the PoW algorithm. PBFT can process thousands of requests every second with a latency of increase of less than a millisecond [18].

2.4. Types

Blockchain could be classify to three main types. They are public blockchain, private blockchain and consortium blockchain. The details of these types are listed in Table 2 [11].

Table 2. Types of blockchain

Blockchain type	Description
Public Blockchain (Permissionless)	Decentralized ledger platforms can be used by anyone to broadcasting blocks in it without the need to obtaining the approval from the authority site. As permissionless blockchain is exposed to any participant, a hacker may try to broadcast blocks in a fashion that disrupts the system. To inhibit this, the permissionless blockchain repeatedly use a consensus algorithm [10]
Private Blockchain (Permissioned)	In the private blockchain, users who broadcast the blocks need be certified through a certain authority site [10]. Private organizations could use this type of Blockchains [4]
Consortium Blockchain	The greatest consortium blockchains are semi-decentralized. More than one party can access the blockchain instead of only one part by means of regulating protocol [4]

2.5. Pros and cons of the blockchain

Although blockchain technologies have many important characteristics such as decentralization [3], validity [16], transparency [3], anonymity and identity, redundancy [3], auditability [16] and immutability [3], it has many pros and cons, which are explained as Through the nature of the blockchain design, the pros that are contracted by implementing a blockchain solution are [3]:

a. Distributed: The BC has many nodes that are distributed over the world (data availability). e.g., Ethereum.
b. Transparency: Data are distributed on a public manner and other concerned node and manager can easily get it.
c. Security: It is a main subject of the digital world of nowadays. The certified documents and the transactions are executed and constantly stored in the blocks, which cannot be altered or deleted by anyone (data integrity).
d. Trust: Participants in this blockchain are the ones who decide the transactions to be added before inserting them in the blockchain. So, trust becomes higher in terms of altering, writing or even reading the information.
e. Efficiency: In the blockchain technology, efficiency of a network can be improved when the financial groups collaborate.
f. Resilience: If a huge number of nodes, the strength of information is improved with extended life.

On the other hand, the blockchain has some cons which are [3]:

a. Block size: In the blockchain, each block that is inserted in to the blockchain increases the size of the database.
b. Speed and cost of the network: It is hard to manage all the nodes in a BC once the node numbers become higher.
c. Wasteful: Every node has to continue the consensus alg., which provides the mistake tolerance and ensures zero interruption. Then, they are totally wasteful since every node tracks the relevant task to grasp consensus. So, the chance of calculating a valid nonce rise according to the computing power that the faster computers have.
d. Standards: Because blockchain is at its initial age, there are no definite standards.

e. Performance: Compared to the centralized database, the blockchain is slower, because the blockchain performs all the operations of a traditional database system in addition to various additional loads like.

Consensus algorithm, signature confirmation and others when it executes the transaction. In order to mitigate the drawbacks mentioned above, efforts were made to improve the protocol speed and the efficiency with a special care to the algorithms associated with the limited access and consensus algorithm [21].

2.6. Challenges

Based on the literature, the blockchain technology encountered many challenges. Some of these challenges are related to security, attacks, power consumption and so on [3]. The most common challenges of blockchain with their details are presented in Table 3.

Table 3. Challenges of blockchain

Challenge	Description
Private key security	A secret and single key is given to each participant in the blockchain (private key). Now, a malicious can catch the user's private key. It is hard to detect the hacker's behavior since the blockchain is decentralized.
Privacy leakage	An assured degree is reserved to keep the privacy of the users contained in the transactions.
Criminal activities	Currently, criminal activities are growing in BCs. As for bitcoin, customers are provided with addresses, which are not related to users' identities. So, the events that are made via bitcoin is greatly hard to be tracked.
Attacks	Many malicious users and attackers attempt to attack a node or a network by conducting several hacks, as we discussed in the sub section 2.7.
Standardization	Increasing the number of nodes from dissimilar networks, in the blockchain no standard to permit the customers to cooperate. The absence of standardization permits developers or coders to prepare everything as they hope and this makes issues for the IT.
Environmental cost	Implementation the blockchain technology in any company, needs definite software and applications that requires to be established via a software organization. Thus, it is acquisition is costly. Also, the company may have not the fixed hardware for the usage of the software.
Energy consumption	Allows the users to operate in the blockchain as some difficult algorithms need to be achieved and their outcome is a large depletion of power.
Slow and cumbersome	The blockchain technology is not fast to perform a transaction related to the traditional fee system (e.g., cash or debit card), because the blockchain achieves more complexity and encryption operations.
Public perception	People must identify the variances amongst blockchain technologies before adopting the blockchain technology as it can be so useful to eliminate the bad idea about blockchain technology in its own.

2.7. Blockchain's attacks

Blockchain is subjected to many attacks. Because the decentralized nature of its operational environment, hackers have conducted numerous multipurpose attacks against blockchain technology by exploiting the vulnerabilities of (structure of the blockchain, peer-to-peer system and applications) [4], [14], as it is shown in Figure 7. In the following, we summarized some attacks against to the structure of the blockchain, peer to peer system, and the applications of blockchain [14].

a. Forks [22]: It exploits the blockchain structure by chain splitting and revenue loss and this in turn affects the blockchain.
b. Stale and orphaned blocks [23]: It exploits the blockchain structure by revenue loss that has an effect on the blockchain, miners and mining pools.
c. Selfish mining [24]: It exploits the blockchain's peer-to-peer system by revenue loss and malicious mining that have an effect on the blockchain, miners and mining pools.
d. Majority attacks (51% attack) [25]: It exploits the blockchain's peer-to-peer system by chain dividing, malicious mining and revenue loss that impact the blockchain, miners and application.
e. Domain name system (DNS) hijacks [14]: It exploits the blockchain's peer-to-peer system by revenue loss, partitioning and information theft that have an effect on the miners, exchanges, mining pools and users.
f. Border gateway protocol (BGP) hijacks [26]: It exploits the blockchain's peer-to-peer system by revenue loss, partitioning and theft information that effect on the miners, mining pools and users.
g. Eclipse attack [27]: It exploits the blockchain's peer-to-peer system by partitioning that effect on the miners and users. A set of hacker nodes separates its bordering nodes utilize internet protocol (IP) addresses, thus compromising their received and leaving traffic.
h. Distributed denial-of-service (DDoS) attacks [28]: It exploits the blockchain's peer-to peer system by malicious mining and information theft that have an effect on the blockchain, miners and mining pools. In bitcoin network, 51% attack could lead to denial-of-service (DoS).
i. Block withholding [29]: It exploits the blockchain's peer-to-peer system by revenue loss and malicious mining that impact the miners and mining pools.

j. Finney attacks [14]: It exploits the blockchain's peer-to-peer system by revenue loss, which affects the miners, mining pools and users, by creating an identical to the preceding transaction and drives it to a receiver. After the receiver gets the transaction and brings the result, the miner publishes the preceding block with the basic transaction in it.
k. Consensus delay [29]: It exploits the blockchain's peer-to-peer system by the delay and info loss that have an effect on the miners, mining pools and users. A hacker might insert false blocks to increase the latency or to prevent peers from achieving the consensus success around the state of the blockchain.
l. Timejacking attacks [30]: It exploits the blockchain's peer-to-peer system by delaying the malicious mining, chain splitting and revenue loss that affect the miners, mining pools and application. A hacker can calculate a new block and put its timestamp forward of network's timestamp with the values of 50 minutes.
m. Blockchain ingestion [14]: It exploits the blockchain's applications by info loss that affects the blockchain. The examination of the public blockchain could expose beneficial information to an opponent.
n. Double-spending [31]: It exploits the BC's applications that impacts the blockchain and the users, by using a one-time transactions several times.
o. Cryptojacking [32]: It exploits the blockchain's applications by chain splitting and malicious mining that effect on the application and users.
p. Wallet theft [33]: It exploits the blockchain's applications by revenue loss and theft that impact the exchanges, application and users. Associated keys with peers in the network are saved in a digital wallet, the "wallet theft" attack get up with sure associations on the applications.
q. Smart contract DoS [14]: It exploits the blockchain's applications by revenue loss, delay and theft that affect the blockchain, application and users.
r. Reentrancy attacks [14]: It exploits the blockchain's applications by revenue loss and theft and this in turn affects the application and users.
s. Replay attacks [14]: It exploits the blockchain's applications by revenue loss and info loss, which impact the blockchain, mining pools, application and users, including the creation of one transaction and send it to dissimilar two blockchains.
t. Overflow attacks [14]: It exploits the blockchain's applications by theft that affects the application and users, when the type adaptable value exceeds (2^256).
u. Short address attacks [14]: It exploits the blockchain's applications by revenue loss and theft that impact the application. Abuses a bug in Ethereum's virtual machine to create additional tokens on boundless consumptions.
v. Balance attacks [14]: It exploits the blockchain's applications by revenue loss and theft, which impact the application and users.

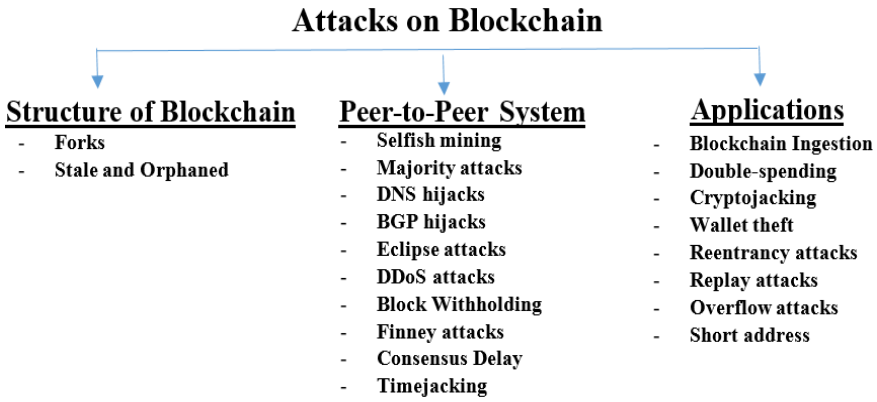

Figure 7. Attacks on blockchain based on vulnerabilities

2.8. Blockchain applications

Nowadays, a great number of corporations earn their profits means of employing BC, as it could be the most suitable solution, if the following conditions are met [3]: i) when the shared common database is needed, ii) when trust is not reciprocated by participants, iii) when the database is common for various writers or parties, iv) when the system or the network is subjected to hackers and malicious, v) when the

same rules are applied to all the participants in the system, vi) when there is transparency in the result of the decision making for all the participants, and vii) when the transactions are no more than 10,000 transactions/second. There are many sectors used a BC, some of them are:

- Business: Recently, organizations are in no need to a third party or a host to safeguard their assets [3]. In particular, financial and healthcare are accustomed to encounter security problems because of the malicious users. By using the BC this issue can be settled.
- Supply chain: Almost all the organizations possess enterprise resource planning (ERP) and supply chain administration software to ensure that the operations move smoothly [34]. But the restricted details and the visibility related to products are two essential elements, which become vital with the increase of the product number. Therefore, BC is a good solution that can follow every item in the organization by means of the process of the supply chain and can also fulfill a powerful security means. To enhance the product safety, several records should also be updated, like the ambient conditions at each stage that minimizes the loss or harm inflicted on products when shipping. The BC is also used to achieve an update and replacement can be performed during the lifetime of any device or product.
- Copy rights: Because of the insufficient transparency, the information of multimedia like photos and music. Encounter the copyright problem when trying to specify the valid owners to use them properly. Authorized owners are not capable of controlling their documents on the internet. A great number of hackers merely by copying the contents of the documents in an unauthorized way and distribute them via the internet. The BC mitigate the issue mentioned earlier by enhancing the information availability concerning the ownership of copyrights. This sort of information is provided as "trusted timestamping". Hence, any timestamp will be identified as an encoded information, which show the time and date of occurrence. So, a trusted timestamping "is a process that takes place to track the modification securely in addition to the creation time of any document".
- Electricity management: In the developed states, management of electricity is considered as an essential concern as the user 's information of electricity is often leaked. Since the number of electricity users is tremendous, it is hard to manage the system entirely. So, the BC is utilized to resolve the above problem by adopting private BC and smart contracts [35].
- Distributed storage: Currently, cloud data storage service is one of the popular services that is used by numerous users. However, one of the significant disadvantages of cloud-based service is that it is centralized and the cloud service provider (CSP) controls all the processes [36]. Occasionally, the CSP uses the users' confidential data illegally to obtain revenue even without notifying the user, and therefore, users' data may be at hazard. The BC data storage service CSP minimizes the above problem through its decentralized characteristic [37]. Hence, the users store their unmodifiable data.
- Digital identity: In the present time, every state is considering the digital identity. so, the digital identity is used in national security, banking industry, healthcare services, citizenship documentation and online retailing. Several states spend considerable amounts of cash in the digital identity field. Occasionally, a digital identity is misused or hacked by malicious users. Therefore, BC can resolve this problem by managing and tracking the digital identity in a secure and efficient way. In this case, the identity is authenticated in a secure and an immutable way. Instead of using system that is based on the password, in BC, identity will be verified by using the digital signature that depends on the cryptography (public key).
- Autonomous organizations: BC is utilized to create decentralized companies through making several smart contracts. These contracts adhere to an interaction in a specific protocol.

2.9. Integration blockchain with IoT

Cryptocurrency and financial transactions have firstly used blockchain where all nodes in the blockchain execute and store all the transactions. Also, the blockchain provides many benefits because it could be adapted with many domains and one of the common domains is IoT [38]. There are many networks smart devices, which construct the IoT such as Raspberry, ESP and so on. IoT interconnects heterogeneous objects and smart devices seamlessly to create a network, which is used for sensing, processing and communication processes. IoT smart devices are managed and controlled automatically without the need to human interventions and they consume low energy and have a lightweight process. According to Statista Com [39], the number of IoT objects in 2020 is estimated to be 31 billion devices worldwide. By the end of 2025, this number is predicted to increase to be 75 billion devices [40], as shown in Figure 8.

In IoT, the smart devices have to spend the largest portion of their energy and execute the process to achieve vital application tasks, which makes achieving the privacy and security tasks fairly challenging. Malignant attacks can prevent IoT services in addition to threatening the users' privacy, data security and the confidentiality of the entire network [13]. There are four main categories of attacks in IoT-based system, which are: physical attack, network attack, software attack and data attack [41]. In The first category, which is called the physical attack, the attacker will be physically near to the network and attempt to conduct the

malicious processes in the entire system through many forms such as manipulating the IoT device, blocking the RF signals, injection of malicious code and performing the side-channel attack. The researcher used the physical unclonable function (PUF) to provide the authentication of IoT devices [42], and thus physical attacks are prevented. The PUF has a characteristic that is impossible to copy the accurate microstructure of the IoT device. In the second category; (network attack), the attackers attempt to manipulate the network of the IoT using many ways such as RFID spoofing, man-in-the-middle, Traffic analysis and Sybil attacks. To prevent this kind of attacks, authentication technique and the secure hash function are used [43]. From the other hand, in the third category, which is called software attacks, the attacker utilizes the current software advantages in the IoT system. The last category is called the data attack and it could be achieved by the unauthorized access to the data and data inconsistency. To prevent these type of attacks, the blockchain could be used by providing privacy-preserving tech. efficiently [44].

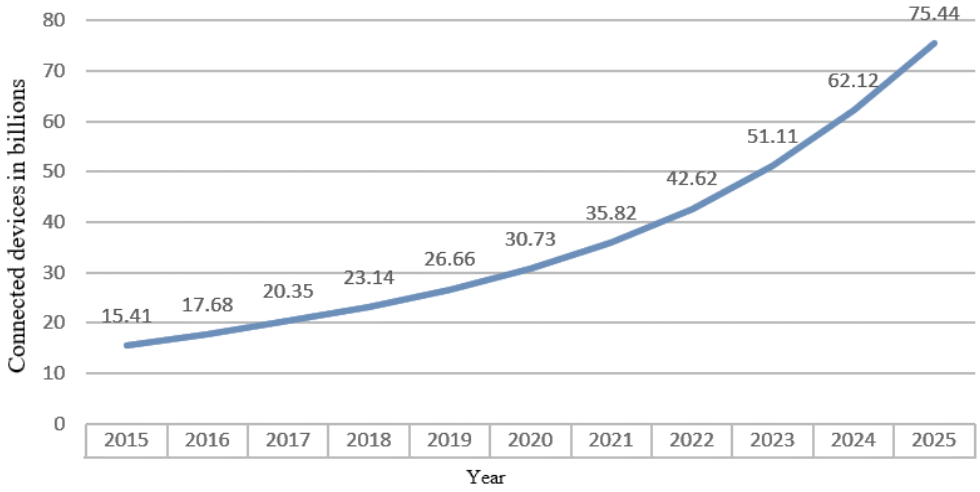

Figure 8. The predicted growth of IoT devices from 2015 to 2025 [40]

The traditional security approaches tend to be costly for IoT in each of processing overhead and consuming of energy [45]. In addition to that, a lot of the state-of-threat security contexts are extremely centralized and they are not suitable for IoT because of the many-to-one nature of the traffic, difficulty of scale [46] and the single point of failure [47].

Integrating the blockchain with IoT achieves many advantages, which are:

- The distributed and decentralize attributes of the blockchain technology do not need a central server that provides a scalable method to manipulate the increasing number of IoT devices.
- The blockchain provides more security and privacy because it uses complex cryptography algorithms such as timestamp and hash functions to ensure a secure environment [46].
- The blockchain provides an immutable ledger and tamper-proof to protect the data from malicious attacks. Consequently, the trusted system will be produced (i.e. only the trusted participants of the IoT devices could accept or reject transactions depending on their consent).
- The blockchain has an important property, which is called Anonymity [8].
- The blockchain supplies a 160-bit address space, which offers 4.3 billion addresses that enable it to assign addresses for multiple objects.
- The monitoring and tracking of ownership, trustworthiness, authorized identity registration could be provided by the blockchain.

The capability of applying blockchain in IoT relies on many assumptions [48]. Firstly, the IoT application requires a decentralized peer-to-peer ecosystem. Secondly, the IoT application needs to keep payment operation for the available services between the two parties only. Finally, If the logs and traceability of the ordered transactions are required by IoT applications. However, Implementing the blockchain in IoT will require addressing the following challenges [8], [13]:

- The mining process of blocks takes a great deal of time, while most of IoT applications require little latency.

- The mining process exhausts energy because of its high computation ability, while the common devices of IoT are resource-constrained.
- The basic Blockchain protocols generate a lot of overhead traffic; therefore, it may be unwanted for a certain bandwidth-restricted IoT devices.
- The blockchain scales is unwanted when the IoT networks are predictable to cover a huge number of nodes.
- IoT sensors produce a huge amount of data, therefore, processing the transactions in blockchain will be very slow or will have a high latency.
- The anonymity of transaction history cannot be ensured on public blockchain. So, the hackers can determine the identities of users or devices by examining the transaction style.

The researching in the field of integrating the blockchain with IoT have seen a major renaissance after the interest rose in cryptocurrencies and mining process. Also, different research publications have provided an advanced solution for constructing decentralized social networking systems, telecommunications, voting, smart homes, and smart city [15] which were all suggested. Recently, there were many studies that investigated the integration of blockchain technology with IoT to solve the privacy and security challenges in the IoT domain. For instance, Dorri *et al.* [8] presented a lightweight architecture for IoT, which depends on the blockchain to produce IoT system with high privacy and omits the overhead of blockchain. Uddin *et al.* [13] suggested an efficient lightweight integrated blockchain (ELIB) model, which was established to meet the constraint of IoT. Polyzos and Fotiou [49] demonstrated the importance of blockchain technologies in examining the requirements of the IoT security and how the security challenges can be solved by combining the IoT with the blockchain technologies. Thakore *et al.* [50] provided a complete survey on the fundamentals of both technologies and the blockchain-based IoT Architecture. Karthikeyan et al. [51] presented a summary of IoT security problems and suggested the blockchain technologies to resolve these problems. They also explain the probability of integrating the blockchain with the IoT. Ramesh *et al.* [15] discovered the way to keep the IoT data on a mixture of a Blockchain with Ethereum swarm and inter planetary file system (IPFS) in an encrypted style. Fotiou *et al.* [52] proposed a smart contract-based solution to solve the privacy and security problems in the IoT system. Uddin *et al.* [13] investigated the latest state-of-the-arts improvements in Blockchain for cloud and IoT, Blockchain and IoT and B.C. and fog of IoT in various applications are analyzed. Tandon [53] presented a review of blockchain technology and the way in which it provides the suitable solution to resolve privacy and security challenges of the IoT system. In addition to that, he discussed the pros and cons of integrating IoT with blockchain. Minoli and Occhiogrosso [54] provided the places of interest in some of IoT environments where Blockchain Technology play an important role. Khan and Salah [55] presented a review of security challenges for IoT and then they presented blockchain technology to resolve the security problems of the IoT system. Sengupta *et al.* [41] presented a review about the security attacks and the problems associated with each of the IoT and industrial IoT (IIoT) and that organizing it depends on the vulnerability. Also, authors showed the methodology of using blockchain technology for detecting these attacks. Banerjee *et al.* [56] proposed a new method represented by using the blockchain to provide IoT dataset for solving the sharing of the IoT dataset problems.

Moreover, the importance of integrating the blockchain with IoT it has been applied on various domains. Tables 4 and 5 shows the most common domains and the recent studies, which depend on the integration of blockchain with IoT applications. Most of these studies were concerned with providing security and privacy services for the IoT environment by using blockchain. As a result, blockchain is considered an effective and active tool to provide these services. We note in Tables 4 and 5 that the articles within this review suffers from some challenges such as (privacy and scale). Thus, we introduce in Table 6 some recommendations for those challenges.

In addition to that, the blockchain can adapt to other technologies such as the following:

a. Software-defined networks (SDN): In this technology, the resources of this network are managed via a centralized controller, which acts as the networking operating system (NOS) [19]. Yet, scalability is a big constraint in the single networking environments that are enabled by SDN and thus the adaptability of BC with SDN can facilitate multi-domain SDNs interconnection and communication [57].
b. Decentralized email: Nowadays, the security service of an email is dependent on an ongoing process of planning in addition to management. One of the solutions to address the vulnerabilities of the email can be in the form of a blockchain-powered decentralized and distributed email system. Email addresses can be allocated to the clients over BC. Most vitally, the communication of email by BC is not influenced by the authorities of government that might invest the centralized email providers such as ISPs and technology giants like Google, Facebook, and Amazon [17].
c. Blockchain-based content distribution: Content distribution networks (CDNs) are regarded as effective approach that enhances the quality of the service of Internet through the content replication at various

geographic locations represented by data-centers. Blockchain technology can be the solution with the necessary ingredients to significantly resolve the challenges related to content distribution. It can stabilize the rights management related issues for studios and artists by providing a better way of content control [17].

d. Distributed cloud storage: Users and organizations encounter and storage management of data problems resulting from the huge growth of data on non-volatile storage systems. the security, privacy and control of data are still important concerns [58]. The solutions of cloud storage that are based on BC inherit characteristics such as anonymity, decentralization and the trusted execution of transactions for the trusted members and can level the path for a cloud computing era characterized with verification and trust.

e. Smart cities: There are inclusive major ingredients related to the smart cities, such as smart healthcare (BC is the well-known method that delivers a major level of democratization in the sector of healthcare and thus enhance their status), supply chain management (SCM), smart transportation (BC can improve information exchange, support the performance of vehicle and enhance the dependability of the network lifetime. Furthermore, BC invigorates the transportation industry by making less turnaround times, faster security detection, swifter data management and inspections), smart grid and financial system [17].

Table 4. Recent studies of integration blockchain with IoT (part 1)

Citation	Survey/ Review	IoT	IoT security	IoT privacy	Supply chain	Health care	Agriculture	Contributions	Weakness
Huh *et al.* [59]	*	-	*	-	-	-	-	BC to control and configure IoT devices	Did not focus on scale and privacy
Ruta *et al.* [60]	*	-	-	-	*	-	-	BC framework for SWoT as Service	Did not focus on Security and privacy
Zhang and Wen [61]	*	*	-	-	-	-	-	IoT E-business model-based BC	Did not focus on Security and privacy and scale
Atlam *et al.* [47]	*	*	-	-	-	-	-	Integration IoT with each of BC and AI	Did not focus on Security and privacy and scale
Novo [18]	-	-	*	-	-	-	-	Access control sys. for IoT Based on BC	Did not focus on scale and privacy
Khan and Salah [55]	*	-	*	-	-	-	-	Present major Security problems for IoT	Did not focus on performance and privacy
Badr *et al.* [62]	-	-	*	*	-	*	-	BC to secure and privacy for e-health	Did not focus on performance and scale
Uddin *et al.* [13]	*	*	-	-	-	-	-	BC for Cloud IoT and BC for Fog IoT	Did not focus on Security and privacy and scale
Dorri *et al.* [8]	-	-	*	*	-	-	-	secure, privacy and lightweight BC-IoT	Did not focus on performance and scale
Salman *et al.* [9]	*	-	*	*	-	-	-	Security, privacy, access control, provenance	Did not focus on performance and scale
Lo *et al.* [63]	*	-	-	-	-	-	-	Analyzing academia, methodology BC-IoT	Did not focus on Security and privacy and scale
Rejeb *et al.* [64]	*	-	-	-	*	-	-	Enhance supply chain transparency, trust	Did not focus on performance
Dai *et al.* [65]	*	-	-	-	*	-	-	Investigate the integration BC-IOT	Did not focus on Security and privacy and scale
Zhang *et al.* [66]	-	-	*	-	-	-	-	Investigates an access control issue in IoT	Did not focus on privacy, scale, performance
Lao *et al.* [67]	*	*	-	-	-	-	-	Components of IoT-BC, BC applications	Did not focus on Security and privacy and scale
Huckle *et al.* [68]	*	-	-	-	*	-	-	Shared economy applications	Did not focus on privacy, scale, performance
Patil *et al.* [69]	-	-	*	*	-	-	*	Lightweight BC for greenhouse farms	Did not focus on performance and scale
Polyzos and Fotiou [49]	*	-	*	-	-	-	-	Potential of a BC-IoT	Did not focus on performance, privacy, scale
Zhu and Badr [70]	*	-	*	*	-	-	-	Digital identification management for IoT	Did not focus on performance and scale
Mishra and Tyagi [71]	-	-	*	-	-	*	-	Secure E-healthcare based on BC	Did not focus on performance, privacy, scale

Table 5. Recent studies of integration blockchain with IoT (part 2)

Citation	Survey/ Review	IoT	IoT security	IoT privacy	Supply chain	Health care	Agriculture	Contributions	Weakness
Banerjee *et al.* [56]	*	-	*	-	-	-	-	Datasets IoT security and integrity	Did not focus on performance, scale
Wang *et al.* [72]	*	-	-	-	-	-	-	BC to support IoT application	Did not focus on performance, privacy, scale
Sengupta *et al.* [41]	*	-	*	-	-	-	-	Security of Industrial IoT (IIoT)	Did not focus on performance, privacy, scale
Jesus *et al.* [11]	*	-	*	*	-	-	-	Secure and privacy of IoT	Did not focus on performance and scale
Dwivedi *et al.* [73]	*	*	-	-	-	-	-	Integration BC-IoT and BC-IIoT	Did not focus on security, privacy and scale
Kamilaris *et al.* [74]	-	-	-	-	-	-	*	Impact of BC in food supply chain, Agric.	Did not focus on security, privacy and scale
Ferrag *et al.* [75]	*	-	*	-	-	-	-	Enhance the security of communication	Did not focus on performance, privacy, scale
Zheng *et al.* [2]	*	-	-	-	-	-	-	BC architecture	Did not focus on security, privacy and scale
Thakore *et al.* [50]	*	*	-	-	-	-	-	Combine BC with IoT	Did not focus on security, privacy and scale
Hassan *et al.* [17]	*	-	-	-	-	-	-	BC – based network App.	Did not focus on security, privacy and scale
Lin *et al.* [76]	-	*	-	-	*	-	-	Traceability food system based on BC	Did not focus on security, privacy and scale
Dogo *et al.* [77]	-	*	*	-	-	-	*	Water management based on BC-IoT	Did not focus on privacy and scale
Yaga *et al.* [10]	*	-	-	-	-	-	-	Overview of BC	Did not focus on security, privacy and scale
Kadam and John [78]	-	-	*	*	-	-	-	IoT architecture, BC-IoT	Did not focus on privacy, scale, performance
Maroufi *et al.* [12]	*	-	-	-	-	-	-	BC-IoT challenges and solutions	Did not focus on security, privacy and scale
Alamri *et al.* [79]	*	-	*	*	-	-	-	Integrate BC-IoT for security and privacy	Did not focus on scale
Conoscenti *et al.* [80]	*	-	-	-	-	-	-	Review on BC	Did not focus on scale and performance
Atlam and Wills [81]	*	-	*	*	-	-	-	Combine Distributed Ledger Tec. With IoT	Did not focus on scale and performance
Saad *et al.* [14]	*	-	-	-	-	-	-	BC attacks	Did not focus on performance, privacy, scale
Atlam *et al.* [46]	*	-	*	-	-	-	-	Integrate fuzzy with expert judgment risk	Did not focus on performance, privacy, scale
Abadi *et al.* [82]	*	-	-	-	-	-	-	BC-IoT recent works	-
Tandon [53]	*	-	*	*	-	-	-	BC-IoT for security and privacy problems	Did not focus on performance, scale
Vokerla *et al.* [4]	*	-	-	-	-	-	-	Blockchain overview	Did not focus on security, privacy and scale
Karthikeyan *et al.* [51]	*	-	*	-	-	-	-	BC-IoT security issues and applications	Did not focus on scale and performance
Fotiou *et al.* [52]	-	-	*	*	-	-	-	Access control for IoT	-
Hang and Kim [83]	-	-	*	*	-	-	-	Integrate BC-IoT	Did not focus on performance
Mahmood *et al.* [42]	*	*	-	-	-	-	-	Multi_server auth. By (PUF)	Did not focus on performance, privacy, scale

Table 6. Some recommendations for security, privacy and scale challenges

Literatures challenges	Recommendation
Maintaining privacy in BC	Homomorphic encryption and proxy re-encryption technique 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 can be integrated with Blockchain technology to ensure the privacy-preserving computation on users' data [13].
Maintaining security in BC	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 [13].
Resource and power constraints	Energy effective consensus algorithms are introduced to save the transactions conducted recently only (e.g., mini-BC [84], PoS and delegated proof-of-space). Xu *et al.* [85] suggested the management of smart resource for cloud data-centers by utilizing the BC technology.
Scalability and availability	Sharma *et al.* [57] also submitted an architecture of cloud that depends on integrating the BC with software-defined networks (SDN) and fog-computing.

3. RESULTS AND DISCUSSION

In this paper, after examining 49 review literatures, it was found that 50% of those literatures are related to the security of internet of things, 25% related to the privacy of IoT, 25% of them to both security and privacy of IoT. The rest of the literatures were related to other fields such as health, agriculture and supply chain, as shown in Table 7. However, the objective of this paper is to present a general reference guide for researchers and practitioners in the fields which are mentioned.

Table 7. Numbers of related literature categorized by scope contribution

Literature scope	Number of literatures
IoT Security	25
IoT Privacy	13
BC and IoT Security	17
BC and IoT Privacy	8
BC-IoT security and BC -IoT Privacy	13
BC-IoT eHealth	2
BC-IoT Supply Chain	5
BC-IoT Agriculture	3
IoT Scale	5

4. CONCLUSION AND FUTURE WORKS

Blockchain Technology is a fresh tool for many applications in various organizations, which allows to secure transactions in a decentralized authority. In this paper, an overview on blockchain technology is presented. Generally, fundamentals of blockchain are discussed. Also, some types of attacks on blockchain are demonstrated and summarize. Based on the literatures, the integration of Blockchain with another technology such as IoT could provide a better result in some possible domain. This integration shows the features of Blockchain that makes it an attractive technology to solve some IoT challenges such as privacy and security issues.

In future works, concern should be focused on investigating new tendencies for security and privacy services by using blockchain technology in particular to design intrusion detection systems (IDS) which work in the IoT environment. The main goal includes the reduction of the numbers of the fields in the blocks and also developing a lightweight mining and consensus algorithms.

ACKNOWLEDGEMENTS

The authors would like to thank the University of Mosul/College of Computer Science and Mathematics for their facilities, which have helps to enhance the quality of this work.

REFERENCES

[1] Y. Elmandjra, "Bitcoin as an investment part 2," ARK Invest Management LLC, 2020.
[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
[3] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, "The revolution of blockchain: state-of-the-art and research challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1497–1515, May 2021, doi: 10.1007/s11831-020-09426-0.
[4] R. R. Vokerla *et al.*, "An overview of blockchain applications and attacks," *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899450.
[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.
[6] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: lessons for securing commodity internet of things devices," in *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security*, May 2016, pp. 461–472, doi: 10.1145/2897845.2897886.
[7] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, Jun. 2015, doi: 10.1109/MCOM.2015.7120028.
[8] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arxiv.org/abs/1608.05187*, 2016, [Online]. Available: http://arxiv.org/abs/1608.05187.
[9] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.
[10] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, Oct. 2019. doi: 10.6028/NIST.IR.8202.
[11] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, pp. 1–27, Apr. 2018, doi: 10.1155/2018/9675050.

[12] M. Maroufi, R. Abdolee, and B. M. Tazekand, "On the convergence of blockchain and internet of things (IoT) technologies," *Journal of Strategic Innovation and Sustainability*, vol. 14, no. 1, Mar. 2019, doi: 10.33423/jsis.v14i1.990.
[13] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutionss," *Blockchain: Research and Applications*, vol. 2, no. 2, 2021, doi: 10.1016/j.bcra.2021.100006.
[14] M. Saad *et al.*, "Exploring the attack surface of blockchain: a systematic overview," *arxiv.org/abs/1904.03487*, Apr. 2019, [Online]. Available: http://arxiv.org/abs/1904.03487.
[15] Vinay Kumar Calastry Ramesh, "Storing IoT data securely in a private Ethereum blockchain," M.S. Thesis, Department of Computer Science, University of Nevada, Las Vegas, 2019.
[16] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *Journal of Industrial Information Integration*, vol. 13, pp. 32–39, Mar. 2019, doi: 10.1016/j.jii.2018.07.004.
[17] F. Hassan *et al.*, "Blockchain and the future of the internet: a comprehensive review," *arxiv.org/abs/1904.00733*, Feb. 2019, [Online]. Available: http://arxiv.org/abs/1904.00733.
[18] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoTT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018, doi: 10.1109/JIOT.2018.2812239.
[19] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.
[20] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Jul. 2017, pp. 1–6, doi: 10.1109/ICCCN.2017.8038517.
[21] M. Vukolić, "The quest for scalable blockchain fabric: proof-of-work vs. BFT replication," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9591, Springer International Publishing, 2016, pp. 112–125.
[22] I. Eyal, "The miner's dilemma," in *Proceedings - IEEE Symposium on Security and Privacy*, May 2015, pp. 89–103, doi: 10.1109/SP.2015.13.
[23] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," *IEEE P2P 2013 Proceedings*, 2013, pp. 1-10, doi: 10.1109/P2P.2013.6688704.
[24] T. Leelavimolsilp, L. Tran-Thanh, and S. Stein, "On the preliminary investigation of selfish mining strategy with multiple selfish miners," *arxiv.org/abs/1802.02218*, Feb. 2018, [Online]. Available: http://arxiv.org/abs/1802.02218.
[25] M. Bastiaan, "Preventing the 51%-attack: a stochastic analysis of two-phase proof of work in bitcoin," *22nd Twente Student Conference on IT January 23rd*, 2015, Enschede, Netherlands, pp. 1–10, 2015.
[26] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: routing attacks on cryptocurrencies," in *IEEE Symposium on Security and Privacy*, May 2017, pp. 375–392, doi: 10.1109/SP.2017.29.
[27] Y. Marcus, E. Heilman, and S. Goldberg, "Low-resource eclipse attacks on Ethereum's peer-to-peer network," *IACR Cryptology ePrint Archive*, p. 236, 2018.
[28] M. Saad, M. T. Thai, and A. Mohaisen, "POSTER: deterring DDoS attacks on blockchain-based cryptocurrencies through Mempool optimization," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, May 2018, pp. 809–811, doi: 10.1145/3196494.3201584.
[29] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: a scalable blockchain protocol," *arxiv.org/abs/1510.02037*, Oct. 2015, [Online]. Available: http://arxiv.org/abs/1510.02037.
[30] C. A. Vyas and M. Lunagaria, "Security concerns and issues for bitcoin," *International Journal of Computer Applications*, pp. 10–12, 2014.
[31] I. Dilhani and T. N., "Transaction verification model over double spending for peer-to-peer digital currency transactions based on blockchain architecture," *International Journal of Computer Applications*, vol. 163, no. 5, pp. 24–31, Apr. 2017, doi: 10.5120/ijca2017913531.
[32] R. Tahir *et al.*, "Mining on someone else's dime: mitigating covert mining operations in clouds and enterprises," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10453, Springer International Publishing, 2017, pp. 287–310.
[33] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "BlueWallet: the secure bitcoin wallet," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8743, Springer International Publishing, 2014, pp. 65–80.
[34] G. Q. Huang, J. S. K. Lau, and K. L. Mak, "The impacts of sharing production information on supply chain dynamics: a review of the literature," *International Journal of Production Research*, vol. 41, no. 7, pp. 1483–1517, Jan. 2003, doi: 10.1080/0020754031000069625.
[35] Z. Ming, C. Jun, W. Yuqing, L. Yuanfei, Y. Yongqi, and D. Jinyue, "The primarily research for multi module cooperative autonomous mode of energy internet under blockchain framework," *Proceedings of the CSEE*, vol. 37, no. 13, pp. 3672–3681, 2017, doi: 10.13334/j.0258-8013.pcsee.162432-en.
[36] S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, and A. Shanthini, "Towards DNA based data security in the cloud computing environment," *Computer Communications*, vol. 151, pp. 539–547, Feb. 2020, doi: 10.1016/j.comcom.2019.12.041.
[37] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: using blockchain to protect personal data," in *IEEE Security and Privacy Workshops*, May 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.
[38] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in *Internet of Things*, Springer International Publishing, 2020, pp. 123–149.
[39] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: a systematic survey," *Sensors*, vol. 18, no. 8, Aug. 2018, doi: 10.3390/s18082575.
[40] M. H. Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, and C. Perera, "The role of big data analytics in industrial internet of things," *Future Generation Computer Systems*, vol. 99, pp. 247–259, Oct. 2019, doi: 10.1016/j.future.2019.04.020.
[41] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoTt," *Journal of Network and Computer Applications*, vol. 149, 2020, doi: 10.1016/j.jnca.2019.102481.
[42] K. Mahmood *et al.*, "PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication," *Journal of Information Security and Applications*, vol. 61, Sep. 2021, doi: 10.1016/j.jisa.2021.102900.
[43] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18295–18325, Nov. 2018, doi: 10.1007/s11042-017-5376-4.
[44] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1913–1922, Dec. 2021, doi: 10.1109/JAS.2021.1004225.

[45] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.
[46] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for risk-based access control model for IoT," *Internet of Things*, vol. 6, Jun. 2019, doi: 10.1016/j.iot.2019.100052.
[47] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and AI," *Big Data and Cognitive Computing*, vol. 4, no. 4, pp. 1–27, Oct. 2020, doi: 10.3390/bdcc4040028.
[48] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S. U. Rehman, "Blockchain and internet of things: a bibliometric study," *Computers and Electrical Engineering*, vol. 81, p. 106525, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106525.
[49] G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the internet of things," in *IEEE International Conference on Information Reuse and Integration (IRI)*, Aug. 2017, pp. 75–78, doi: 10.1109/IRI.2017.83.
[50] R. Thakore, R. Vaghashiya, C. Patel, and N. Doshi, "Blockchain - based IoT: a survey," *Procedia Computer Science*, vol. 155, pp. 704–709, 2019, doi: 10.1016/j.procs.2019.08.101.
[51] P. Karthikeyyan, S. Velliangiri, and I. T. Joseph, "Review of blockchain based IoT application and its security issues," in *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies*, Jul. 2019, pp. 6–11, doi: 10.1109/ICICICT46008.2019.8993124.
[52] N. Fotiou, V. A. Siris, and G. C. Polyzos, "Interacting with the internet of things using smart contracts and blockchain technologies," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11342, Springer International Publishing, 2018, pp. 443–452.
[53] A. Tandon, "An empirical analysis of using blockchain technology with internet of things and its application," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9S3, pp. 1469–1475, Aug. 2019, doi: 10.35940/ijitee.I3310.0789S319.
[54] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1–2, pp. 1–13, Sep. 2018, doi: 10.1016/j.iot.2018.05.002.
[55] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.
[56] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.
[57] A. Ukil, S. Bandyopadhyay, and A. Pal, "IoT-Privacy: to be private or not to be private," in *IEEE INFOCOM*, Apr. 2014, pp. 123–124, doi: 10.1109/INFCOMW.2014.6849186.
[58] EMSA, "Discussion paper: the distributed ledger technology applied to securities markets," *European Securities and Markets Authority*. 2016.
[59] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *International Conference on Advanced Communication Technology*, 2017, pp. 464–467, doi: 10.23919/ICACT.2017.7890132.
[60] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Scaiscio, "Semantic blockchain to improve scalability in the internet of things," *Open Journal of Internet of Things (OJIOT)*, vol. 3, no. 1, pp. 46–61, 2017.
[61] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, Jul. 2017, doi: 10.1007/s12083-016-0456-1.
[62] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," *Procedia Computer Science*, vol. 141, pp. 159–166, 2018, doi: 10.1016/j.procs.2018.10.162.
[63] S. K. Lo *et al*., "Analysis of blockchain solutions for IoT: a systematic literature review," *IEEE Access*, vol. 7, pp. 58822–58835, 2019, doi: 10.1109/ACCESS.2019.2914675.
[64] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and blockchain technology in supply chain management," *Future Internet*, vol. 11, no. 7, Jul. 2019, doi: 10.3390/fi11070161.
[65] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.
[66] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019, doi: 10.1109/JIOT.2018.2847705.
[67] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–32, Jan. 2021, doi: 10.1145/3372136.
[68] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 58, pp. 461–466, 2016, doi: 10.1016/j.procs.2016.09.074.
[69] A. S. Patil, B. A. Tama, Y. Park, and K. H. Rhee, "A framework for blockchain based secure smart green house farming," in *Lecture Notes in Electrical Engineering*, vol. 474, Springer Singapore, 2018, pp. 1162–1167.
[70] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, Dec. 2018, doi: 10.3390/s18124215.
[71] S. Mishra and A. K. Tyagi, "Intrusion detection in internet of things (IoTs) based applications using blockchain technology," in *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud*, Dec. 2019, pp. 123–128, doi: 10.1109/I-SMAC47947.2019.9032557.
[72] X. Wang *et al*., "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, Feb. 2019, doi: 10.1016/j.comcom.2019.01.006.
[73] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-based internet of things and industrial IoT: a comprehensive survey," *Security and Communication Networks*, vol. 2021, pp. 1–21, Aug. 2021, doi: 10.1155/2021/7142048.
[74] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends in Food Science and Technology*, vol. 91, pp. 640–652, Sep. 2019, doi: 10.1016/j.tifs.2019.07.034.
[75] M. A. Ferrag, L. Maglaras, and H. Janicke, "Blockchain and its role in the internet of things," in *Springer Proceedings in Business and Economics*, Springer International Publishing, 2019, pp. 1029–1038.
[76] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT based food traceability for smart agriculture," in *Proceedings of the 3rd International Conference on Crowd Science and Engineering*, 2018, pp. 1–6, doi: 10.1145/3265689.3265692.
[77] E. M. Dogo, A. F. Salami, N. I. Nwulu, and C. O. Aigbavboa, "Blockchain and internet of things-based technologies for intelligent water management system," in *Artificial Intelligence in IoT*, Springer International Publishing, 2019, pp. 129–150.
[78] S. B. Kadam and S. K. John, "Blockchain integration with low-power internet of things devices," in *Handbook of Research on Blockchain Technology*, Elsevier, 2020, pp. 183–211.
[79] M. Alamri, N. Z. Jhanjhi, and M. Humayun, "Blockchain for internet of things (IoT) research issues challenges & future directions: a review," *International Journal of Computer Science and Network Security*, 2019.

[80] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: a systematic literature review," in *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov. 2016, pp. 1–6, doi: 10.1109/AICCSA.2016.7945805.
[81] H. F. Atlam and G. B. Wills, "Intersections between IoT and distributed ledger," in *Advances in Computers*, vol. 115, Elsevier, 2019, pp. 73–113.
[82] F. A. Abadi, J. Ellul, and G. Azzopardi, "The blockchain of things, beyond bitcoin: a systematic review," in *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)*, Jul. 2018, pp. 1666–1672, doi: 10.1109/Cybermatics_2018.2018.00278.
[83] L. Hang and D.-H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, May 2019, doi: 10.3390/s19102228.
[84] L. Axon and M. Goldsmith, "PB-PKI: a privacy-aware blockchain-based PKI," in *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, 2017, pp. 311–318, doi: 10.5220/0006419203110318.
[85] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Computing*, vol. 4, no. 6, pp. 50–59, Nov. 2017, doi: 10.1109/MCC.2018.1081060.

BIOGRAPHIES OF AUTHORS

Mahmood Subhy Mahmood received the B.Sc. degree in Computer Science from Mosul University, Mosul, Iraq, in 2003 and the M.S. degree in Computer Science/Network Security from Mosul University, Mosul, Iraq, in 2011. Currently, he is Lecturer at the Department of Biology, Mosul University and he is a Ph.D. student in Computer Science Department in College of Computer Science and Math., Mosul University. His research interests include network security, internet of thing security, computer network, cyber security, programming, and artificial intelligence (AI). He can be contacted at email: mahmoodsubhy1981@uomosul.edu.iq.

Najla Badie Al Dabagh received her B.Sc. degree in computer science from Mosul University, Iraq in 1988, M.Sc. degree in Computer Science\Data Security from Technology University, Iraq in 1995 and Ph.D. degree in Network security from Mosul University, Iraq in 2006. Currently she is an Associate Professor at the department of Computer Science, College of Computer Science and Mathematics, Mosul University. Her research interests include cryptography, honeypot and intrusion detection, IoT security, network security, and AI. She can be connected at email: najlabadie@uomosul.edu.iq.