*inventions*

*Review*

# Blockchain and 6G-Enabled IoT

**Houshyar Honar Pajooh [1,*], Serge Demidenko [1], Saad Aslam [1] and Muhammad Harris [2,3]**

[1] School of Engineering and Technology, Sunway University, Selangor 47500, Malaysia
[2] Massey Agrifood Digital Labs, Massey University, Palmerston North 4472, New Zealand
[3] Department of Industrial and Manufacturing Engineering, Rachna College of Engineering and Technology, Gujranwala 52201, Pakistan
[*] Correspondence: houshyarh@sunway.edu.my

**Abstract:** Ubiquitous computing turns into a reality with the emergence of the Internet of Things (IoT) adopted to connect massive numbers of smart and autonomous devices for various applications. 6G-enabled IoT technology provides a platform for information collection and processing at high speed and with low latency. However, there are still issues that need to be addressed in an extended connectivity environment, particularly the security and privacy domain challenges. In addition, the traditional centralized architecture is often unable to address problems associated with access control management, interoperability of different devices, the possible existence of a single point of failure, and extensive computational overhead. Considering the evolution of decentralized access control mechanisms, it is necessary to provide robust security and privacy in various IoT-enabled industrial applications. The emergence of blockchain technology has changed the way information is shared. Blockchain can establish trust in a secure and distributed platform while eliminating the need for third-party authorities. We believe the coalition of 6G-enabled IoT and blockchain can potentially address many problems. This paper is dedicated to discussing the advantages, challenges, and future research directions of integrating 6G-enabled IoT and blockchain technology for various applications such as smart homes, smart cities, healthcare, supply chain, vehicle automation, etc.

**Keywords:** 6G; blockchain; Internet of Things

check for updates

**Citation:** Pajooh, H.H.; Demidenko, S.; Aslam, S.; Harris. M. Blockchain and 6G-Enabled IoT. *Inventions* **2022**, *7*, 109. https://doi.org/10.3390/inventions7040109

Academic Editors: Paolo Attilio Pegoraro and Emilio Ghiani

Received: 21 October 2022
Accepted: 24 November 2022
Published: 28 November 2022

## 1. Introduction

Following the large-scale commercial deployment of 5G (as well as beyond 5G) networks, there have been substantial developments in the sixth generation generally (6G) of mobile communication. It is anticipated that the introduction of the 6G will bring significant benefits to human productivity and lifestyles. In September 2018, the Federal Communications Commission (FCC) discussed 6G technology for the first time. It was mentioned that the 6G frequency band would advance into the TeraHertz (THz) range in the near future. The FCC decided in March 2019 to open the THz frequency band from 95 GHz to 3 THz for 6G network trials. It was suggested in January 2020 that it was essential to vigorously promote and engage in preliminary research for forward-looking and essential 6G technologies. It has been expected that the standardisation of 6G could take place around the year 2025 and that the 6G pre-commercial networks will be put into use around the year 2030 [1].

To be applicable, 6G needs to provide ubiquitous security [2]. In addition, this is where the blockchain and distributed ledger technologies (DLT) are essential. The blockchain was initially introduced for cryptocurrencies. However, at present it has found applications well beyond that field, e.g., in wireless communications, smart grids, the Internet of Things (IoT) and many others [3–5]. The 6G should support Reconfigurable Intelligent Surfaces (RIS), smart cells working with Artificial Intelligence (AI), and potentially operate in TeraHertz frequency bands [6]. A trustworthy environment will be required to implement these technologies [3]. This will be complicated as the network density expects to increase tremendously thus putting additional pressure on the network resources and maintenance schemes.

There is a growing consensus that blockchain, a popular kind of distributed ledger technology, will play a crucial role in the future of mobile communication systems. Whether or not 5G networks will be useful has become a popular area of study in just the last few years [7,8]. Blockchain technology is considered to be crucial for the safe and full automation of the next generation of mobile networks, particularly 6G, which will be progressively softwarized, decentralised, and a mesh of open systems. Particularly, the use of blockchain technology is anticipated to improve both the technical aspects of 6G (such as security, privacy, network service management, resource utilisation, and spectrum management) and the applications of 6G (such as healthcare, energy Internet, unmanned aerial vehicles (UAVs), autonomous vehicles (CAVs), and extended reality (some of these applications are discussed in detail in Section 4). To realize these applications, researchers have begun to investigate blockchain's potential impact on 6G networks [9–11]. It is important to understand that new and improved decentralized techniques and means would be required. When it comes to network security and openness, blockchain can provide distributed functionality. An important aspect of blockchain technology is its adaptability (as depending on the applications, its appropriate components can be adjusted).

A blockchain is a decentralised distributed ledger maintained by an underlying peer-to-peer (P2P) network of nodes. A blockchain, as its name suggests, consists of a series of blocks of transactions that are logically linked or chained together to form a digital record. Verified transactions within a particular time range are then grouped into a unit known as a "block". Consequently, each block has a fixed number of transactions. Using cryptographic hashes, these blocks are logically linked in the order of their generation. This means that each block stores the previous block's hash value in the "previous block hash" field. The initial block, known as the "genesis block", has no predecessors. The prior block hash field of the genesis block is therefore set to all zeroes. The digital ledger contains all prior transactions in chronological order and is encrypted. In addition, every node in a peer-to-peer blockchain network replicates this ledger. Because write operations are executed only in append mode, the distributed ledger continues to grow over time.

From a technological standpoint, blockchain is viewed as a single technological invention that is a powerful combination of concepts, methodologies, and technologies. Blockchain, for instance, employs cryptographic techniques such as public key infrastructure (PKI), hashing, digital signatures, and the Merkle tree. It also uses P2P technology to connect nodes (also known as miners) in order to create a blockchain network. A consensus mechanism also allows nodes in the blockchain network to stay in sync and agree on the current state of the distributed ledger. Blockchain promises to resolve issues such as peer-to-peer transactions without involving third parties running centralised mechanisms. Blockchain also helps to deal with fraudulent duplication of digital assets (e.g., double spending) and establishing trust through pseudonymity, transparent yet immutable recordkeeping.

In the era of 6G, it is intended that blockchain implementations will be deployed and interconnected in such a way that they will span different network domains (i.e., core, transport, edge, and access networks) and drive a complex 6G ecosystem. The concept of blockchainized 6G refers to an ecosystem where the blockchains will become integrated, inherent to, and widespread throughout the entire environment. This will offer various additional benefits to the domain of 6G. For example, blockchain has a tremendous amount of potential to enable and enhance a large number of key 6G functionalities, such as the automation of network management; the dynamic spectrum management of THz communication; AI-powered edge computing; federated resource sharing in trustless environments; and the security of Machine Learning (ML) and Federated Learning (FL) models [12]. The blockchainized version of 6G could also help to develop new 6G applications, such as connected autonomous vehicles, the energy internet, extended reality, swarms of unmanned aerial vehicles, digital twins, industry 5.0, and smart healthcare based on the intelligent internet of medical things.

The emergence of IoT facilitates sensing capabilities, actuation, and over-the-internet communications, hence giving a new approach to handling a variety of commercial, government, and public/private sector concerns and issues [13]. IoT devices range from tiny wearable sensors to sizable hardware platforms. IoT systems have numerous important applications in a variety of fields. However, they also pose a number of challenges. For example, the heterogeneity of devices and networks needs standard protocols to optimize IoT integration and eliminate vertical silos. IoT data transparency is another significant challenge. The large volumes of generated data should be secured and not be tampered with, falsified, or altered in any way. A single point of failure can lead to malfunctions of several entities of a centralized IoT architecture. Distributed services are a promising solution to provide trustworthiness in IoT data, which guarantees data's immutability by all its participants. Blockchain-based technology plays a crucial role in developing distributed and secure networks [14]. A blockchain is an immutable and distributed ledger that is deployed in a P2P network structure. Blockchain secures transactions during registration and updates them in a distributed architecture. IoT systems can potentially utilize the blockchain to secure the IoT system and devices.

The purpose of this article is to analyse the integration of blockchain technology in 6G to provide a comprehensive understanding of the advantages that may be realised in the 6G era. Specifically, the motivation is to present the most important research questions targeting the use of blockchain technology for 6G and bring these to the attention of concerned researchers. The current research trends show that the community has gained pace toward the development of 6G and its integration with blockchain technology. Thus, this paper provides a comprehensive review of related and most recent research trends.

This research paper discusses the trends influencing the future growth of 6G and its enabling technologies. An in-depth analysis of the trends and applications that the merger of 6G-enabled IoT and blockchain can present is discussed which helps in explaining the specific requirements of 6G and paves the way for a comprehensive investigation into the integration of blockchain in the 6G ecosystem.

The contributions of this work are as follows:

1. A comprehensive discussion on the integration of 6G-enabled IoT and blockchain technology has been presented. It is seen in the recent literature that these technologies are discussed separately however, we believe their integration has numerous benefits and embodies new applications, discussed in detail later in the manuscript.
2. The security of IoT-based applications is of paramount importance. This study presents the inherent security benefits of using 6G-enabled IoT with blockchain technology. This also serves as a solid foundation for Industry 5.0-related research.

This paper is organized as follows. Section 2 presents the related work and fundamental technologies enabling the 6G-IoT networks. The blockchain for 6G-IoT is discussed in Section 3. Section 4 explores the blockchain-enabled opportunities in 6G-IoT. Discussion around the deployability of blockchain in 6G is presented in Section 5. Finally, Section 6 concludes the article.

## 2. Technology Definitions and Related Work

### *2.1. 6G Technology*

The motivation behind the 6G technology is the support for device proliferation and mobile data trafficking. The shift to 6G aims to enhance connectivity for everyone and everything from everywhere through a highly scalable and flexible network structure. The new structure requirements include a higher data rate, low latency, and cost, as well as energy reduction [15]. The ubiquitous connectivity of 6G will enable a multitude of industrial applications such as smart energy networks, smart mobility applications, industrial IoT, smart health, and AR/VR-enhanced consumer services [16]. A comparison of technological advancement offered by various cellular generations is presented in Figure 1.

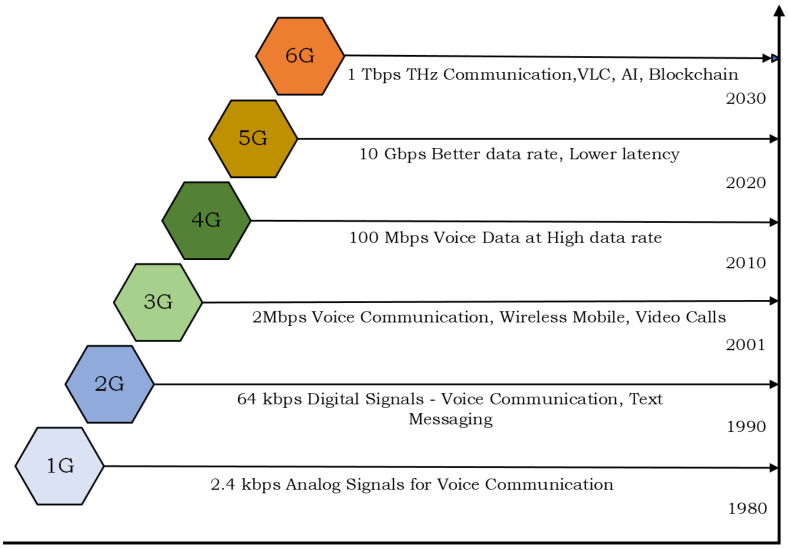
6G
1 Tbps THz Communication,VLC, AI, Blockchain
2030
5G
10 Gbps Better data rate, Lower latency
2020
4G
100 Mbps Voice Data at High data rate
2010
3G
2Mbps Voice Communication, Wireless Mobile, Video Calls
2001
2G
64 kbps Digital Signals - Voice Communication, Text Messaging
1990
1G
2.4 kbps Analog Signals for Voice Communication
1980

**Figure 1.** Cellular technology evolution.

It is anticipated that 6G will provide a significant increase in the data rate (about 1000× compared to 4G) and is expected to be 100 times faster than 5G and is likely to offer enhanced reliability and wider network coverage. In addition, it will support a higher edge rate of up to almost 1 Gbps. It is important to mention that the cell load and size affect the edge rate. The peak rate is a marketing factor, and it is expected to reach about 10 Gbps. New applications of 6G, including virtual reality, machine-to-machine communication, cloud-based technologies, two-way gaming, etc., need a round-trip latency of about 1 ms. The technologies associated with 6G, such as the use of the mmWave spectrum (with frequencies ranging up to the sub-THz range of 300 GHz), new base stations and small cells offer reasonable cost and power scaling capability.

In addition to the protection offered by encryption technology, a higher level of security will need to be offered by further developing the physical layer security system. This should be applied to a wide variety of computers and gadgets.

It is expected that the overall capabilities of 6G will be anywhere from 10 to 100 times higher than those of 5G. It will be capable of providing full coverage and ultra-wireless connectivity while integrating terrestrial wireless mobile, short-range direct, and medium/low orbit satellite communication technologies and relevant resources. In addition, 6G will incorporate a wide variety of technologies, including communication, computation, navigation, location, perception, control, sensing, buffering, imaging, and artificial intelligence, among others. Some of the essential technologies that will be used in 6G networks include THz band communications, Inertial Measurement Systems (IMS), Holographic Beamforming (HBF), Orbital Angular Momentum (OAM) multiplexing, Visible Light Communications (VLC), blockchain-based spectrum sharing, nano-Internet, and others.

Advanced 5G communication networks offer three different service options that are selected depending on the type of application being used. They are Massive Machine-Type Communications (mMTC), Enhanced Mobile Broadband (eMBB), and Ultra-Reliable and Low Latency Communications (URLLC) [17]. The first of them, i.e., mMTC, helps to increase the number of supported devices and provides support for low-cost devices while the second one (i.e., eMBB) improves the spectral efficiency and peak throughput. Finally, URLLC targets end-to-end latency reduction and data transmission robustness. However, such an options arrangement might not be sufficient for 6G where the multitudinous nature and complexity of the tasks and processes would lead to varying and even conflicting requirements.

Several 6G-related developments have begun to emerge targeting the following areas; network density; connectivity of diverse communication networks; convergence of Communication, Caching, Computation, Control, Sensing, and Localization; transition to network intelligence; and the shift from the centralization to dispersal and distributed arrangements. Consequently, 6G has to have the capacity to link millions of devices and applications while simultaneously offering assured performance. Thus, 6G will play a crucial role in addressing the vast interconnectedness and highly diversified service requirements of the Internet of Things thus creating, the so-called, 6G-enabled IoT (or just 6G-IoT). 6G will have a new network design and new technologies that will make it possible for a huge number of IoT devices to work together. Enhanced Mobile Broadband Plus (eMBB-Plus), Big Communications (BigCom), Secure Ultra-Reliable Low-Latency Communications (SURLLC), Three-Dimensional Integrated Communications (3D-InteCom), and Unconventional Data Communications (UCDC) are all expected to be utilised within 6G.

### *2.2. 6G-Enabled IoT*

THz communications are expected to be a key technology for 6G-IoT with data rates of 100 Gbps or more and latency times of milliseconds or less. It is also expected that the THz band of 0.1–10 THz will be able to address the 6G-IoT application needs, such as picosecond level symbol endurance, integration of thousands of submillimeter-long antennas, and weak interference without full legacy control [18].

6G will provide a platform for connecting billions of smart devices. Massive IoTs bring ubiquitous smart devices that can interact and share data with each other without human interference. Current IoT systems use various wireless technologies such as sensor networks, ZigBee, Near-Field Communication (NFC), Low-Energy Bluetooth (BLE), and Radio Frequency Identification (RFID) [19]. Unfortunately, these technologies may not be sufficient for new efficient IoT system implementations aiming at novel industrial applications. The limitations of these technologies are security concerns, privacy, latency, and lack of regulations and standards [20]. New technology is required to provide high bandwidth for transmitting the vast amount of data generated from the numerous smart devices in the IoT system. Furthermore, new and improved technology is required to address the prime requirements of the next generation of IoT devices including higher data rate, expanded bandwidth capacity, and decreased latency [21]. 6G technology meets the requirements of ubiquitous IoT computing applications as well as the need for higher availability, enhanced scalability, reduced latency, increased data rates, lower energy consumption, etc. [22,23]. The 6G-IoT integration changes the landscape of different industries with device-to-device and machine-to-machine communications. It also facilitates the proliferation of IoT-enabled smart devices. End-users, businesses, governments, and public authorities benefit from the rise in the number of fragmented and heterogeneous devices and the fast growth of IoT systems.

Mobile connectivity has grown significantly in recent years, driven by the proliferation of smart devices and the quick development of wireless communication technology [24]. It is predicted that mobile traffic on a global scale will grow to reach over 5000 exabytes in 2030. Growing communications involving future smart gadgets will be supported by networks powered by low-earth orbit satellites and broadband access platforms. Furthermore, in order to offer seamless connectivity across future large-scale IoT networks, the use of flying platforms will also be required in situations where fixed base stations are unable to guarantee steady and reliable device communications.

The URLLC technology was developed and employed in real-world IoT solutions based on 5G. However, it still needs to be improved to make 6G-IoT networks more useful for applications such as fully autonomous IoT systems and flying IoT systems. Significant architectural changes of existing mobile networks will be required in order to introduce new vertical IoT applications in future intelligent networks (e.g., for autonomous driving and e-healthcare). In this case, the network communication standards and protocols become very important to the large-scale deployment of 6G-IoT ecosystems as they work with important computing (e.g., edge, cloud) and wireless services.

Future 6G-IoT networks are expected to rely on smart devices where edge intelligence and computing could be fully realized. Each IoT smart device would be able to operate as an end-user terminal while providing connectivity and services (e.g., intelligent control, caching, and network signalling) to other devices at the network edge without the need for a centralized controller. This could be expanded to demand-driven opportunistic networking adapting to various users, services, or network requirements, such as energy cost minimization or spectrum efficiency maximization.

### *2.3. What Is Blockchain?*

In 2009, Satoshi Nakamoto implemented a decentralized digital currency known as Bitcoin [25]. The promising fundamental technology behind digital currency was named a "blockchain". A cryptographically secured network consists of untrustworthy peers interacting in a distributed peer-to-peer manner. The blockchain is described as a distributed ledger consisting of immutable and verifiable transactions. Timestamped blocks are linked through cryptographic hashes to create a chain [26]. The cryptographic techniques (such as symmetric and asymmetric algorithms) verify all interactions. Blockchain technology does not need third-party authority to hold network control. All nodes and participants store a copy of the blockchain ledger as well as transactions [27]. The tracking and ownership management of assets (coins) is facilitated by a proof of work (PoW) as a consensus algorithm while using public-key cryptography. The consensus algorithm evaluates the reliability and validity of all transactions when a new block is added to a previous block. The nodes will reach a consensus when 51% of the nodes are truthful. Blocks in the blockchain are a collection of transactions that are bundled together by using the Merkle tree (a binary hash tree in which each leaf represents the data hash). Integrity, immutability, transparency, non-repudiation, and equal rights are the principal properties of the blockchain system.

The immutability of blockchain means that data cannot be changed once it has been stored on the blockchain. Simplified blockchain architecture is shown in Figure 2.

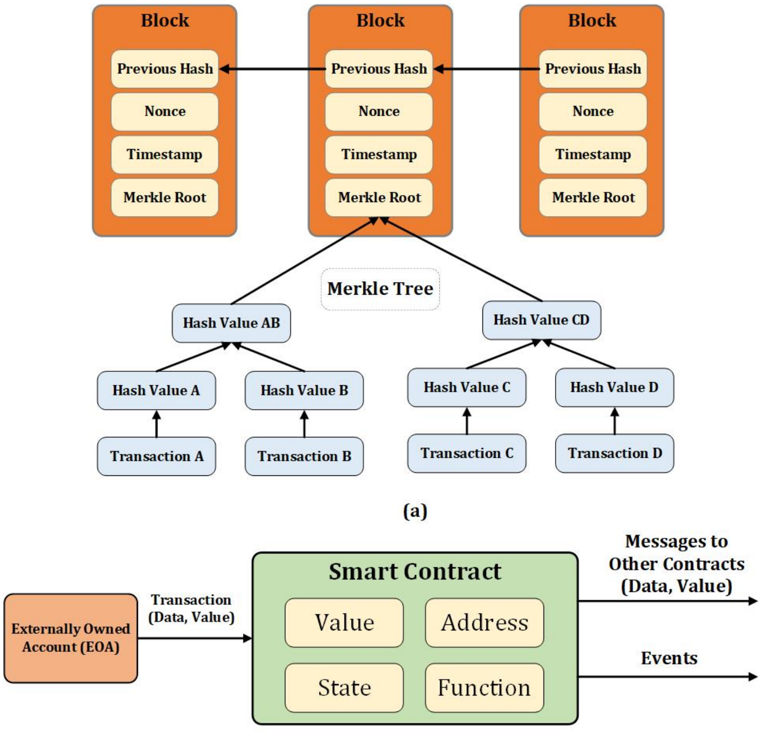

**Figure 2.** (**a**) Simplified blockchain structure. (**b**) Smart contracts.

### 2.3.1. Blockchain Implementation Types

There are three main types of blockchain implementation based on the level of access granted to nodes and users participating in the network. They are (i) public blockchain (permissionless), (ii) private blockchain (permissioned), and (iii) consortium blockchain.

The first category allows an unlimited number of nodes to join and read the public blockchain anonymously. The nodes can securely communicate using a pair of public and private keys. The nodes can participate in the consensus process after validation. Bitcoin and Ethereum are an example of this type of blockchain.

The second type provides permission only to private members for contributions in the consensus (trustful members can validate the transactions only). There is a restriction for the nodes to participate in this type of blockchain.

The consortium blockchain includes chosen miners [25] in advance and is not entirely decentralized. Pre-selected nodes can contribute to the consensus process

### 2.3.2. Blockchain Components

The four main pillars of blockchain technology are consensus, ledger, cryptography, and smart contracts [28]. PoW verifies all network actions. This method maintains the history of transactions and keeps the entire network from being dominated by a miner node. The information about all transaction details within the network is stored in an immutable and shared ledger. Cryptography is used to secure all network and ledger data by cryptographic encryption and prevent unauthorized users from decrypting this information. Smart contracts facilitate the verification and validation of network participants.

### 2.3.3. Blockchain Architecture

Blockchain technology was initially developed for Bitcoin. However, it can be implemented regardless of the currency. A distributed blockchain network architecture is formed in a peer-to-peer network manner. A group of nodes (data centres, devices, computers, etc.) sharing information in a P2P way on top of the network layer. Therefore, the blockchain is a transparent and secure decentralized transactional database.

### 2.3.4. Nodes

Nodes play a crucial role within the blockchain network. They are responsible for carrying out mining [25] functionality as well as routing and storing data. They also perform transaction verification and broadcast them. All the nodes maintain peer-to-peer connection discovery and establishment. The nodes use the discovery protocol to find other peers and connect to them using a particular TCP port. They save a ledger copy, which is a copy of all transaction history. Therefore, a centralized server is not required to store this information. Miners validate and verify all the transactions that have happened within the blockchain network.

### 2.3.5. Blocks

The block contains primary data, previous block hash, current block hash, timestamp, and other information. The first block in the blockchain is called the genesis block. Primary data are application-dependent. They are described based on the type of application blockchain is implemented (e.g., IoT data transaction). A transaction is hashed to code before execution and is broadcasted to each node. The Merkle tree function generates the final hash value known as the Merkle tree root that is placed in the block header. The timestamp shows the generated block time. A block also includes a node value, a block signature, user-defined data, etc.

### 2.3.6. Merkle Tree and Hash Function

The transaction history and related information are stored in a Merkle Tree associated with each block in the blockchain network. The hash tree or Merkle tree performs the transaction storing within a block along with all other transactions' hash values. This method performs hashing a large set of "chunks" of data together, which is based on the "chunks into buckets" division. Generally, a bucket includes a few chunks. Taking the hash of each bucket and repeating the process in a bottom-to-up manner is facilitated through implementing double SHA-256 hash until the tree's root.

#### 2.3.7. Transactions

In a most general sense, transactions are an unencrypted data structure stored in files known as blocks in the blockchain. Transactions form links with previous transactions to build a chain of blocks. A public key and the generated hash from it are used to sign the previous transaction digitally by the owner. Following this process, the previous transaction owner uses its private key to sign the hash. The transaction structure fields are shown in Figure 2. Miners are paid to guarantee the blockchain network's security and consistency with fees for transactions, which are calculated automatically. Figure 2 presents the chain of ownership within the blockchain network.

#### 2.3.8. Mining

The blockchain guarantees security through the mining process to verify, create, publish, and broadcast blocks in the blockchain. Transaction verification and validation are the primary responsibilities of the mining process. An incentive-driven model is being used to generate new coins [25] for the blockchain network through the mining process. The miners who can solve the next block in the blockchain receive these new coins as a reward. The mining process starts with calculating the blockchain difficulty results and choosing the block with the highest level of difficulty. After a specified interval, all full nodes contribute to estimating the level of difficulty. The increase or decrease in the difficulty level depends on the time duration for generating a certain interval of blocks. The block creation rate increases with each increment in the number of miners. It leads to an increase in average consensus time as well as a difficulty level. Such a time is at a rate of ten minutes in the case of Bitcoin. Following this process, the Merkle tree is constructed based on block information and transaction history downloaded by miners, which results in making the Merkle root. The maximum block size limits the size of the block added to the blockchain. However, a miner can select the desired transaction numbers. In Bitcoin, this maximum size is 1 MB to accommodate transactions within this space. In the next step, the miner matches the difficulty level of the blockchain network with the hash that is formed from the block header values. The implemented consensus algorithm within the blockchain produces this hash. The primary concern in a computing system with distributed multi-agents is network reliability. This system requires agents to deploy an agreement process based on a particular data value for computational purposes. There might be some faulty agents in the system thus causing the unreliability. Therefore, a consensus algorithm could be chosen to address such an issue. The main consensus mechanisms used in the blockchain are listed as follows:

- Proof of Work (PoW);
- Proof of Stake (PoS);
- Proof of Concept (PoC);
- Proof of Authority (PoA);
- Delegated Proof of Stake (DPoS);
- Practical Byzantine Fault Tolerance (PBFT).

Blockchain technology offers many technological advantages for applications in diverse areas such as those in the IoT domain. A comparison of different blockchain technology platforms for IoT applications is presented in Table 1.

**Table 1.** Blockchain Platforms for IoT Applications.

| Blockchain Platform | Blockchain Type | Used Consensus | Crypto Currency | Smart Contracts |
|---|---|---|---|---|
| Ethereum | Public and permission-based | PoS | Ether (ETH) | Yes |
| Hyperledger Fabric | Permission-based | PBTF/SIEVE | None | Yes |
| Multichain | Permission-based | PBTF | Multi-currency | Yes |
| Litecoin | Public | Scrypt | litecoins (LTC) | No |
| Lisk | Public and permission-based | DPoS | LSK | Yes |
| Quorum | Permission-based | Multiple | ETH | Yes |
| HDAC | Permission-based | ePoW,Trust-based | Multi-asset | Yes |

## 3. Blockchain and IoT Integration

Rapid development offered by new IoT services and smart applications has been associated with the proliferation of heterogeneous smart devices and the growth of a number of access points. In turn, the number of seamless interactions and shared information in the network increases dramatically. The existing centralized cloud-based platforms and services contribute considerably to the revolutionization of IoT systems. However, they have several drawbacks. A tremendous amount of data is generated from a vast number of heterogeneous smart devices and objects. At the same time, the network contributors do not observe the use of the information they supply to the cloud service provider. In addition, the centralized data storage requires significant network bandwidth. Moreover, providing data transparency through a centralized architecture is a significant challenge [29,30]. The central point of failure acts as a black box to the centralized system mode [31,32]. Providing synchronization to external computing resources is another challenge for centralized IoT security and performance [31].

Establishing a high level of security and privacy in 6G-based IoT networks is a practical challenge since they tend to be distributed and thus are more susceptible to attacks and threats. Achieving the requirement of keeping the data private in open sharing systems in multi-layer 6G systems (such as the exchange of data between autonomous vehicles) is also crucial. As an emerging disruptive technology, blockchain is capable of providing novel solutions to successfully address privacy and security concerns in 6G-IoT networks. The blockchain is conceptually a decentralised, immutable, and transparent database in which no central authority is required to handle the data. This is made possible by a peer-to-peer network structure that gives each entity (such as an IoT device) an equal right to control and authorise the data recorded in the blockchain. The adoption of blockchain technology with IoT will develop the data-sharing structure through trustability, audibility, and openness. The exchange of information in such an enhanced architecture occurs on a traceable and reliable platform. The benefits of this integration are outlined in Figure 3 and can be summarized as follows [33,34].

1. Publicity. The ledger is shared between all participants, giving them a clear view of all transactions and blocks. The participant's private keys encrypt the block's content. IoT users' privacy is guaranteed in the blockchain-based platform, while heterogeneous and fragmented smart devices share information.
2. Scalability and Decentralization. Avoiding the reliance on a single authority for transaction approval presents a much needed decentralized structure.
3. Security. The security of the vast number of untrusted IoT participants is improved in the blockchain architecture. Participants employ smart contracts to exchange information. Thus, it helps to enhance inter-network communication security.
4. Autonomy. Blockchain eliminates third-party authority and intermediate involvement.
5. Immutability. One of the main advantages of the blockchain system is an immutable ledger. Distributed ledger modification is performed by the majority of nodes within the blockchain network thus eliminating the transactions from alteration and deletion.
6. Reliability. The shared information between network participants is verified by all nodes with certainty to achieve accountability. All blockchain participants verify transaction authenticity.

7. Identity. The use of the blockchain-based platform enhances the IoT device's identification. Furthermore, the authentication and authorization of IoT devices on the network are improved by means of trustability.
8. Secure Code Deployment. Carrying out updates and changes in heterogeneous devices by different vendors is possible within the secured blockchain system. Moreover, the immutable ledger facilitates the updated history of each device to be tractable.

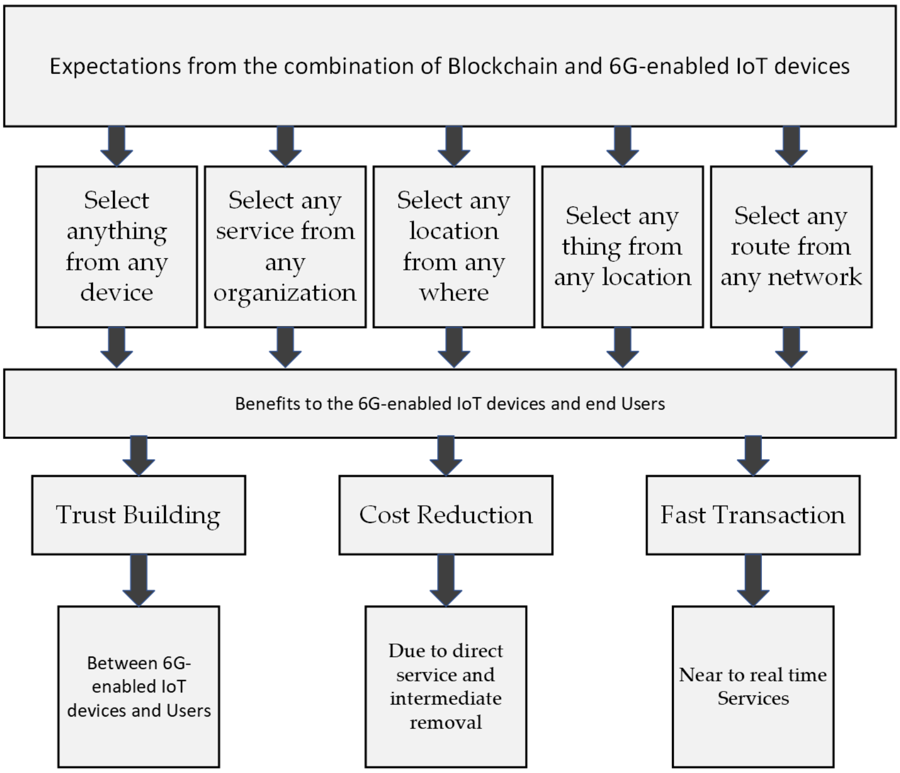
Expectations from the combination of Blockchain and 6G-enabled IoT devices
Select anything from any device
Select any service from any organization
Select any location from any where
Select any thing from any location
Select any route from any network
Benefits to the 6G-enabled IoT devices and end Users
Trust Building
Cost Reduction
Fast Transaction
Between 6G-enabled IoT devices and Users
Due to direct service and intermediate removal
Near to real time Services

**Figure 3.** Expansion from the combination of Blockchain and 6G-enabled IoT.

## 4. Blockchain for 6G-Enabled IoT

Blockchain is a promising solution in 6G-IoT automation, particularly in applied domains. For example, blockchain is capable of establishing secure autonomous systems where UAVs can act as blockchain clients to communicate with ground base stations in order to exchange and share data for their missions (e.g., emergency search tasks, environmental monitoring, etc.). By utilising blockchain, UAVs, terrestrial users, and network operators can rely on the data stored on the distributed ledger, which provides shared control and tracing rights across a distributed environment. Smart healthcare is another potential IoT application. Blockchain and its inherent smart contract technology can be used to implement the verification of health data in 6G-based healthcare systems where no third party would be required while ensuring a high level of trust.

However, the implementation of blockchain in future 6G-IoT networks may be characterised by higher costs in terms of latency and energy consumption. The mining process (such as block verification and information exchange between miners) could cause excessive network delays and excessive energy consumption. Thus, when applying blockchain technology to future IoT networks, it is essential to consider operational expenses.

The blockchain technology principle was described in Section 2.3. Many industries and applications benefit from blockchain deployment including IoT networks. The 6G and blockchain integration within the IoT system is intended at improving the system security and attaining larger bandwidth while minimizing operating and capital expenditures. Adopting blockchain technology in IoT systems was reported in the literature (e.g., [26,35]) showing benefits in areas such as security, privacy, scalability, and energy efficiency. Different aspects of decentralized consensus [36] and smart contracts [37] were reviewed within the IoT domain. Therefore, the detailed summary of the existing blockchain technology applications in IoT systems is discussed in the following subsections. Figure 4 depicts blockchain applications in 6G-enabled IoT.

The 6G-IoT integration can be categorized into the following sub-classes based on the different technical aspects of blockchain technology.

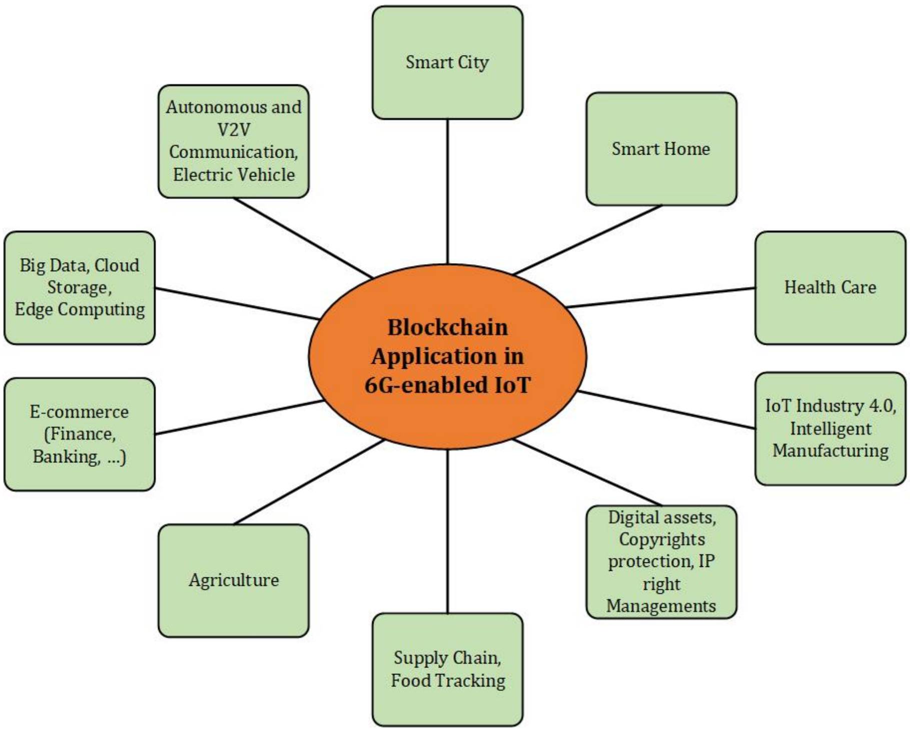
Smart City
Autonomous and V2V Communication, Electric Vehicle
Smart Home
Big Data, Cloud Storage, Edge Computing
Health Care
Blockchain Application in 6G-enabled IoT
E-commerce (Finance, Banking, ...)
IoT Industry 4.0, Intelligent Manufacturing
Agriculture
Digital assets, Copyrights protection, IP right Managements
Supply Chain, Food Tracking

**Figure 4.** Blockchain applications in 6G-enabled IoT.

### *4.1. Smart Contract-Based E-Commerce*

Smart contracts present a suitable solution to enhance decentralized e-commerce and smart property trading. The smart contract helps the trading entities to program a potential contract with a piece of code, which is encrypted and recorded in the blockchain system as a public ledger. Traders do not need to rely on a third party in the trading process. The piece of code is shared between all network participants in a transparent and tamper-resistant form. The automatic execution of smart contracts is based on meeting predefined rules and conditions within the system. The rules allow the participants to decrypt specific smart contracts making the trading procedure protected. In the event the system needs to use currency, self-defined cryptocurrencies such as IoTcoin can be used. Any registered property in IoT systems, such as IoT data and services, can be treated as trading assets. Slock and Filament are two examples of smart contract implementation.

### *4.2. Intelligent Manufacturing*

Manufacturers industries applied the IoT technology for quality assurance and logistics. The integration of IoT and blockchain paradigms promise to significantly improve the following manufacturing and logistic aspects [38].

1. Intelligent Maintenance and Diagnostics. Self-service diagnostic and smart maintenance applications can be implemented within the joint IoT-blockchain system. Procurement procedures can be automated by using smart contracts between manufacturers and vendors.
2. On-Demand Production and Manufacturing. All the manufacturers and their customers (consumers) can participate in a joint IoT-blockchain system. Peer participants

can update a copy of the local blockchain ledger. Customers can write their needs and requested products into a blockchain-based system to automate production.

3. Supply Chain and Asset Tracking. As a shared ledger, blockchain could record all product information, including fabrication date, item identity, materials, manufacturer information, etc. In addition to that retailers' and logistics information also could be recorded in the blockchain system. In addition, the integration of blockchain and industrial IoT facilitates asset and supply chain product tracking.
4. Traceability. Smart contracts can be used to facilitate traceability applications. All product information and production records are stored in the blockchain. Customers and manufacturers can perform trades based on smart contracts with predefined rules.
5. Inventory and Asset Registry. Manufacturers' assets and inventory can be recorded in a secure and trustable ledger while eliminating third-party involvement.
6. Product Certification. Protecting product certification from counterfeits would become much easier and more trustworthy since all the relevant information is recorded in the blockchain system in a traceable manner.
7. Supplier Identity Management and Reputation. Customers and manufacturers could use the industrial IoT-blockchain system to keep their desirable requirements. It enhances the management of the supplier's identity and reputation, which can be tracked based on performance indicators such as recorded customers' feedback, delivery time, sellers' reviews, and ratings among others.
8. Machine-to-Machine and Machine-to-Customer Transactions. Manufacturing services can be automated by means of machine-to-machine and machine-to-consumer applications on a blockchain platform.

### *4.3. Decentralized Data Storage*

Existing IoT systems typically use centralized cloud computing platforms. Data are collected from heterogeneous IoT devices and end-users and stored in a third-party cloud platform by various providers. A centralized cloud server poses a single point of failure vulnerability in IoT systems and may result in data exposure. The centralized cloud storage can be substituted with decentralized and distributed solutions provided by the blockchain. The advantages of such blockchain-enabled distributed data storage include enhanced network robustness, increased data privacy and security, reduced cost, etc.

### *4.4. Big Data*

The use of blockchain in various industrial sectors such as finance and banking can largely reduce the issues of traditional real-time transfers (e.g., double-spending). The blockchain-enabled service is a promising solution to avoid these risks. Big data tools and analytics make the procedure much easier while identifying different customer patterns and making faster transactions. Human genetic data will play a vital role in future IoT-enabled industries due to the benefits of the smart production concept. Blockchain brings an important addition to that by providing enhanced privacy, security, efficiency, and resiliency of a vast amount of the associated data [39].

### *4.5. Smarter Society*

The 6G-enabled IoT represents a significant change compared to previous wireless technologies in terms of societal impact. Technologically enriched connectivity is embedded in every sector of society to make homes and cities smarter. The interaction with devices at home is automated using different applications in the IoT system in a real-time and uninterrupted manner. A smart home infrastructure provides network connectivity for heterogeneous devices, IoT sensors, and remote access-enabled mobile applications. Smart homes provide most of the essential services, including smart lighting, smart thermostats, smart surveillance cameras, smart parking, smart environmental tools, and smart door locks. Smart homes implemented with a blockchain-enabled IoT remove interoperability issues between different home devices as well as security and privacy challenges. 6G-enabled IoT system integration with blockchain also provides a platform for secure connectivity of home devices and sensors with reliability guarantees and sufficient bandwidth [40]. The smart city notion responds to unprecedented urban growth and its associated problems, such as resource constraints and an increase in the population. The smart city facilitates the efficient and optimal use of resources. The smart city vision aims to provide enhanced communication technologies to support a better quality of service for the public administration of the city and for the citizens [41]. The core aspect of the smart city is the collected information coming from heterogeneous IoT devices. Key aspects of the smart city are illustrated in Figure 5. The distributed nature of entities in a smart city poses the need to have a robust solution to tackle security and privacy issues. The integration of blockchain technology with the upcoming 6G technology paves the way to address the aforementioned goals for entity communication in a smart city [42]. The blockchain-enabled architecture should be able to provide fast and reliable communication, fault tolerance, efficiency, optimal operation, and scalability.

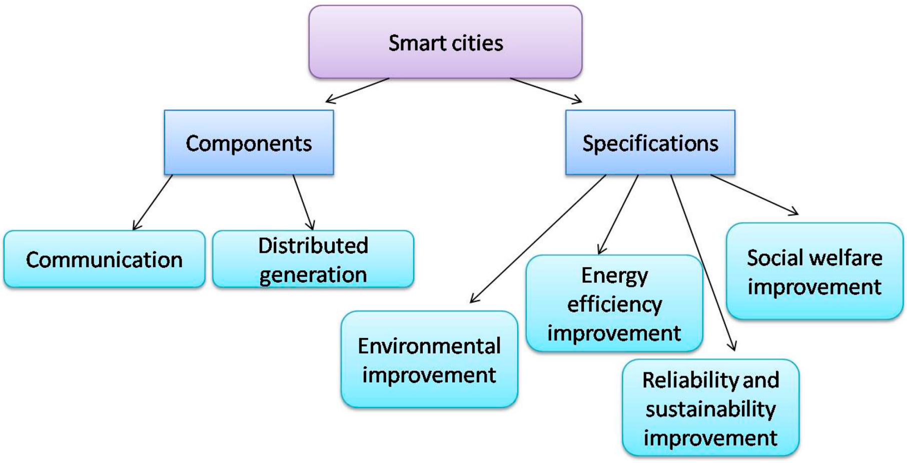
Smart cities
Components
Specifications
Communication
Distributed generation
Environmental improvement
Energy efficiency improvement
Reliability and sustainability improvement
Social welfare improvement

**Figure 5.** The aspects of a smart city.

### *4.6. Privacy and Security Management*

With the wide range of applications supported by IoT, new use cases are aggressively investigated. Each application involving IoT generates a significant amount of data. This data belongs to various devices (i.e., sensors) and numerous users. Naturally, the security of this data is of utmost importance. Traditionally, centralized security mechanisms are utilized. The centralized mechanisms utilize third-party verification that exposes the system to the risk of a central point of failure. Secondly, as it has been reported in the literature, many of the centralized security systems are not even suited for IoT-enabled networks due to scalability issues and traffic handling capabilities [43]. Thirdly, data generated are normally shared among various nodes of the network, which exposes privacy concerns for the users. In such situations, it is imperative to develop decentralized privacy and security management techniques for IoT-enabled systems. This leads us to the merger of IoT and blockchain technology. A standardized IoT infrastructure, decentralized privacy, and security management can be realized with the help of blockchain technology. Such a system has great potential to be readily used for 6G systems offering novel security solutions.

### *4.7. Smart Grid*

The appearance of distributed renewable energy resources changes as energy consumers transition from pure consumers to prosumers (i.e., both consumers and producers). Energy prosumers with excess energy sell it to other consumers. The exchange of energy between a prosumer and a consumer constitutes P2P energy trading. It is challenging to ensure the security of energy transactions in such scenarios. Blockchain technology enables secure P2P energy trading. Costs could be reduced by implementing a system for energy trading that relies on consortium blockchains through blockchain consensus. A blockchain based decentralized energy trading system can be introduced to protect the confidentiality of smart grid transactions.

### *4.8. Internet of Vehicles*

The Internet of Vehicles (IoV) includes vehicle-to-vehicle networks, vehicle-to-roadside networks, vehicle-to-infrastructure networks, and vehicle-to-pedestrian networks. Integrating blockchain technology with IoV is beneficial to address security issues. IoV blockchains implement a trust-management policy. Through the PoW/PoS consensus implemented by Road Side Units (RSUs), their liability for messages is authorised.

### *4.9. Edge Computing (EC)*

Edge Computing (EC) will continue to play its role in enabling 6G networks by extending the computing and caching capabilities of cloud servers to the edge of mobile networks, i.e. very near to the end-users. EC's close proximity, extremely low latency, context awareness, real-time access, and high bandwidth capacity are well-known features. In addition, the possible application of AI and ML approaches within the context of edge computing is commonly referred to as "Edge AI". To train AI and ML models, systems must routinely transfer a large quantity of raw data to a centralised server. This sharing of raw data raises concerns in terms of data and user privacy, communication costs, and additional burden on mobile devices with limited resources [44]. Federated Learning (FL) [12] proves to be a potential distributed AI method for addressing these difficulties.

In lieu of exchanging raw data, FL permits devices to upload the locally trained model to the server. Blockchain is under consideration as a tool for edge AI [45] and edge-based FL systems to provide trust, security, and stringent access control. It is anticipated that AI-native 6G will provide intelligent predictive pre-caching at the network's edges to efficiently satisfy the needs of network tenants. For such insights and predictions, however, user activity logs are given to AI and ML systems, which raises privacy concerns. In this regard, Sun et al. [46] created a blockchain-driven edge caching architecture that optimises cache hit rate and redundancy rate while maintaining user privacy and security. A rising number of projects try to capitalise on the synergy between FL and EC by utilising blockchain. For instance, Lu et al. [47] use digital twins to increase the dependability of EC applications by establishing digital twins of IoT devices on the EC server and performing data analysis on the digital replicas existing on the edge servers. To safeguard and protect the data privacy of digital twins, the authors implemented a blockchain-based FL. In [48], the authors presented a blockchain-enabled FL scheme for a digital twin edge computing platform that would service a large number of IoT devices in the 6G era. The authors demonstrated through numerical findings that their idea can enhance communication security and maintain data privacy.

## 5. Discussion: 6G and Blockchain

This section elaborates on the fact that blockchain technology offers 6G networks much more than security solutions. Blockchain-based resource optimization has the ability to accomplish extraordinarily high data rates demanded by 6G. Blockchain's application is especially advantageous for network structures with decentralized control. Moreover, blockchain can facilitate the required cooperative nature of 6G RAN [49]. Despite recent advances security remains a primary concern for blockchain-integrated IoT systems [50]. Exploring heterogeneous and multi-tiered networks, such as combined aerial and terrestrial networks, is a potential strategy for allowing massive connectivity [51]. To do this, blockchain can facilitate multi-mode connectivity in heterogeneous networks. The permissionless systems enable more cooperation between various RAN-related entities of a 6G network, hence enhancing its capacity for ubiquitous coverage. For example, blockchain can offer extensive coverage by operating network clusters with intermittent connectivity, where it can be utilised to manage cluster operations [52]. However, such systems are more sophisticated and may necessitate a higher level of security. Consequently, there is a tradeoff between the openness of a blockchain system for extending coverage and its complexity and security concerns. The existing objective of supporting small-packet and sensing-based URLLC services in 5G networks will be challenged by the introduction of an entirely new level of connectivity. 6G requires blockchains to enable ultra-massive sensing applications to cater to such a huge level of connectivity.

It should be noted that though blockchain presents numerous applications and advantages to the next-generation cellular networks (e.g., 6G) and IoT systems, however blockchain implementation still remains an uphill task. The reason is the computational complexity of the algorithms that run the whole blockchain process. The devices running blockchain algorithms consume tremendous energy and increase the carbon footprint. It might not be ideal for sustainable and green solutions. Moreover, the complexity of the system increases when integrated with blockchain and implementation requires a significant increase in the signaling overhead. In a nutshell, to design blockchain-based systems, all these factors should be considered, and more efficient and optimized implementation solutions should be developed.

## 6. Conclusions

The integration of 6G-enabled IoT and blockchain is a significant technological revolution and game-changer for the future of IoT-enabled industrial sector. The benefits of blockchain-enabled IoT systems should be studied carefully to eliminate the risk of implementation failures in different scenarios. The benefits of 6G-enabled IoT and blockchain, potential use cases and the challenges associated with this merger are presented in detail in this manuscript. The key points where blockchain can improve IoT applications are identified in this paper. It is predicted that blockchain technology will further advance the 6G-enabled IoT. The regulation adaption is the key to the integration of these two technologies for most infrastructure providers. Though recent research focuses on the issues of consensus and mining processes for blockchain-enabled systems, we believe scalability, storage capacity, data security, and embedded devices inclusion need researchers' attention and combined efforts to ensure both technologies (6G-enabled IoT and blockchain) successfully work together.

**Author Contributions:** Conceptualization, H.H.P. and S.D.; methodology, H.H.P. and S.D.; validation, H.H.P., S.D. and S.A; formal analysis, H.H.P. and S.A; investigation, H.H.P., S.A. and M.H.; writing—original draft preparation, H.H.P., S.A. and S.D.; writing—review and editing, H.H.P., S.D., S.A. and M.H.; supervision, S.D.; project administration, S.D. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| ML | Machine Learning (ML) |
| FL | Federated Learning (FL) |
| FCC | Federal Communications Commission |
| THz | TeraHertz |
| EC | Evolutionary Computation |
| IoT | Internet of Things |
| RIS | Reconfigurable Intelligent Surfaces |
| AI | Artificial Intelligence |
| P2P | Peer-to-Peer |
| mMTC | Massive Machine-Type Communications |

| | |
|---|---|
| eMBB | Enhanced Mobile Broadband |
| URLCC | Ultra-Reliable and Low Latency Communications |
| eMBB-plus | Mobile Broadband Plus |
| BigCom | Big Communications |
| SURLLC | Secure Ultra-Reliable Low-Latency Communications |
| 3d-InteCom | Three-Dimensional Integrated Communications |
| UCDC | Unconventional Data Communications |
| NFC | Near-Field Communication |
| BLE | Low-Energy Bluetooth |
| RFID | Radio Frequency Identification |
| IRS | Inertial Measurement Systems |
| HBF | Holographic Beamforming |
| OAM | Orbital Angular Momentum |
| VLC | Visible Light Communications |
| PoW | Proof of Work |
| PoS | Proof of Stake |
| PoC | Proof of Concept |
| PoA | Proof of Authority |
| DPoS | Delegated Proof of Stake (DPoS) |

## References

1. Chavhan, S. Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts. *Sustain. Energy Technol. Assess.* **2022**, *54*, 102666.
2. Hewa, T.; Gür, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The role of blockchain in 6G: Challenges, opportunities and research directions. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
3. Khan, A.H.; Hassan, N.U.; Yuen, C.; Zhao, J.; Niyato, D.; Zhang, Y.; Poor, H.V. Blockchain and 6G: The Future of Secure and Ubiquitous Communication. *IEEE Wirel. Commun.* **2021**, *29*, 194–201. [CrossRef]
4. Hassan, N.U.; Yuen, C.; Niyato, D. Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions. *IEEE Ind. Electron. Mag.* **2019**, *13*, 106–118. [CrossRef]
5. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
6. Mahmood, M.R.; Matin, M.A.; Sarigiannidis, P.; Goudos, S.K. A Comprehensive Review on Artificial Intelligence/Machine Learning Algorithms for Empowering the Future IoT Toward 6G Era. *IEEE Access* **2022**, *10*, 87535–87562. [CrossRef]
7. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]
8. Praveen, G.; Chamola, V.; Hassija, V.; Kumar, N. Blockchain for 5G: A prelude to future telecommunication. *IEEE Netw.* **2020**, *34*, 106–113. [CrossRef]
9. Xu, H.; Klaine, P.V.; Onireti, O.; Cao, B.; Imran, M.; Zhang, L. Blockchain-enabled resource management and sharing for 6G communications. *Digit. Commun. Netw.* **2020**, *6*, 261–269. [CrossRef]
10. Pokhrel, S.R. Federated learning meets blockchain at 6G edge: A drone-assisted networking for disaster response. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 49–54.
11. Li, W.; Su, Z.; Li, R.; Zhang, K.; Wang, Y. Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Netw.* **2020**, *34*, 31–37. [CrossRef]
12. Ogundokun, R.O.; Misra, S.; Maskeliunas, R.; Damasevicius, R. A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology. *Information* **2022**, *13*, 263. [CrossRef]
13. Mazon-Olivo, B.; Pan, A. Internet of Things: State-of-the-art, Computing Paradigms and Reference Architectures. *IEEE Lat. Am. Trans.* **2021**, *20*, 49–63. [CrossRef]
14. You, X.; Wang, C.X.; Huang, J.; Gao, X.; Zhang, Z.; Wang, M.; Huang, Y.; Zhang, C.; Jiang, Y.; Wang, J.; et al. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. *Sci. China Inf. Sci.* **2021**, *64*, 1–74. [CrossRef]
15. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.; Zhang, J.C. What will 5G be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [CrossRef]
16. Liu, G.; Huang, Y.; Li, N.; Dong, J.; Jin, J.; Wang, Q.; Li, N. Vision, requirements and network architecture of 6G mobile network beyond 2030. *China Commun.* **2020**, *17*, 92–104. [CrossRef]
17. Mihret, E.; Haile, G. 4G, 5G, 6G, 7G and Future Mobile Technologies. *J. Comp. Sci. Info Technol.* **2021**, *9*, 75.
18. Han, C.; Wu, Y.; Chen, Z.; Wang, X. Terahertz communications (TeraCom): Challenges and impact on 6G wireless systems. *arXiv* **2019**, arXiv:1912.06040.

19. Sreekantha, D.; Koujalagi, A.; Girish, T.; Sairam, K. Internet of Things (IoT) enabling technologies and applications—A study. In *Advances in Artificial Intelligence and Data Engineering*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1425–1442.
20. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Res. Appl.* **2021**, *2*, 100006. [CrossRef]
21. Kim, J.H. 6G and Internet of Things: A survey. *J. Manag. Anal.* **2021**, *8*, 316–332. [CrossRef]
22. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.* **2021**, *9*, 359–383. [CrossRef]
23. Alsulami, M.M.; Akkari, N. The role of 5G wireless networks in the internet-of-things (IoT). In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; pp. 1–8.
24. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open J. Commun. Soc.* **2020**, *1*, 957–975. [CrossRef]
25. Nakamoto, S.; Bitcoin, A. A Peer-to-Peer Electronic Cash System. Bitcoin. 2008; Volume 4, p. 2. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 1 September 2022).
26. Tran, N.K.; Babar, M.A.; Boan, J. Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. *J. Netw. Comput. Appl.* **2021**, *173*, 102844. [CrossRef]
27. Lockl, J.; Schlatt, V.; Schweizer, A.; Urbach, N.; Harth, N. Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1256–1270. [CrossRef]
28. Singh, M.; Singh, A.; Kim, S. Blockchain: A game changer for securing IoT data. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 51–55.
29. Karajeh, H.; Maqableh, M.; Masa'deh, R. Privacy and security issues of cloud computing environment. In Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain 13–14 May 2020; Volume 2016.
30. Ziani, A.; Medouri, A. A survey of security and privacy for 5G networks. In *Emerging Trends in Ict for Sustainable Development*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 201–208.
31. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* **2021**, *21*, 772. [CrossRef]
32. Abiodun, O.I.; Abiodun, E.O.; Alawida, M.; Alkhawaldeh, R.S.; Arshad, H. A review on the security of the internet of things: challenges and solutions. *Wirel. Pers. Commun.* **2021**, *119*, 2603–2637. [CrossRef]
33. Sanka, A.I.; Irfan, M.; Huang, I.; Cheung, R.C. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Comput. Commun.* **2021**, *169*, 179–201. [CrossRef]
34. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
35. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
36. Bhushan, B.; Sahoo, C.; Sinha, P.; Khamparia, A. Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. *Wirel. Netw.* **2021**, *27*, 55–90. [CrossRef]
37. Lone, A.H.; Naaz, R. Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. *Comput. Sci. Rev.* **2021**, *39*, 100360. [CrossRef]
38. Khan, P.W.; Byun, Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy* **2020**, *22*, 175. [CrossRef] [PubMed]
39. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
40. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
41. Mehmood, Y.; Ahmad, F.; Yaqoob, I.; Adnane, A.; Imran, M.; Guizani, S. Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Commun. Mag.* **2017**, *55*, 16–24. [CrossRef]
42. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Netw.* **2020**, *34*, 8–14. [CrossRef]
43. Mehedi, S.; Shamim, A.A.M.; Miah, M.B.A. Blockchain-based security management of IoT infrastructure with Ethereum transactions. *Iran J. Comput. Sci.* **2019**, *2*, 189–195. [CrossRef]
44. Peltonen, E.; Bennis, M.; Capobianco, M.; Debbah, M.; Ding, A.; Gil-Casti neira, F.; Jurmu, M.; Karvonen, T.; Kelanti, M.; Kliks, A.; et al. 6G white paper on edge intelligence. *arXiv* **2020**, arXiv:2004.14850.
45. Qiu, C.; Yao, H.; Wang, X.; Zhang, N.; Yu, F.R.; Niyato, D. AI-chain: Blockchain energized edge intelligence for beyond 5G networks. *IEEE Netw.* **2020**, *34*, 62–69. [CrossRef]
46. Sun, W.; Li, S.; Zhang, Y. Edge caching in blockchain empowered 6G. *China Commun.* **2021**, *18*, 1–17. [CrossRef]
47. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5098–5107. [CrossRef]

48. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet Things J.* **2020**, *8*, 2276–2288. [CrossRef]
49. Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. In *Future Generation Computer Systems*; Elsevier: Amsterdam, The Netherlands, 2022.
50. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
51. Gür, G. Spectrum sharing and content-centric operation for 5G hybrid satellite networks: Prospects and challenges for space-terrestrial system integration. *IEEE Veh. Technol. Mag.* **2019**, *14*, 38–48. [CrossRef]
52. Hu, Y.; Manzoor, A.; Ekparinya, P.; Liyanage, M.; Thilakarathna, K.; Jourjon, G.; Seneviratne, A. A delay-tolerant payment scheme based on the ethereum blockchain. *IEEE Access* **2019**, *7*, 33159–33172. [CrossRef]