electronics

MDPI

Review

Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions

Abdelzahir Abdelmaboud [1,*], Abdelmuttlib Ibrahim Abdalla Ahmed [2], Mohammed Abaker [3], Taiseer Abdalla Elfadil Eisa [4], Hashim Albasheer [5,6], Sara Abdelwahab Ghorashi [7] and Faten Khalid Karim [7]

1 Department of Information Systems, King Khalid University, Muhayel Aseer 61913, Saudi Arabia
2 Center for Mobile Cloud Computing Research, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia; abdelmuttlib@siswa.um.edu.my
3 Department Computer Science of Community College, King Khalid University, Muhayel Aseer 61913, Saudi Arabia; moadam@kku.edu.sa
4 Department of Information Systems-Girls Section, King Khalid University, Muhayel Aseer 61913, Saudi Arabia; teisa@kku.edu.sa
5 Faculty of Computer Science, King Khalid University, Abha 61421, Saudi Arabia; hhtaha@kku.edu.sa
6 College of Engineering, School Computing, Universiti Teknologi Malaysia (UTM), Johor Bahru 81310, Malaysia
7 Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; saabdelghani@pnu.edu.sa (S.A.G.); fkdiaaldin@pnu.edu.sa (F.K.K.)
* Correspondence: aelnour@kku.edu.sa

Abstract: The Internet of Things (IoT) has become a popular computing technology paradigm. It is increasingly being utilized to facilitate human life processes through a variety of applications, including smart healthcare, smart grids, smart finance, and smart cities. Scalability, interoperability, security, and privacy, as well as trustworthiness, are all issues that IoT applications face. Blockchain solutions have recently been created to help overcome these difficulties. The purpose of this paper is to provide a survey and tutorial on the use of blockchain in IoT systems. The importance of blockchain technology in terms of features and benefits for constituents of IoT applications is discussed. We propose a blockchain taxonomy for IoT applications based on the most significant factors. In addition, we examine the most widely used blockchain platforms for IoT applications. Furthermore, we discuss how blockchain technology can be used to broaden the spectrum of IoT applications. Besides, we discuss the recent advances and solutions offered for IoT environments. Finally, we discuss the challenges and future research directions of the use of blockchain for the IoT.

Keywords: decentralization; blockchain; general ledger; internet of things; security; smart contract; trust

Citation: Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. https://doi.org/10.3390/electronics11040630

Academic Editor: KiSung Park

Received: 10 December 2021
Accepted: 27 January 2022
Published: 18 February 2022

1. Introduction

In recent years, the Internet of Things (IoT) has emerged as a new and significant technology of the computing paradigm. The market demand for smart devices is projected to be worth trillions of pounds annually in the near future, and almost all businesses will use some sort of technology to improve their financial operations [1]. However, as critical applications of the IoT rapidly increase (for instance, smart healthcare, smart grids, smart cities and smart finance), they face numerous security and privacy challenges. In fact, in October 2016, the US internet was brought down by cyberattacks. These attacks targeted the servers of Dyn, a corporation that controls and operates the largest infrastructure of the internet's domain-name system (DNS). The company estimated that attacks were launched from tens of millions of IP addresses and that attacks have become larger. These attacks were due to malicious software called Mirai that infected web traffic obtained from IoT devices, including home routers, baby monitors, webcams, and video recorders for

digital use. The Mirai attacks had a much wider scope than the most distributed denial of service (DDoS) attacks that have historically been able to reach more than 100,000 malicious endpoints, according to Dyn's estimate [2].

As IoT attacks become more sophisticated, the threat vector grows. Therefore, blockchain technology plays a critical role in addressing security challenges and the issues involved in using the IoT [3,4]. A blockchain system involves a type of large database leveraged with several new computational technologies and protocols. Blockchain stores data on servers that commonly consist of huge arrays of computers with the storage space and computing power required to support multiple users simultaneously accessing the database [5]. The first version of the blockchain, known as Bitcoin, was invented in 2009 by Satoshi Nakamoto [6]. Bitcoin was set up as a stable, decentralized global currency, which could be used as an exchange for financial transactions. The blockchain concept uses a decentralized public ledger designed to permanently record transactions without any need for authorization from a third party [6].

Vitalik Buterin created the first cryptocurrency 'smart contract' in 2013. This system enables citizens to directly share value without intermediaries. Further, a smart contract's ability to enforce or self-execute contractual provisions is one of its most important aspects. Furthermore, smart contracts have considerably assisted the growth of blockchain. The combination of automatically executed contracts in a trusted environment with no centralized control has the potential to revolutionize the way business is conducted today. In addition, smart contracts and improving trust the IoT's mechanisms while lowering expenses, whereas data security in the IoT is ensured by time series data and encryption. The blockchain network collects a lot of information and uses the right techniques to secure data at a higher level [3]. Smart contracts are increasingly being used by businesses to minimize costs and improve efficiency [7].

Blockchain technologies, such as distributed ledger technology, have provided benefits to organizations requiring high levels of trust in the execution of their core transactions. In fact, the blockchain is a distributed ledger technology that differs from standard distributed ledger technology in terms of storage mechanisms and data types. As a result, blockchain technology realizes privacy and security requirements, ensuring the validity and security of the data. Besides, record sets are a new thing in a ledger that preserves connected devices. In the blockchain, there is no such thing as a master or slave; each device has equal authority and a copy of the entire chain. A private or public blockchain can be used to implement a blockchain ledger. The use of a general ledger has enabled the benefits of blockchain to be extended beyond financial services to all aspects of daily life, and blockchain technologies have recently been explored in areas such as healthcare, transport, and energy. Companies' blockchain market value could hit $20.3 billion by 2025 from $4.6 billion in 2018, with finance and manufacturing dominating the blockchain market [8].

Consensus mechanisms are required for the integrity of the information stored in blockchains as well as defense against double attacks, and they are thus an essential component of blockchain technology. The ultimate goal is to create consensus in a dispersed network with no central authorities and participants who may or may not trust one another. Therefore, multiple consensus processes are possible with blockchain, and data privacy is achieved by cryptography and segmentation [3].

Asymmetric encryption algorithms are used to encrypt data on the blockchain. In blockchains, this asymmetric encryption is used for data encryption and digital signatures. Data encryption in the blockchain ensures transaction data security and decreases the risk of data loss or falsification. The transaction data is sent over the network and digitally signed to show the signatory's identity and whether the transaction has been identified. It is not essential to reveal the genuine identity of the node associated with the participant in the blockchain system. This feature is problematic because it indirectly aids criminal operations such as money laundering, but it does safeguard the participants' privacy and security. Blockchain technology's decentralization and data encryption make it ideal for developing distributed security systems. IoT security is enhanced by blockchain. The

blockchain's decentralization creates a safe environment for the IoT and creates a fully distributed system [9].

Blockchain technologies are used in multiple situations in many fields involving IoT applications such as data storage, management of identities, timestamps, sensors, supply chain management and applications to daily life, including smart healthcare and smart homes. The use of blockchain technologies is a promising solution for several problems in IoT applications, thus attracting the attention of both academia and industry aimed at developing and integrating blockchain technologies into IoT applications [10]. This paper focuses on the latest advancements in blockchain technologies and properties, with consideration of their applicability to IoT applications. The main contributions of this article appear in Sections 3–7. These are to:

- Provide a thematic taxonomy based on crucial parameters (Section 3);
- Discuss the most important and common blockchain platforms that support the IoT (Section 4);
- Discuss the key roles of blockchain in IoT systems (Section 5);
- Investigate the recent advances reported in the literature (Section 6);
- Discuss open challenges and future research directions in the IoT (Section 7).

2. Related Works

Many survey reviews have been published in the literature to investigate the proposed solutions regarding the use of blockchain for IoT systems. This section briefly summarizes the related surveys and presents a comparison in Table 1, which also includes the content of the present paper. Kshetri [2] examines the roles of blockchain in protecting privacy and strengthening cybersecurity. He provides a detailed analysis of the blockchain approach related to the supply chains of IoT devices. He also offers some policy implications of how blockchain technology is used to preserve the security of the IoT. These policy implications include providing training for stakeholders on how to protect privacy using a blockchain approach and increased investment in blockchain technology to adapt it to IoT applications. Khan et al. [11] investigate the security challenges for the IoT. They discuss the major security challenges of protocols, management, architecture, and network communication related to the IoT. In addition, they discuss security requirements and problems of the IoT identified in the literature, such as attacks and threats, and how the blockchain approach can be used to solve these problems. Reyna et al. [3] conducted a survey to investigate the issues and challenges of the blockchain approach related to IoT applications so that the two technologies can be integrated to successfully work together. They also highlight the main ways in which the blockchain approach can support the improvement of IoT systems. In addition, they examine the existing blockchain applications and platforms to provide a comprehensive summary of the collaboration of the blockchain approach with the IoT paradigm. Makhdoon et al. [12] undertake a systematic study of the performance and security requirements of IoT systems and developments in blockchain approaches. They highlight the gap between blockchain approaches and blockchain-based IoT systems by mapping the blockchain benefits of performance and security of IoT requirements. They also analyze and review the impact of the blockchain approach and IoT applications to highlight the future trends of blockchain and IoT applications. Hassan et al. [13] address the issues of privacy triggered by the adoption of blockchain into IoT apps by concentrating on everyday applications. The authors focus on the introduction of five privacy protection techniques used in blockchain-based IoT networks. These techniques are anonymization, encryption, a private contract, combining, and privacy differential. In fact, anonymization is a well-known strategy for maintaining privacy in IoT-based systems. A number of researchers have used anonymization approaches to secure the privacy of blockchain-based IoT applications.

Table 1. Related works.

Survey Paper	Year of Publication	Major Contribution	Blockchain Technology Covered	Comparison of Current Research Works in Terms of	Domain
Kshetri [2]	2017	Overview of protection privacy of cybersecurity based blockchain	N/A	Cloud and blockchain	IoT devices
Khan et al. [11]	2018	Investigation of security challenges based IoT	N/A	Threats of security, implications, and solutions	IoT
Reyna et al. [3]	2018	Overview challenges of the blockchain approach related to IoT applications	Smart contract Consensus protocol	Blockchain platforms Blockchain nodes	IoT
Makhdoon et al. [12]	2018	A systematic overview of the performance and security requirements of IoT systems	Smart contract Consensus protocol	Private and Public blockchain Cloud and blockchain Blockchain platforms IoT requirement and Blockchain approaches	IoT
Hassan et al. [13]	2019	An investigation the issues of privacy of adoption blockchain into IoT applications	Smart contract	Techniques of privacy-preservation	IoT
Yang [9]	2019	A discussion of using blockchain technology related to IoT security, data management and applications	Smart contract Consensus protocol	N/A	Healthcare service 5G network
Wang et al. [5]	2019	Overview of blockchain approaches related to IoT applications.	Consensus protocol	Blockchain platforms performance	IoT
Cui et al. [14]	2019	An investigation of blockchain relevant to IoT applications	Smart contract Consensus protocol	N/A	IoT
Viriyasitavat et al. [15]	2019	Overview of how blockchain can satisfy the requirements of the IoT	Smart contract	Modes of blockchainIoT characteristics	IoT
Mohanta et al. [16]	2020	Overview of protection and privacy problems based IoT systems	Smart contract	N/A	IoT
Lo et al. [17]	2019	A systematic review of IoT problems and comprehensive architecture of blockchain-based data storage and management	Consensus protocol	N/A	IoT

Table 1. *Cont.*

Survey Paper	Year of Publication	Major Contribution	Blockchain Technology Covered	Comparison of Current Research Works in Terms of	Domain
Mohsin et al. [18]	2019	Overview of blockchain application taxonomy of network authentication	Distributed ledger	N/A	Network
Mistry et al. [19]	2020	An investigation way of use of blockchain related to industrial applications	Smart contract	Approaches	5G network Healthcare
Wang et al. [20]	2020	Overview of blockchain characteristics and outlined Industry 4.0 based IoT protection criteria.	N/A	N/A	Industrial IoT
Rao and Clark [21]	2020	An investigation applications of supply chains, smarter electricity and healthcare.	Smart contract	N/A	IoT devices
Uddin et al. [22]	2021	An investigation of eHealth, smart cities and intelligent transport.	Consensus mechanism	IoT applications	IoT
Azbeg et al. [23]	2021	An investigation of how IoT and blockchain used in the healthcare domain.	N/A	Permissionless vs. Permissioned Blockchain IoT applications in healthcare.	IoT Healthcare
Saxena et al. [24]	2021	An in-depth detail assessment of the security in IoT systems based blockchain.	Smart contract	Types of blockchain. Consensus protocols.	IoT
Singh et al. [25]	2021	Discussion of ideas related to blockchain with assessment of various security threats.	Smart contract	Smart contract vulnerabilities.	IoT Network
This study	2022	Deep analysis of all the blockchain technologies, protocols and properties to support security and trust for IoT applications	Entire blockchain modes Technologies (smart contract, general ledger . . .)	Platforms Modes of blockchain Provided service Supported IoT applications	IoT

In addition, to ensure data security in blockchain-based IoT systems, certain encryption and authentication mechanisms are used. Due to its decentralized nature, blockchain technology enables the concept of private contracts. Furthermore, private contracts are a type of blockchain-based programmable code that IoT nodes can create based on transaction requirements and then execute on the network. Besides, to facilitate anonymity in financial transactions of blockchain-based IoT systems, coin mixing methods were created. On the other hand, differential privacy is an effective privacy preservation approach that ensures data confidentiality while minimizing the danger of data leakage. In addition, the authors, address problems and future research avenues related to the defense of privacy in blockchain-based IoT networks. The study is intended to serve as a basis for designing potential plans for privacy protection to resolve a range of privacy concerns over the use of blockchain systems in IoT devices.

Yang [9] discusses the significance of using blockchain technology related to IoT security, data management and applications. He also discusses the potential benefits of a blockchain approach to secure IoT applications and suggests future research directions. Wang et al. [5] review the existing blockchain approaches related to IoT applications. They provide an analysis of the consensus protocols of blockchain approaches that are suitable to be adapted and developed for IoT applications. They also highlight future research directions for integrating blockchain approaches into IoT systems.

The paper by Cui et al. [14] focused on blockchain technology in IoT applications and considered blockchain technology features such as transparency, decentralization, and tamper resistance to enhance device, data, and service management as well as the security of IoT systems. They also highlight the applications of blockchain to refine and support IoT domains such as energy, agriculture, healthcare, and smart cities. In addition, they provide a roadmap of the future and identify research trends for blockchain technology as a baseline for its adoption and integration into IoT systems. Viriyasitavat et al. [15] also reviewed how blockchain technology can meet the needs of the IoT and how the characteristics and capabilities of blockchain applications can be combined with the IoT. They explored how research into both the block approach and IoT can produce benefits for adoption in the business model. In addition, they analyzed the strengths and weaknesses of business opportunities to integrate and adapt blockchain technology to the IoT.

Mohanta et al. [16] reviewed the extent to which protection and privacy problems originally identified and established have persisted in the IoT system. In addition, they discuss how some encryption options are supported by blockchain technologies. Previous research, including technologies supporting IoT integration, is explained in depth. Finally, a case study is carried out using the blockchain method built on Ethereum in a clever IoT system, where the findings are addressed. Lo et al. [17] collected knowledge on current technical methodologies adopted to incorporate blockchain into the IoT by doing a systematic literature review (SLR) on peer-reviewed, published articles on blockchain-based solutions for the IoT. From the perspectives of data and thing management, they elicited the IoT difficulties being addressed, as well as the particular design of blockchain-based solutions.

Mohsin et al. [18] reviewed the blockchain application taxonomy of network authentication. They highlight the detection of different kinds of authentication schemes using blockchain technologies across various platforms. In addition, they explore challenges related to blockchain platforms and potential solutions that satisfy networks' implementation requirements. The study identifies the importance, strengths, motives, and threats of the blockchain approach in diverse domains. Mistry et al. [19] highlighted the ways in which the use of blockchain may revolutionize most existing and potential industrial applications in numerous industries by offering a global fine-grained method of regulating entry. Based on this feature, various types of transfers and network logs can be successfully tracked by blockchain in the industries in which it is applied to maintain consistency and privacy. The problems and issues of 5G-enabled IoT for blockchain-based industrial automation are also

discussed. Finally, a comparison is provided of the criteria of different existing proposals, which enables end-users to decide which is their preferred proposal.

Wang et al. [20] introduced blockchain's basic and core features and outlined Industry 4.0 and IoT protection criteria. They then discuss how blockchain could be used with its encryption tools and technologies in the IoT for business under Industry 4.0. They also identify the most appropriate blockchain-based IoT implementations to support the functions and drawbacks of the IoT and blockchain technologies. Finally, several guidelines are suggested to direct potential researchers and entrepreneurs in the blockchain field. Rao and Clark [21] investigated several promising applications, such as supply chains, smarter electricity, and healthcare. The authors outline techniques that could address many of the obstacles and thus contribute to successful adoption of blockchains for IoT. Finally, they note the possible cybersecurity consequences of IoT systems, including expanded attack surfaces and system weaknesses.

Uddin et al. [22] investigated eHealth, smart cities, intelligent transport, and other industries. In addition, the authors present blockchain breakthroughs for both the IoT and cloud IoT, as well as an assessment of blockchain for Fog IoT. Furthermore, the study delves into a variety of issues, such as research gaps with potential solutions. Azbeg et al. [23] explored how the IoT and blockchain may be used in the healthcare domain. The study looks at difficulties and possible solutions related to healthcare IoT-based systems that have adopted blockchain technology. For instance, IoT devices have limited computing and storage resources. However, blockchain requires high energy usage and computational resources. Several solutions have been proposed to resolve these problems. Using permissioned blockchains for IoT systems is one of these solutions. Another option is to employ blockchain networks that are powered by an energy-efficient consensus mechanism. Saxena et al. [24] presented a detailed assessment of the security advances made in IoT systems employing blockchain, as well as the issues that arise as a result of this integration. The study also highlights the most significant blockchain-based IoT applications and provides future research possibilities. Singh et al. [25] discussed important considerations and ideas related to blockchain and provided a full assessment of various security threats and current solutions that may counter such assaults. The study also covers blockchain security enhancement solutions by summarizing key aspects that may be used to prepare different blockchain solutions as well as tools that address security flaws.

This review provides an exhaustive analysis of all of the blockchain technologies, protocols, and properties that offer a critical role in supporting security and trust for IoT applications. In addition, deep analysis of recent advances has been discussed to illustrate strengths, weaknesses, and threats to support the integration of the blockchain approach relevant to IoT applications. In the end, the study explored significant outcomes of the key challenges and issues in developing and incorporating IoT systems with a blockchain approach.

3. Taxonomy

Most of the current survey studies classify blockchain approaches based on architectural components and the mode of blockchains [9,16,26]. We adopted and derived our classification from blockchain technologies [27], as well as blockchain applications [28], supported by the literature with more relevant blockchain approaches. In fact, we present a broader categorization of blockchain-based IoT applications. We classify additional blockchain modes, protocols, technologies, and properties that are critical in providing security and privacy solutions for IoT applications, as shown in Figure 1.

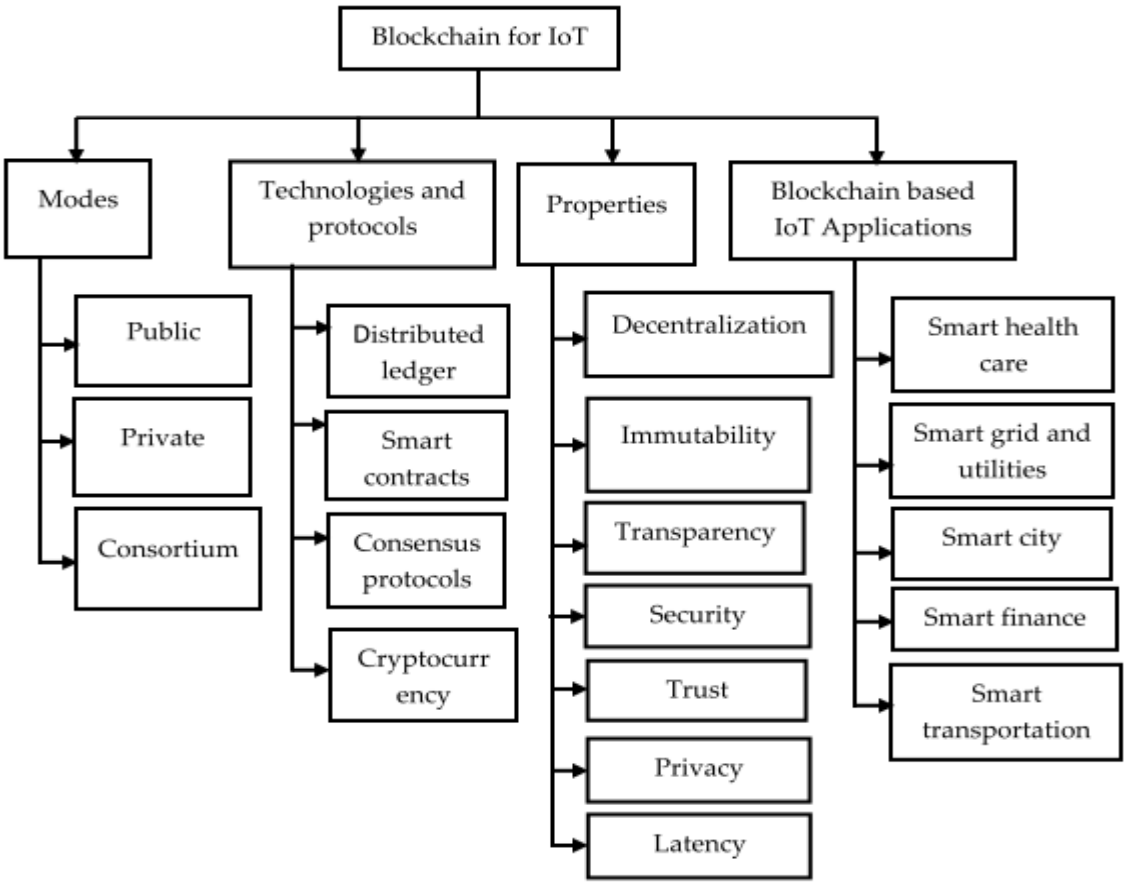

Figure 1. Thematic taxonomy of blockchain.

3.1. Blockchain Modes

The blockchain approach is a decentralized platform that allows participants on a peer-to-peer network to share data. Partially decentralized (permissioned blockchain) and fully decentralized (as non-permissioned blockchains) blockchains can be classified (permissionless blockchain) [29]. Furthermore, based on various principles, such as authentication and access control mechanisms, the blockchain can be a public blockchain, a private blockchain, or a consortium blockchain [13] (see Table 2).

Table 2. Comparison of blockchain modes.

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Management	Non centralized	Centralized	Partially centralized
Access permission	Reading is public	Public/restricted	Public/restricted
Consensus determination	All miners	One organization	Selected set of nodes
Consensus process	Permission-based	Permission-based	Permission-free

3.1.1. Public Blockchain

Public blockchain is a non-permissioned and essentially decentralized open-source network, where any person, regardless of entity or context, can participate and conduct mining or transaction operations [13,30]. Any blockchain node has the maximum powers to undertake writing, reading, checking or analysis of blockchain records such as cryptocurrency. A public blockchain-based peer-to-peer (P2P) network enables users to gather transaction records and launch mining processes to obtain the desired output. Miner nodes gather information about transactions in blocks and validate their legitimacy, and then start to reach a consensus and add the outcome and block to the current blockchain [31]. A con-

sensus process is used to guarantee that blocks are identical throughout the blockchain and to ensure that no node has so many blocks that they clash. The members are unidentified in the public blockchain; they have been permitted to build a block before mining, and each node in turn renders the public blockchain vulnerable to Sybil attacks.

Proof-of-Work (PoW) consensus is a powerful method for dealing with such problems in public blockchains. In this process, if a competitor wishes to dominate the blockchain, 51% of the blockchain network's mining power is needed. To protect transactions in blockchain, cryptographic keys are used, where any user's address is the hash of the user's public key. A node can participate in the transaction and transmit the additional node asset just by signing a hash of its ability to retrieve information and including the new owners' public keys throughout transactions. Likewise, the current owner must verify the signature to validate the chain of ownership [32]. However, neither the PoW protocol nor the public blockchain approach is suitable for finance and banking applications due to the huge amount of data required and the complexity of the computing systems involved. However, effective and less complicated methods for these applications are currently being designed [32]. The ePoW consensus algorithm reduces the number of nodes participating in PoW and encourages multiple mining nodes to participate. As a result, we plan to reduce energy waste caused by excessive hashing power in mining competitions and to fairly distribute mining opportunities [3].

3.1.2. Private Blockchain

Private blockchain technology is a permissioned, centralized-based network that allows private exchange and distribution of a volume of data within an entity or community of people. In addition, a private blockchain mining operation is run by a person or a particular company, therefore the blockchain cannot be used by a new or unfamiliar user unless a special order has been issued by the governing body to add another new user [13,33].

One of private blockchain's most popular features is the Hyperledger [34]. To ensure confidentiality and stability, a deterministic shared consensus protocol that works in planning, preparation and interaction phases has been proposed to be used in private blockchains. Writing inside a private blockchain is limited, and the network may only write or transact in the governing nodes. That is why private blockchains appear to be centralized. However, other properties of private blockchains, such as consensus and distributed ledgers, render this type of blockchain suitable for banks and financial institutions.

3.1.3. Consortium Blockchain

The consortium blockchain approach is a hybrid of private and public blockchains. Decisions on block verification and consensus are made by a group of companies or individuals [13,35]. This coalition of organizations agrees on the network's presence and mining nodes. The network block, where the extracted block is assumed to be a legitimate block, is minted by a multi-signature method if it is accepted and signed by the governing nodes [33]. Instead of requiring everyone to participate in the process or having a single entity decide the validation process, the consortium blockchain allows the participants of individuals or organizations to validate blocks. Examples of consortium blockchain frameworks include Hyperledger Fabric [36]. The consortium blockchain validates transactions using consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) and Byzantine Fault Tolerance (BFT) through the Tendermint algorithms that replicate applications on multiple machines in a secure and consistent manner.

3.2. Blockchain Technologies and Protocols

Blockchain involves several technologies, which run based on different protocols. This section discusses the major technologies and protocols, which are summarized in Table 3.

Table 3. Blockchain services and benefits for IoT applications.

Blockchain Technologies and Protocols	Benefits for IoT Applications
Distributed ledger	Perform large of transactions Support IoT devices Offer data collection
Smart contracts	Enhance the autonomy of IoT devices Eliminate regulatory overheads Provide high level of collaboration and authority
Cryptocurrency	Control central authority Ensure integrity of transactional data Change business and finance directions
Consensus protocol	Manage and integrate information Support IoT applications Support agreement between vendors without need to central authority

3.2.1. Distributed Ledger

The distributed ledger is designed to work without a central administrator and instead involves the consensus of multiple locations, organizations, or countries that provide replicated, shared, and coordinated digital data [37,38].

Recently, the distributed ledger system has been extended to IoT applications, allowing millions of IoT devices to efficiently perform billions of transactions [39]. Supporters point to the potential of this technology in an IoT context through encouraging supply chain initiatives, self-executing payments and strengthening the cybersecurity of connected devices. The distributed ledgers help create trust in the minds of users. Moreover, as peers are linked in a P2P network, each pair has ample device and storage space to support a distributed ledger. The connectivity layer enables connectivity between sensors and peers. In addition, the distributed ledger layer offers facilities for data collection [40].

3.2.2. Smart Contracts

A smart contract is an executable code located on a blockchain performed on the basis of a particular circumstance. Smart contracts cannot be processed until a new block includes their calling transactions. Transactions are organized by blocks to remove non-determinism, which could otherwise impact their output outcomes. Blockchain contracts enhance the autonomy of IoT devices by enabling them to directly determine whether agreements comply with contractual requirements. A smart contract is able to eliminate regulatory overheads, while blockchain functions act as a kind of ledger, confirming that the transactions have taken place. Thus, a blockchain-enabled IoT implementation could boost the overall performance of the application by enabling devices to record and validate the transactions and then activate them. In a blockchain-based IoT system, business logic is implemented automatically through smart contracts without subjecting the core mechanism to threats such as denial of service attacks [41]. A smart contract ensures a high level of collaboration and maintains cohesion with regards to handling transactions and connections. Therefore, a smart contract enables the service of the ledger to include the vocabulary of the terms of the transaction and the calculations to decide when those requirements have been fulfilled [42].

3.2.3. Cryptocurrency

A cryptocurrency is a new digital asset founded on a network spread over a multitude of platforms. Furthermore, cryptocurrency retains its value in the absence of centralized authority or financial object support [3]. The decentralized structure supporting a cryptocurrency enables it to operate beyond the influence of governments. The term "cryptocurrency" derives from the encryption methods used to protect the network. The use of blockchains is

an integral aspect of many cryptocurrencies, such as the organization's methods to maintain transactional data transparency. Cryptocurrencies have been criticized for illegal activities, exchange rate fluctuations, and the technology vulnerabilities that underlie them. However, blockchain promotes divisibility, portability, tolerance of inflation, and openness. It is clear that blockchain and its related technology will change the direction of business and finance; therefore, its legal and regulatory dimensions must be considered.

3.2.4. Consensus Protocol

The consensus protocols used represent the crucial part of the blockchain approach because they are responsible for managing and integrating the information within the blockchain, as well as supporting IoT applications. Consensus protocols need to be supported and agreed upon by most vendors and participants through a distributed network without the necessity of a central authority [3]. Proof-of-stake (PoS), Proof-of-Authority (PoA) and Delegated Proof-Of-Stake (DPoS), together with PoW, are the most general forms of consensus protocols. The Bitcoin Network uses proof of operation. Bitcoin validates Bitcoin blockchain mining transactions that verify and allow a block record of Bitcoin. PoS targets forgers rather than miners. These forgers have an amount of cryptocurrency that enables them to be a block validator, depending on probability. The good blacksmith is awarded with the appropriate block transaction fees. Stacking its own cryptocurrency in a block provides a forger with an opportunity to try to cheat the network because it loses stakes if the network's transactions are wrongly applied. The DPoS approach operates similarly to PoS. However, instead of using chance, cryptocurrency investors are allowed to cast ballots redistributed to their stake to nominate witnesses. These witnesses protect and verify the blockchain; they require no cryptocurrency, only votes. This consensus mechanism is more centralized than in most PoA protocols that set block validators. New blocks can only be generated on a blockchain if the validators have the majority, which is identical to the PoS protocol. The validators are recognized and responsible for the status and eligibility of PoS validation. A recent blockchain, Elysian, uses PoA and Ethereum testnet blockchains [43,44].

Practical Byzantine Fault Tolerance (PBFT). It is intended to be more efficient than a PoW in terms of energy and latency costs, but it can only withstand up to 33% of malicious nodes. Due to the large number of messages needed for consensus, PBFT is thought to be a costly protocol. Based on shaky timing assumptions, the PBFT protocol ensures liveness. It works as a primary backup system, with replicas moving through a series of configurations known as views. Istanbul Byzantine Fault Tolerance (IBFT) was the first consensus algorithm to be implemented in Quorum, and it has since proven to be a very common consensus protocol for the development of enterprise permissioned networks needing byzantine fault tolerance and finality. The gathering of signatures from the candidate and voting validators ensures that IBFT blocks are highly resistant to tampering [12]. In addition, the Raft consensus protocol is an excellent choice for a private blockchain-based IoT. If there are pending transactions, the Raft consensus does not always mint blocks. This can save a lot of space, particularly when the transaction power is low, since no empty blocks with zero transactions are created. Furthermore, Greedy Heaviest-Observed Sub-Tree (GHOST) is a protocol for arranging blocks in tree structures. It follows the path from the blockchain network, the first block in the blockchain, to the fattest sub-tree with the most blocks, or, in other words, the publicly accepted main chain, which contains the heaviest computation quantity. GHOST can reduce block generation time from around 10 min in Bitcoin to 12 s in Ethereum. As a result, blockchain's capacity can be enhanced [5].

Although blockchain technologies and protocols provide security and privacy for applications, there are still many issues and challenges that need to be addressed. In fact, the consensus protocol uses a lot of computing resources and power in real-world transactions, resulting in low system throughput and long system latency. The blockchain, on the other hand, necessitates greater operational and platform compatibility. The blockchain must

address the issue of designing an interaction approach to aggregate and use the collective intelligence of distributed consensus nodes [9]. In addition, working with smart contracts necessitates the use of oracles, which are trusted sources of real-world data. Since the Internet of Things is inherently unstable, testing these smart contracts might be put at risk. Furthermore, accessing various data sources could cause these contracts to become overloaded. Smart contracts are currently decentralized and distributed, but they really do not share resources in order to distribute tasks and address large amounts of computation. Smart contracts should also account for the IoT's heterogeneity and constraints. Smart contracts should be used in conjunction with filtering and grouping mechanisms to enable applications to resolve the IoT based on context and requirements. A discovery mechanism might allow for device incorporation on the fly, enhancing the utility of these applications. Finally, smart contract-based actuation mechanisms would allow for faster IoT reactions [3]. Moreover, because of the massive IoT systems' computational loads, applying blockchain protocols to IoT applications can lead to a new set of issues. The size of a blockchain grows in the IoT as the number of connected devices grows, generating a massive amount of data in real time. Therefore, the validation of an IoT blockchain is extremely difficult. Many blockchain implementations in the current cryptocurrency market are not scalable enough to meet requirements.

3.3. Propeties

Blockchain is characterized by several properties, such as decentralization, immutability, transparency, security, and trust.

3.3.1. Decentralization

The existing IoT systems focus on unified, brokered communication models that are often referred to as the paradigm of the server-client. Owing to the high service and storage costs for networking facilities, large server farms and centralized clouds, existing IoT technologies are costly. As more vital activities such as human wellbeing and survival start to rely on the IoT, this is particularly important [45]. In fact, IoT services are decentralized, with no single authority. The system may allow for transactions or set unique rules for the approval of transactions. Since all of the network nodes want to approve transactions by consensus, there is a huge amount of confidence involved. The blockchain's decentralized, independent, and trustless characteristics make it an integral component for IoT application solutions. Without the need for a centralized broker, the service provided by the blockchain would allow truly independent smart devices to share data or even perform financial transactions. This form of sovereignty is possible because, without depending on a single authority, the peers in the blockchain-based network can validate the legitimacy of transactions. One of the most important services offered by blockchain is the ability to keep a properly unauthorized, trustworthy database of all of the transactions in a network. These facilities are relevant without having to rely on a centralized approach that oversees many IoT application compliance and regulatory requirements [46].

3.3.2. Immutability

Immutability can be described as the capacity of a blockchain ledger to stay unchanged. Maintaining an unchanged blockchain guarantees the immutability of transactions, which stems from the manner in which the distributed ledger approach encrypts the previous entry for each new block. Participants must also consider the potential for immutability in terms of individual blockchain features, including security thresholds and other potential threats. For instance, when bad players undermine a majority of the members, overpower the consensus system and change blockchain contents to their advantage, a 51% attack takes place [47]. Any knowledge block, such as a set of facts or descriptions of transactions, uses a cryptographic concept or hash value. This hash value is an independently generated alphanumeric string for each block. Each block contains not only its own hash and/or digital signature but also that for the first. This means that the blocks are retroactively

connected and impartial. This blockchain functionality means that no one can access the system or change the block records. Furthermore, blockchain is distributed and decentralized in nature, as consensus is reached between the different nodes that hold data replicas. This consensus ensures that the originality of the data is retained. It is clear that immutability, where each code block is independently guarded by the hash value, is a key distinguishing characteristic of this technology, which will redefine the entire data auditing process, making it more efficient, cost-effective and trustworthy [48].

3.3.3. Transparency

Blockchain is intended to be a mechanism for openness where everyone can access the network and see all its details [49]. The majority of blockchains are open-source applications, which anyone can access and use their code. Any IoT member has access to the on-chain consensus-building mechanism and to the full record of the blockchain process. Transparency increases corporate convenience (for certain cases) and ensures an audit record and a confidential workflow. This also helps auditors verify security in a cryptocurrency such as Bitcoin. This also implies that there is no actual authority to regulate or modify the Bitcoin code. As a result, anyone can recommend code improvements or enhancements. When a number of users on the network think the new updated version of code is sound and useful, Bitcoin is modified. Blockchain protections work by the requisite encryption and enforcement mechanisms. Details are saved, meaning all changes are recorded. Thanks to the technology's capacity to show confidentiality by cryptographically sending unchanging data to other parties, it has the power to render transfers more open and facilitate system accountability. The terms of any contract are irrevocable and available to everyone or to qualified auditors to carry out inspection in ways that have never been available before. In the case of cryptocurrency, blockchain openness allows consumers to explore the past history of all transactions. The openness and accountability offered by blockchain technology will play a future role in restricting improper internet monitoring and surveillance and violations of human rights [50].

In the case of a completely public blockchain, for example, all of the information becomes public: everyone will consider all of the data stored as both available to everyone and open to stop data abuse. Blockchain will empower shoppers to trace something in the supply chain and to know specifically what their food comprises, whether it is healthy and fair trade and whether the items they purchase are legitimate or made with respect for the rights of workers. By increasing openness through blockchain, proper transparency can help to create an equitable, open, and accountable digital economy.

3.3.4. Security

Since on-chain "addresses" are encryption-protected, the integrity and safe characteristics of the consensus process to ensures that the identity of participants and the integrity, changes or exchanges of information can be guaranteed. Knowledge and contracts can be secured if they are stored as blockchain transactions. Blockchain will thus guarantee connectivity between devices in the form of transfers, validated by smart contracts. The implementation of blockchain will simplify existing standard protocols used in the IoT. In addition, blockchain security is stronger than that obtained through centralized data processing, which is likely to be damaged by interference by hackers. More than 50% of networks in the network are vulnerable to hacking crashes. However, falsifying data is almost impossible in blockchain due to the simultaneous monitoring of the computers where data are stored, including handheld devices. Moreover, the hacker would have to falsify all of the data saved on the computers [3]. Thus, by distributing data among many interlocked computers, blockchain is protected. A block data chain is generated that includes the complete history of the purchase to render the ledger secure by using a hashing feature [18].

3.3.5. Trust

The blockchain service obtains a copy of the ledger record and runs a copy of the intelligent contracts on acceptance of transactions. This is achieved without a centralized jurisdiction. Since each participant in the blockchain corporate network can access the details and business rules, the participants can trust the record of transactions in the blockchain. Currently, the blockchain ledger can be used to register and exchange almost anything without having a single point of control. Thus, a trusted and effective business network can be created between the individuals and parties who transact together. In the IoT context, devices may engage in transactions as a group that carries out transactions within blockchain. The indelible database of transactions and data from devices deposited in the blockchain provides the requisite confidence for companies and people to cooperate by ensuring that a computer is in charge of its own identity. In addition, a computer with an identity may establish credibility or a background that is monitored by a blockchain.

Blockchain offers a service to develop and express mutual confidence in knowledge provided by and shared by things. An observable log of blockchain events maintains definitive information about provenance, tracking and executing information access policies and autonomously acts on information through smart contracts. As a decentralized framework, blockchain reduces the need for a reliable third party by empowering users to ensure data integrity and immutability. IoT systems may use blockchain to register themselves and to efficiently and securely organize, store, and exchange data streams. With the development of the IoT, businesses can now collect information, obtain knowledge from data, and determine the basis of data to have end-to-end trust for trading. The IoT will also trust the data collected with blockchain. The underlying concept is to provide devices with an identity that can be validated and tested over their life cycle with blockchain. There is great potential for IoT networks that focus on protocols for user identification and reputation systems with blockchain technology services. Each device can use its own public blockchain key to transfer encrypted challenges and answer messages to other devices to ensure that the device has control over its identity. A system with an identity also creates a legacy or history monitored by a blockchain [51].

3.3.6. Privacy

Numerous IoT applications work with sensitive data such as when a device is connected to a person, as in the e-health scenario. Addressing the issue of data privacy and anonymity is critical. Although blockchain is promoted as the ideal solution for IoT identity management, there might be some applications where anonymity is required, similarly to Bitcoin. This is the case with wearables that can hide a person's identity when sending private information, or with smart vehicles that protect the privacy of users' itineraries. The issue of data privacy in transparent and public blockchains, as well as some of the existing solutions, has already been discussed. Data privacy in IoT devices, on the other hand, is a more difficult problem to solve because it begins with data collection and extends to communications and application levels. Securing the device so that data is stored safely and not made accessible by people without permission is difficult because it necessitates the integration of security cryptographic software. These enhancements should consider the device's limited resources and economic viability constraints. Internet Protocol Security (IPsec), Secure Socket Layer/Transport Layer Security (SSL/TLS), and Datagram Transport Layer Security (DTLS) are some of the technologies that have been used to encrypt communications. Due to the limitations of IoT devices, it's frequently necessary to use less-restricted devices such as gateways to implement security protocols. Use of cryptographic hardware might speed up cryptographic operations while also reducing the burden of complicated secure software protocols [3].

3.3.7. Latency

In decentralized blockchain networks, the high latency of blockchain is often used to ensure consistency. For many IoT applications, the latency that blockchain is known for

is unacceptable. For example, Bitcoin's 10 min block confirmation time is considered for delay-sensitive IoT systems such as vehicle networks. In fact, because of the high latency of blockchain, its capacity is limited. Blockchain capacity, for example, 1 MB per 10 min of Bitcoin, is far less than what IoT applications require. IoT capacity requirements vary depending on the application. For example, in an IoT-based smart city application. The vehicular trace amounts of 700 cars in 24 h total 4.03 GB, or about 0.24 MB per car per hour. In the meantime, the parking lot data from 55 points has been estimated to be 294 KB in 5 months, or 36 B per day per point. With the growing number of IoT devices, the capacity requirements of IoT applications will continue to grow [5].

3.4. Blockchain-Based IoT Applications

Blockchain has been integrated with different IoT applications to boost various performance aspects, such as smart healthcare, smart grids and utilities, smart cities, smart finance, and smart transportation.

3.4.1. Smart Healthcare

Intelligent healthcare plays an important role in medical treatments involving the use of embedded devices such as sensors in patient bodies for testing and recording purposes. Through the IoT, the integrated sensors are capable of gathering data from the patient's body and transmitting it to the doctor to monitor and check patients' status. This approach will liberate the patient from the hospital's centralized structure and keep him or her in constant contact with the doctor. Thus, there is a strong interest in introducing such modern IoT-based technology to ensure patients' real-time surveillance in the context of aging populations and rising medical costs [52].

The potential health benefits have been demonstrated in a collaboration between the FDA and IBM Watson Health focused on the use of blockchain responsibility to ensure oncology-related data. They concluded that blockchain can accept data exchange from diverse sensors with consensus among patients and mutually agreed terms [53]. Healthcare providers are likely to use blockchain to safely store their patients' medical records. When a health history is developed and signed, blockchain can provide confirmation and confidence for patients whose records cannot be modified. Sensitive medical data can be encoded and preserved in a blockchain with a secret password, such that only medical users can access them, thus ensuring security.

3.4.2. Smart Grid and Utilities

Recently, new IT technology has been used to maximize electricity output by taking into account consumer demands through the power supply. This distribution line's infrastructure, or smart grid, has the key aim of increasing the consistency of end-user service and maximizing the efficient generation of electricity. It consists of an interconnected network of the power plants and the final consumers that coordinates the output of power with end-user demand [52]. This extensive data sharing in smart grids poses significant risks for privacy in such a complex system, as the data will expose considerable and confidential information. Thus, a stable, confidential, decentralized framework needs to be established [54]. The benefits of blockchain for smart grids are decentralized trust, increased safety, greater resilience, greater transparency, improved scalability, greater efficiency, and enhanced computer capacity. The cryptographic securitization implemented, together with the consensus process, guarantees the immutability of the data inserted into the blockchain. Once an electricity transaction is included in the blockchain, it is difficult to change or delete it, leading to a stable and robust framework. Compared to the traditional, unified data architecture, there is no single compromise point, which eliminates exposure to malicious attacks. For both customers and power companies, blockchain-based trading infrastructure will provide greater clarity on pricing in terms of the production and consumption of electrical energy.

3.4.3. Smart City

The smart city is seen as a complex IoT model to handle and solve public challenges using the ICT approach [55]. Smart cities aim to use IoT services more effectively to improve service quality and reduce running costs. Thus, research has begun on integrating blockchain technology with advanced urban technology, using blockchain technology to ensure decentralization, and preserving security and privacy. The interconnected intelligent city network produces vast quantities of data from multiple sensors and methods and analyzes these data in decentralized blockchain databases. Privacy protection in smart cities cannot be simply achieved through the usual default methods. Some established technologies can, however, also be commonly used for various smart town implementations, including differential privacy, asymmetric encryption, and smart agreements to meet the need for secure data sharing across different processes. From the viewpoint of smart cities, lightweight privacy security is one of the most feasible solutions, as it offers good secrecy protection along with data utility power. Smart contracts are also considered a technology in smart city projects running over blockchain technology [52]. Moreover, blockchain has been used to facilitate a new voting system in smart cities. A voting blockchain has the ability to eradicate electoral fraud and increase electoral participation, as established at the Western Virginia mid-term election of November 2018.

3.4.4. Smart Finance

The extensive interconnections of IoT networks introduce new levels of financial services by improving performance measurement and data processing facilities [56]. The efficiency and standards of service in banks and the financial sector can be enhanced by IoT technology. For example, financial institutions may build the most effective way to monitor each transaction across their framework or contact layer. Using RFID, social networks, global positioning systems (GPSs), sensors and related mobile equipment offer intelligent data monitoring in certain types of gateways [57]. Blockchain technology can save distributors, exporters and other firms substantial time and resources by enabling and simplifying the dynamic world of trade finance. The use of smart contracts may lead to completely new kinds of financial services, including services that do not entail much hands-on work by legal experts to develop and execute. Smart contracts greatly minimize the confidence factor required to achieve an agreement [58]. The most profound feature of blockchain technology and the Bitcoin approach is that everyone can use it irrespective of race, gender, or cultural context. According to the World Bank, nearly 2 billion adults do not have bank accounts; most live in developing countries whose economies fully rely on money. These people also earn small incomes, paid in cash, which then must be stored in their homes or other places where it may be stolen or misused. Keys for a Bitcoin wallet can be kept on a cheap mobile phone or memorized, if needed. Future blockchain applications are also looking for solutions that not only serve as wealth storage accounts but also store medical records, property rights, and a number of other legal contracts [59].

3.4.5. Smart Transportation

Smart-transportation systems (STSs) are designed to reduce congestion and enhance the safety, sustainability, and performance of conventional transport systems using connectivity, device-to-device (D2D) communication, smart traffic and systems, and public transport systems. STSs are also called the Internet of Vehicles (IoV), where each passenger vehicle is connected to each other vehicle in a particular region by means of vehicle-to-vehicle (V2V) and device-to-device (D2D) connectivity [52]. Any vehicle can be tracked with the assistance of IoT technologies in the event of an emergency; it is also possible to use routes and past experience of vehicles to identify best routes at a particular time. In the future, real-time data on cars will be distributed and saved by smartphone apps such as Google Maps [60]. However, smart vehicles largely rely on onboard program and control functions. Thus, an attack on a vehicle's software may create severe safety issues for passengers and drivers, and wrongdoing by service providers or other customers cannot

be rapidly tracked or identified. Moreover, the cumbersome key security, verification, and authorization processes, as well as access control protocols and high costs, discourage the use of protected facilities [61]. The blockchain has properties that can help in exploiting and exchanging the data of a smart transportation system and ensure the system's trustworthiness and traceability. Using blockchain technologies allows numerous parties to be included, completely integrating the road network's potential, addressing multiple transport issues, and enhancing road safety and environmental security [62].

4. Blockchain-Based Platforms for IoT

This section discusses the most commonly used and popular blockchain platforms that support the integration of IoT application development and services.

4.1. Bitcoin Platform

Bitcoin is a popular blockchain platform which includes active cryptocurrency that provides decentralized systems to carry out transactions reliably without intermediaries or third parties [63]. Bitcoins are involved in many IoT platforms to make micropayments, acting as a wallet for transactions. However, Bitcoin uses limited Script language to carry out these transactions, whereas most IoT platforms use the common and reliable solution of smart contracts that are more secure for managing and recording all interactions in transactions without the limitations of Script language.

4.2. Ethereum Platform

Ethereum is a blockchain open-source framework that utilizes decentralized applications where anyone can own and control the platform [64]. Furthermore, this platform is flexible and adaptable, including smart contracts that allow integration of new technologies and applications of the IoT. It is an active and popular platform that uses the broad community to support the development of applications based on multiple languages, such as Go, C++ and Python. The platform is developed based on consensus mechanisms that allows the development and adaptation of IoT applications and reduces the latency of blockchain approaches. However, the platform does not provide the data confidentiality privacy required by most IoT applications.

4.3. Hyperledger-Fabric Platform

The Hyperledger-Fabric platform is a highly popular open-source platform (built based on the Golang and Java languages) allowing developers to build blockchain applications using a modular architecture approach [34]. This modular approach enables the platform to be extended with multiple components, such as membership services and consensus algorithms, making it a good choice to support business enterprise solutions, along with various other blockchain platforms. In addition, Hyperledger Fabric is a permission-based network that provides a data confidentiality feature to encrypt transactions so that they cannot be modified by unauthorized persons. However, there are numerous limitations and drawbacks related to the platform's ability to support IoT applications and development. For example, it is less or partially decentralized, more vulnerable due to trust issues, has only one validator node and has poor scalability of the consensus algorithms required to make a reliable system-based agreement across multiple devices of an enterprise's distributed network [12].

4.4. Multichain Platform

Multichain is a private blockchain platform that provides application development and deployment as well as offers privacy and a control-based P2P network [65]. The Multichain platform enhances and uses the existing Application Program Interface (API) of the core software of Bitcoin by extending new functionalities to support financial transactions. The platform provides both API and command-line interfaces to support Multichain configuration. In addition, Multichain is a permissioned blockchain that provides options

for application development: it can be either an open or closed blockchain depending on business needs. Moreover, it is an open-source blockchain platform that supports C, C++, Python and Java scripts. Although Multichain is a permissioned blockchain that provides a good solution for the IoT to collect data in case of concerns about data deletion, it does not protect against risks of data theft. Moreover, communication of smart things with other resources among a permissioned Multichain has a low performance level and is costly [66].

4.5. Quorum

Quorum is an open-source blockchain platform that was originally an extension of the Ethereum platform. Used in both industries and financial services, it offers public and private processing with higher transaction rates (100 transactions per second) [67]. Quorum is a permissioned network platform that includes smart contracts based on a simple consensus algorithm. However, there are bugs and defects in the code of Quorum, affecting file descriptors and increasing the load of contracts, which lead to consensus failure [68].

4.6. Lisk

Lisk is a fairly popular open-source blockchain framework that allows developers to build and adapt a decentralized system service using JavaScript [69]. The platform enables anyone to own and develop a customized sidechain that can be transformed into a complete application. The Lisk platform is still in its developmental stages, which includes three main tools: Lisk Commander, Lisk Element and Lisk Core. However, it has a number of issues: for example, the core infrastructure to build the designed proof-of-stake is apparently broken, and application development is very slow and inconsistent due to a lack experience of the people running Lisk Projects.

4.7. Litecoin

Litecoin is an open-source blockchain platform that provides a universal payment network with decentralized authorities and no central administration [70]. It is cryptocurrency blockchain and complementary to Bitcoin. Litecoin is technically similar to Bitcoin, but due to a reduction in block generation time and a proof of work based on Scrypt, a memory-intensive password-based key derivation function, it has faster transaction confirmation times and better storage efficiency [3]. In fact, Litecoin provides faster transaction confirmation times by producing a block every 2.5 min compared to Bitcoin, which generates a block every 10 min. Consequently, Litecoin solves the storage limitation issues of Bitcoin by improving storage efficiency. However, Litecoin supports C++ language-based cryptocurrency, which does not include the smart contracts required by most IoT platforms and application development services. It also requires more processing power. Neither is Litecoin as popular or broadly accepted as Bitcoin. In fact, some users of Litecoin lost access to their funds by computer malfunction because they failed to back up their private keys [71].

4.8. HDAC Technology

HDAC technology is a public permissioned blockchain platform that includes the first IoT contract with a designed payment platform [72]. It offers a transaction service for a machine-to-machine or machine-to-mobile (M2M) approach to control and support IoT devices such as smart cars, smart homes, and smart waters. The IoT contract includes a broad set of capabilities, including security processing and the reliable connection of devices. In addition, HDAC supports the Web Assembly language, which is an open standard language-based virtual machine that provides a compilation of numerous programming languages. However, the HDAC platform is still under development and will be launched as an IoT contract for smart homes.

4.9. IOTA

IOTA is an open-source blockchain platform based on the new concept of a block less distributed ledger [72]. The IOTA is based on "TANGL" technology, which means there are no chains, blocks, or fees. Tangle adopts Blockchain's anti-tampering distributed ledger, but instead of using chains such as Bitcoin, it uses a directed acyclic graph (DAG) structure. Transactions are validated in parallel and accepted almost instantly by the Tangle, giving IOTA a high transaction rate capacity [12]. In addition, the IOTA has abandoned transaction fees because IoT participants may become discouraged if the consumed transaction fee is comparable to the recorded transaction value. The IOTA platform offers secure and efficient real-time transactions with no fees based on a decentralized cryptocurrency to support IoT devices. The platform is less popular than previously described blockchain platforms. It supports many languages for application development, including Python, C, and JavaScript. However, the platform does not include smart contracts and does not offer open sources of coordinator nodes that lead to central risk [73]. Table 4 presents a comparison of the compound blockchain platforms for integrating and developing IoT applications. Most of these blockchains offer smart contracts to integrate the security of blockchain-based IoT applications. As a result, blockchains provide many security and performance requirements regarding IoT systems. However, there are still some unresolved security and performance challenges to improving integration between blockchain technologies and IoT systems, such as an IoT-centric consensus protocol, a checker for software integration, authentication of devices and validation roles to support financial transactions in IoT-based systems. The details of security and performance issues and challenges will be presented in Section 7.

Table 4. Blockchain platforms.

Platform	Blockchain	Popularity & Active	Consensus Algorithm	Pricing	Supported Languages	Smart Contracts
Bitcoin	Public	High	PoW	Fees per transaction	Script and C++	No
Ethereum	Public and permissioned	High	PoW, PoS GHOST	Ether for translation and computational service	Python, Go, C++, Java Scripts	Yes
Hyberledeger-Fabric	Private, Permissioned	High	PBTF	Open Source price	Python, Golang and Java	Yes
Multichain	Private, Permissioned	Medium	PBTF	Free, Open Source price	Python, C#, JavaScript, PHP, Ruby	Yes
Quorum	Public, Permissioned	High	Raft, IBFT	Fees per transaction	Python, Go, C++, Java Scripts	Yes
Lisk	Public and permissioned	Medium	DPoS	Fees per transaction	JavaScript	Yes
LiteCoin	Public	Low	Scrypt	Fees per transaction	C++	No
HDAC	Public and permissioned	Low	EPoW	Fees per transaction	Web Assembly	Yes
IOTA	Public, Permissioned	Low	PoW, TANGLE	Pricing not clear as yet	Python, C, JavaScript	No

Table 4 shows a comparison of the existing platforms of blockchain that are used to develop the IoT applications presented in this section. Most platforms include smart contracts, which allow application logic to be extended beyond cryptocurrency transactions. The most widely used programming languages are Python, Java Script, and C++, as well as the consensus algorithms are PoW and PBT. Since most platforms have public and consortium permissions, they can be used to build global and consortium applications. In fact, consensus algorithms are the core functions that determine how well blockchain-

based IoT applications perform in terms of block rates, consistency, scalability, and security. In open networks, consensus algorithms based on PoW are said to be the most secure. Due to its high computational requirements, pow, on the other hand, eliminates the possibility of block mining on IoT devices. PBFT-based consensus mechanisms for private blockchains can provide high block generation rates for IoT systems, but they restrict the number of miners that can participate [74]. Among the blockchain projects mentioned above, Ethereum is suitable for many IoT applications containing a large number of IoT systems and heterogeneous networks. Ethereum, as a public blockchain, has a high level of scalability because it can support a large number of heterogeneous devices. On the other hand, Hyperledger Fabric is appropriate for IoT networks with large amounts of data. Fabric has integrated blockchain through its client-service approach and achieved high transaction volumes of up to tens of thousands per second. Hyperledger Fabric needs a controllable network infrastructure and is not as open to the public as Ethereum.

5. Role of Blockchain in IoT

This section discusses the crucial roles blockchain plays in boosting the domain of IoT applications, include providing high scalability, preserving full data privacy, ensuring interoperability and orchestration of connected devices. Figure 2 presents the roles of blockchain in IoT.

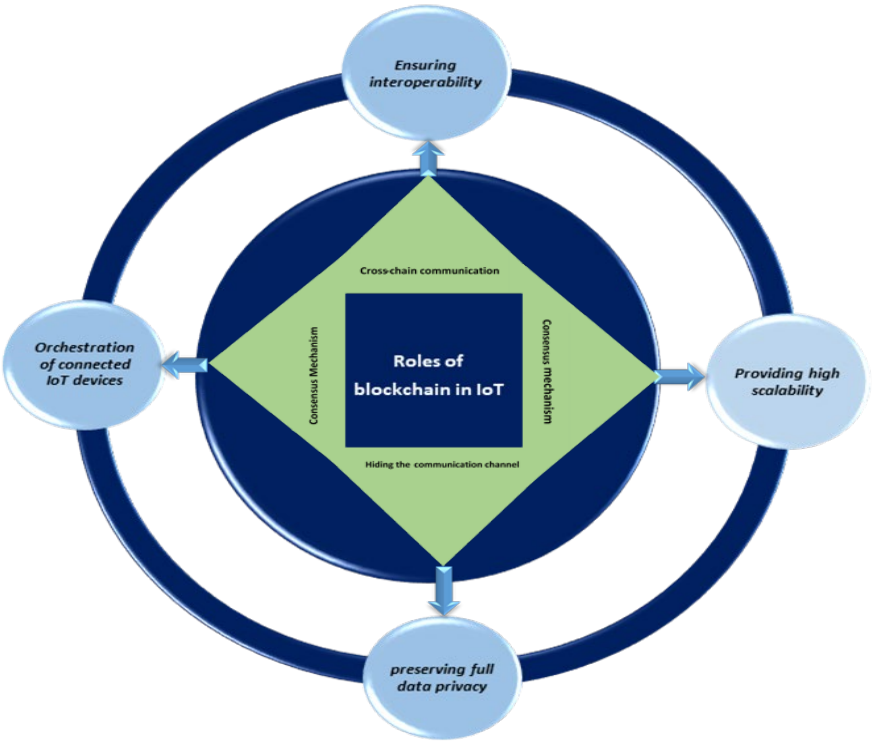

Figure 2. The role of blockchain in IoT applications.

5.1. Providing High Scalability

In IoT settings, millions of devices enter IoT networks; as a result, networks become incredibly slow and costly. This delay occurs because billions of microtransactions between connected devices must be verified and authenticated. A lack of scalability means huge delays in the verification of transactions. Blockchain includes a fast consensus mechanism for providing high scalability [75,76]. The transition from a centralized to a P2P distributed network will eliminate central failures and limitations [77]. It will also help to avoid scenarios in which a few business corporations govern the processing and storage of a large number of people's information. Other advantages of decentralizing the architecture include increased system scalability and fault tolerance. It would help to reduce IoT silos while also contributing to improved IoT scalability.

5.2. Preserving Full Data Privacy

The blockchain mode relies on access privileges that IoT users have to read/write mostly on general grounds, that is, whether they have public or private access to read, write and achieve agreements of consensus. Blockchain preserves data privacy by different approaches, such as using pseudonyms to avoid linking transactions to real identities [78]. In their journey, IoT users are not truly totally anonymous because the users behind all these pseudonyms can be tracked and linked, particularly when managing multi-entry transactions with multiple addresses from different accounts of the same user [79]. Public blockchains, which support most cryptocurrencies, allow any IoT users in any location to join the system based on the implementation of consensus mechanisms. Private blockchains follow either an automatic approach or use a gatekeeper to control access to an IoT network and transaction levels [79]. Blockchain enables the system user to share the important data in real time while hiding the communication channel from forgery and theft. Each blockchain-based transaction maintains the corresponding hash, which generates a binary Merckle tree in the header along with a timestamp and identifier of the next block. When an attacker tries to modify the records stored in the blockchain, modification of the hash of every subsequent block is required, which is practically impossible to achieve [80]. Privacy-preserving techniques in blockchain support anonymity in transactions and control privacy. The most important technologies and crypto solutions for privacy security in blockchain include secure multiparty computing, zero information checks, commitment plans, ring signatures and homomorphic hiding [79].

5.3. Orchestration of Connected IoT Devices

The blockchain orchestrates the management of IoT infrastructure and smart contracts in a given environment. Smart contracts are responsible for defining the decisions of blockchain relevant to IoT systems. Blockchain facilitates the coordination of all IoT operations, including the management of access to and from smart devices, data development and processing, dynamic positioning, and container changes, such as software devices [81]. The orchestration of the activities of IoT devices is associated with different trust and security concerns, such as recording the identity of all IoT entities in the system, recording the provenance of devices' data and of other entities entering the IoT system, and recording the processing steps by using smart contracts [82].

5.4. Ensuring Interoperability

Interoperability concerns enabling two or more completely different IoT systems or devices to communicate and exchange information. A blockchain-based IoT system implements interoperability by enabling different blockchains to easily communicate with each other (cross-chain communication) [83–85]. This ensures integration with existing systems by initiating transactions on other networks, conducting transactions with other chains, and integrating the apps on the same chain. Cross-chain communication archives data through two main approaches, including atomic swaps and stateless Simplified Payment Verifications (SPVs). Atomic swaps allow IoT users to trade the same cryptocurrency directly in P2P transactions. This approach allows two entities to coordinate transactions across chains, although it is not considered a true form of cross-chain communication. Stateless SPVs allow a smart contract to verify a subset of transaction history. Relays enable a smart contract to verify block headers and events on another chain. Merged consensus enables two-way interoperability between chains by utilizing a relay chain. In federations, a selected group of trusted parties are allowed to confirm the events of one chain by another.

6. Recent Advances

This section highlights recent progress in research efforts (frameworks, models, architectures and protocols) aimed at blockchain for IoT. The proposed solutions are summarized in Table 5 and discussed below.

Table 5. Recent advances in Blockchain for IoT systems.

References	Mode of Blockchain	Addressed Blockchain Technology	Solution Type	Proposed Solution	Supported IoT Application
Latif et al. [86]	Private	Distributed ledger	Architecture	To secure lightweight, and decentralized private blockchain	IIoT
Wu and Liang [87]	Private	Smart contract	Method	To manage trust and check computation process	IoT
Fan et al. [88]	Private	Not mentioned	Scheme	To secure data sharing and data transmission	IoT
Zhang et al. [89]	Private	Smart contract	Algorithm	To secure outsource of bilinear-pairings of IoT devices	IoT devices
Rathee et al. [90]	Private	Not mentioned	Framework	To secure records of products in various zones	IIoT
Singh et al. [91]	Private	Smart contract	Framework	To manage data protection, authentication, and immutability.	Healthcare applications
Latif et al. [92]	Private	Smart contractDistributed ledger	Framework	To manage and control health data	Healthcare Applications
Lin et al. [93]	Private	Smart contract	System	Security of bilinear pairings-based outsourcing	IoT devices
Uddin et al. [94]	Private	Consensus protocol	Architecture	Manage and monitor patient data	Smart health
Gong et al. [95]	Private	Smart contract	Model	Store IoT data	IoT devices
Huang et al. [96]	Private	Consensus protocol	System	Improve identity authentication	IoT network
Zhang et al. [97]	Private	Not mentioned	Connection protocol	Support distributed services	IoT network
Singh et al. [98]	Private	Consensus protocol	Architecture	Secure and scale of IoT resources	General IoT
Memon et al. [99]	Private	Not mentioned	Architecture	Eliminate device drop rate	IoT devices
Si et al. [100]	Private	Consensus protocol	Mechanism	Secure information sharing of IoT based blockchain	General IoT
Jiang et al. [101]	Private	Not mentioned	Scheme	Improve privacy-preservation of thing-clients (check this)	IoT devices
Casado-Vara et al. [102]	Private	Not mentioned	Model	Improve monitoring and controlling of searching IoT data	IoT network

Table 5. *Cont.*

References	Mode of Blockchain	Addressed Blockchain Technology	Solution Type	Proposed Solution	Supported IoT Application
Bruneo et al. [103]	Private	Smart contract	System	Manage and monitor smart cities	Smart cities
Rathee et al. [104]	Private	Not mentioned	Framework	Extract IoT information	Industrial IoT
Wang et al. [105]	Public	Consensus protocol	Model	Validate test-beds and impact on public blockchain	IoT devices
Huang et al. [106]	Private	Consensus protocol	Mechanism	Secure IoT devices	Industrial IoT
Biswas et al. [107]	Private	Local ledger	Framework	Improves scalability of local ledger	General IoT
Pan et al. [108]	Private	Smart contract	Framework	Manage and improve resources of IoT devices and Cloud	IoT devices
Novo [109]	Private	Smart contractConsensus protocol	Architecture	Manage accessibility of IoT systems	IoT devices
Qian et al. [110]	Private	Not mentioned	Scheme	Manage security based blockchain of IoT	HealthcareIoT devices
Minoli and Occhiograsso [26]	Private	Consensus protocol	Mechanisms	Secure IoT as general	General IoT
Agrawal et al. [111]	Private	Not mentioned	Mechanism	Secure IoT systems	IoT systems
Zhang and Wen [112]	Private	Smart contract	Model	Supports business-based IoT	Smart financial

Latif et al. [86] proposed an architecture to enable an IoT network based on blockchain that is stable, lightweight, and decentralized and that executes many essential operations, such as user and system registration, data storage, and computer activity, in a trusted manner. The experimental findings demonstrated that the planned architecture outperformed other state-of-the-art systems. Wu and Liang, [87] presented a method of trust management based on blockchain named BBTM. The proposed BBTM is used to compute trust while maintaining desirable trust precision, convergence, and attack resiliency. The effectiveness of the proposed BBTM method is demonstrated by the experimental results. However, the study lacks a model of more complex smartphone scenarios and verify BBTM for real-world IoT systems. Fan et al. [88] suggested a scheme of authentication and data sharing of the IoT based on blockchain technology. The study evaluation of the proposed scheme indicated that it achieved a tradeoff between IoT security and performance properties compared with recent studies in the literature. However, the study does not cover all of the authentication approaches to provide better security of IoT data transmission.

Zhang et al. [89] presented an algorithm to secure outsources of bilinear pairings of IoT devices. The performance of the proposed algorithm is vastly improved over the implementation of standard bilinear pairing. According to theory and experiments, the algorithm works well and is quite stable. However, the study is limited to secure outsources of bilinear pairings of IoT devices. Rathee et al. [90] suggested a framework based on a hybrid blockchain approach for securing a multinational level industrial Internet of Things (IIoT) of offices in several countries. The proposed framework has been rigorously tested against different security parameters in comparison to standard mechanisms. However, the study does not cover cost-related problems for customers or organizations, which remain unresolved obstacles. Singh et al. [91] suggest a framework of patient-centric blockchain that discusses the concerns of data protection, authentication, and immutability. The proposed framework is built on the Hyperledger platform. The findings support the feasibility of the suggested framework. However, the framework does not support service-based fault tolerance. Latif et al. [92] proposed a framework-based Ethereum platform of smart contracts for a blockchain-based healthcare infrastructure. The proposed framework would be altered by leveraging the values and technology of a distributed ledger, which would alter the healthcare industry's blockchain-based vision. A database of medical treatments that can be segmented into blocks for diagnosis, reports of test findings, and commentary by experts can all be maintained as transactions. The framework would be beneficial in hospital settings and would help improve the efficiency of the healthcare environment. Lin et al. [93] introduced an approach based on an open-source blockchain (Ethereum) to secure out-sourcing of bilinear pairings of IoT systems. Their approach addresses the insufficiency, assumptions, and centralization limitations of bilinear pairings. They validated the feasibility and efficiency of the approach for securing IoT applications.

Uddin et al. [94] designed an eHealth system for sensing NEAR processing and FAR processing layers. They proposed a patient agent system to enable reliable security and private communication to be replicated across the three layers. The proposed system is based on 5G architecture to manage the 5G network resources and health data based on blockchain approaches. The patient agent system involves a blockchain-based consensus mechanism that utilizes an algorithm to leverage task offloading for the purpose of ensuring patients' privacy during outsourcing tasks. The test results of the eHealth system demonstrated the reliability of processing the health data in real-time by using blockchain approaches.

Gong et al. [95] explored a simple four-layer IoT blockchain modeling approach comprising various types of IoT computers. In fact, the first layer is the perceptual layer, which consists of IoT devices. The second layer is the network layer, which serves as the backbone of the IoT, transmitting and processing information obtained by the perception layer. The third layer is the blockchain layer. It serves as a secure ledger for all participants, and smart contracts are built on top of it to enable fast, immutable transactions between various devices. The last layer is the application layer, which is responsible for implementing the

interface between the IoT and users. The proposed model shared a file system for storing massive quantities of IoT. They proposed the use of an Ethereum blockchain as a case study for blockchain-based IoT technology and an autonomous trading device. The suggested model validated the claim that blockchain boosts IoT applications in terms of confidentiality, tracking and security. Huang et al. [96] proposed an authentication system based on networked identity and blockchains. The system was tested in terms of the block speed and the performance time of the blockchain under the condition of blockchain privacy. The memory and the related traffic use of the wallet and data upload method were analyzed to verify device stability and the rationality of the blockchain-based IoT authentication system.

Zhang et al. [97] presented a connection protocol-based blockchain to ensure terminal reliability in the IoT. The proposed protocol confirmed terminal device protection in IoT networks. The protocol also offered a trusted network link protocol based on blockchain to carry out shared authentication processes, platform validation and trusted network access via cryptography between IoT terminals. Singh et al. [98] proposed an intelligent IoT architecture based on blockchain to combine artificial intelligence and blockchain to support the goal of secure and scalable IoT systems. The proposed architecture provides secure, decentralized big data analysis tasks in IoT applications, as well as efficiency in terms of accuracy, centralization, security, privacy, and latency. The results of the proposed architecture outperformed existing IoT architectures. However, the issues of latency and computational power are not completely addressed.

Memon et al. [99] proposed an architecture that contrasts with the current centralized IoT datacenter. The proposed architecture eliminates the device drop rate and further discharges the cloud datacenter with limited upgrades to the current IoT ecosystem. Furthermore, the architecture's reduced device load saves capital and maintenance costs and reduces energy supplies and carbon emissions. The suggested architecture was also evaluated for maximizing cloud computing capabilities. Si et al. [100] introduced a framework for the security of blockchain-based IoT knowledge exchange. The proposed framework integrates data and a transaction blockchain by adopting a double chain model and improving the consensus algorithm. The results of the proposed framework show that it is effective, safe, and feasible for verifying location information and securing the system's storage devices. The proposed solution concerns security during information sharing in IoT systems. However, privacy leakage is not addressed.

Jiang et al. [101] presented a privacy-preserving thin-client scheme based on a blockchain approach to address privacy and authentication issues of IoT devices. The proposed scheme solves the limitation of the storage capacity of thin-client equipment. The scheme was also validated by a high-security analysis with comprehensive functionality. However, the impact of the computational overhead of thin clients on smartphones needs further investigation. Casado-Vara et al. [102] presented a model to improve the efficiency of the control and monitoring of IoT network-based blockchains. The model validated a number of blocks for processing efficiency using queuing theory. In addition, the model improved search speeds, based on HashMaps (a basic data structure for storing key-value pairs and retrieving them quickly), to enable an efficient, reliable, and faster monitoring process for IoT platforms. However, this solution requires further extension to meet the requirements of generic IoT applications.

Bruneo et al. [103] developed a solution approach based on blockchain technology via a SmartME project (Integrated program management and MEL suite for development funds and programs), which offers a uniform and abstract environment in the layer of heterogeneous devices to support crossing to the IoT and cloud. They demonstrated the adaptability and flexibility of the developed approach to allow small and medium cities to transform into smart cities easily and at a low cost by recycling existing infrastructure. However, the scalability of the proposed solution has not been properly tested. Rathee et al. [104] proposed a blockchain framework that was used to strip metadata-based IoT devices and store the records extracted in blockchain to ensure confidentiality among the

various users residing at different locations. They also explored the use of the framework by applying it to blockchain internal communication, in which multiple intruders searched IoT computers. The results were evaluated against other simulation results and included an 89% performance rate over the user implementation period for falsifying attacks, black hole attacks and probabilistic encryption scenarios based on blockchain technologies.

Wang et al. [105] suggested a time model Markov chain to validate test beds and to evaluate the effect of block mining speeds and network capacity on public blockchain capability. The test bed and study demonstrated that blockchain capability can be enhanced by speeding up the process of block mining, although this increases blockage. The model analysis gives the blockchain potential an exponential upper limit. Huang et al. [106] presented a credit-based mechanism for industrial IoT. The mechanism provides a credit-based PoW algorithm for IoT devices that can simultaneously guarantee system safety and transaction performance. The mechanism introduced the Raspberry Pi framework, and a case study was carried out for the intelligent factory. The results of extensive assessment and analysis indicate that the credit-based PoW and internet connectivity control system are secure and effective in industrial IoT.

Biswas et al. [107] proposed a framework based on blockchain to secure transactions in the IoT. The proposed framework generates a local peer network to enable the blockchain ledger to be scaled through all peers. The evaluation of the proposed framework showed reductions in universal peers, the ledger scale and block weight. It also enhanced the rate of a transaction with peers by loading distribution. Pan et al. [108] designed an IoT framework based on smart contracts and blockchain. The designed framework integrates blockchain and a coin system to connect the pooled resources and usage of a cloud with each account of IoT devices. In addition, smart contracts organize the behavior of IoT devices via policies and roles, and all transactions and activities of the IoT are registered into the blockchain for secure data logging and auditing. The evaluation of the framework showed significant scale security of IoT applications by using the security benefits of smart contracts and a blockchain approach.

Novo [109] proposed an architecture of proof-of-concept based on a blockchain approach to develop a system of access management for IoT resources. He designed a decentralized policy for the system that stored data into blockchain technology. A validation of the architecture suggested the significant advantage of scalability when the load is distributed across multiple nodes of the blockchain network toward IoT devices. Qian et al. [110] proposed a scheme based on blockchain to secure and manage multiple IoT devices. The proposed scheme allows analysis of the security problems of applications, the network, and perception layers. In addition, they adopted an algorithm-based identification device to connect the blockchain database and IoT devices to guarantee reliability and security.

Minoli and Occhiograsso [26] presented blockchain mechanisms to support the security of IoT applications. The proposed mechanisms enable a cluster of IoT ecosystems to be protected from attacks. Involving blockchain enables the cooperation of the mechanisms through multiple domains and layers, starting from the bottom layer to the top layer of the applications. Agrawal et al. [111] presented a blockchain mechanism for IoT security based on the decentralization feature of blockchain to enable continuous security for the IoT system without user intervention. Zhang and Wen [112] introduced a model of an IoT E-business. The model investigated 4 stages of transaction of traditional E-business: negotiation, preparation, contract signing and contract fulfillment. They introduced a model of P2P transaction based on blockchain to support decentralization of IoT E-business. They also designed an approach based on a smart contract to facilitate transaction of IoT E-businesses' paying data and intelligent property.

7. Challenges and Open Future Trends

This section addresses the primary issues which need to be overcome in the challenging task of implementing and integrating IoT applications with a blockchain approach. For an

internet scenario, blockchain approaches have been built with high-performing devices, but this is far from the IoT reality; transactions using the blockchain approach need a cryptographic identity and this capability must be provided for machines capable of working with a currency. In this section, several of the challenges and future trends are discussed, as shown in Figure 3.

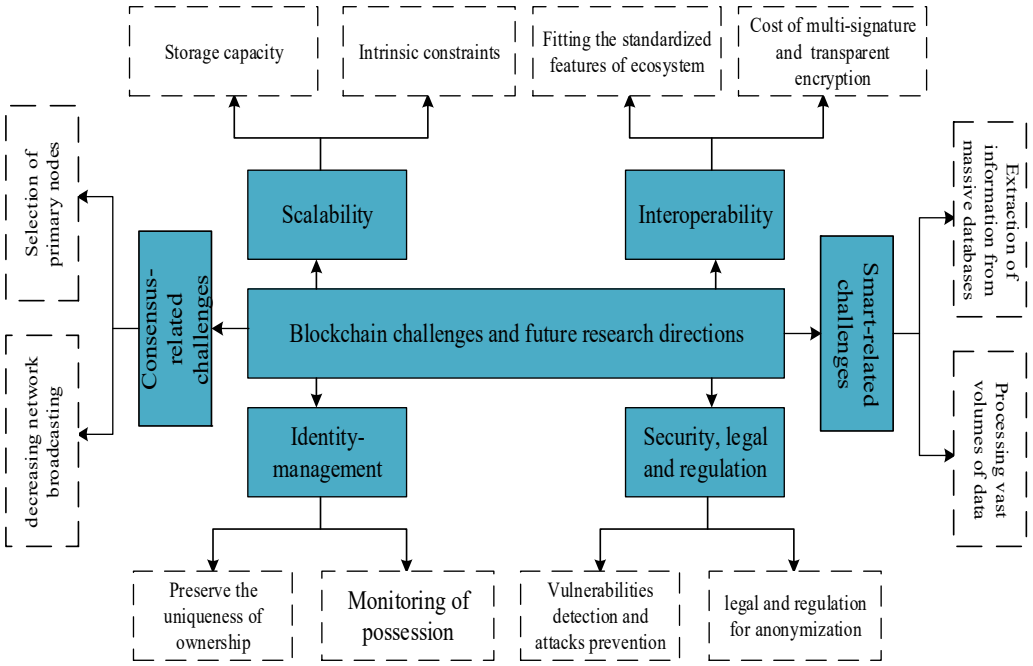

Figure 3. Blockchain challenges and future research directions.

7.1. Scalability-Related Challenges

The scalability and storage capacity of blockchains are issues that are always under consideration. In the case of IoT implementations, however, the intrinsic constraints of scalability and storage capacity make these concerns much greater. Only a few transactions per second can be handled by many existing blockchain implementations. This may be a possible bottleneck for the IoT Blockchain, which might seem inappropriate for IoT systems, where sensors can generate real-time gigabytes of data (GBs). Appropriate technologies should be incorporated to reduce or eliminate these constraints [3].

7.2. Interoperability-Related Challenges

The key element for maintaining interoperability in blockchain-based IoT applications is resource sharing. However, resource sharing faces many challenges, including high costs, user identity scores, and management of shared resources. A secure, low-cost trading mechanism is simple to implement as a platform-centered blockchain solution. For data sharing, the issues are how data worth can be measured, how data can be traded and exchanged, and how the accumulation of data can be avoided. The common ledger generated by the blockchain approach allows the flow of real-time information between different parties to be monitored and controlled to reduce the expense of the management of the data sharing mechanism. For example. the creation of a consolidated energy sharing system is feasible. It is possible to apply a blockchain approach to the network associated with electricity. Its benefits include no central scheduling control agency, a cross-energy universal management system for the system, confidentiality, and data reliability. The multi-signature and transparent encrypted information-related decentralized energy trading framework allows colleagues to anonymously determine costs for energy and maintain transaction protection. It also solves issues regarding the correct measurement, interaction, self-discipline regulation and decisions on optimization [9,106,113,114].

7.3. Consensus-Related Challenges

The consensus protocol of the blockchain approach consumes a significant number of computational resources and energy in realistic transactions, which leads to poor system performance and lengthy system latency. However, for the applications proposed in recent studies, the blockchain needs greater and more compliant operating capabilities. A significant problem that the approach needs to address is a method of interaction that combines and uses the community knowledge of distributed consensus nodes. While the study of the blockchain approach is comparatively mature, several problems still need to be solved regarding the development of protocols. The goal is to build consensus structures to improve system efficiency. For instance, an algorithm for consensus protocols is needed to improve accuracy in selecting primary nodes from a limited number of trusted nodes. In addition, a consensus algorithm is needed to decrease network broadcasting centered on a basic security premise. To date, a set of protocols has been tailored to the specifications and functionality of various channels for blockchains. Studies on consensus protocols from different viewpoints have been analyzed and contrasted. The ultimate objective is to achieve optimum protocols to save time and costs and to manage competitors while ensuring scalability, execution and identity, privacy, and protections at higher levels [9,115].

7.4. Smart-Contract-Related Challenges

Smart contracts have been characterized as representing the ultimate development of the blockchain approach, but there are multiple ways to incorporate them into IoT applications and many related issues. A contract is a set of code, methods, and data from a functional point of view with states residing in a particular blockchain address, whereas public roles may be named by the function of devices are a cause of accidents, and applications search to respond correctly to the targets for the case. A transaction must be released on the network to alter the conditions of the contract, that is, to adjust to the blockchain change approach. Transactions are approved by consignors and must be approved by the network. Intelligent contracts will provide the IoT with a stable and secure processing device, documenting and controlling all its interactions. The component elements will be efficient and safe to process. Smart contracts should, therefore, model the application logic of IoT applications securely. However, various problems arise in that integration, which will be discussed below [3]. Acting with smart contracts requires the use of data feeds from real-world systems, known as oracles. These are unique tools that provide real-world data with confidence. Since the IoT can be unreliable, validating such smart contracts may be compromised.

In addition, accessing multiple sources of data could overwrite these agreements. Smart contracts are currently decentralized and distributed, but they still cannot address the problems of massive computational quantity by sharing resources to spread tasks. In fact, only a single node executes smart contracts, while multiple nodes undertake code execution simultaneously. This distribution is only performed for the verification process rather than using it to distribute all the activities. To boost its computational power, the IoT has leveraged cloud computing and big data delivery capabilities to solve problems of data mining, allowing a deeper interpretation through increased computational capacity. The distributed nature of smart contracts is used in the incorporation of IoT applications with the blockchain approach to allow the processing capabilities offered by most other paradigms, for instance, cloud platforms and big data, which are necessary to support IoT applications [3].

7.5. Identity-Management-Related Challenges

A key need is the management of personal identity. There are several information acquisition issues regarding identification records, which include weak correlation of data, inadequate data, and outdated or false data. The management of possession is generally used for property rights and copyright management and traceability, including vehicles, buildings, paintings, and publications in digital format. In this context, significant issues

include product authentication and ownership of management, security and efficiency of transactions, and protection of privacy. Ownership may be written on the blockchain and cannot be changed. The blockchain approach can ensure precise execution of the contract and monitoring of possession of properties after the contract is made. Using hashing algorithms and timestamps, the blockchain approach confirms ownership and establishes the presence, validity, and uniqueness of judgments by offering digital evidence, such as video, text, and sound, with no manipulation. Ownership needs to be verified once it is established. To preserve the uniqueness of ownership, documents are kept in the common ledger [9,116–118].

7.6. Security, Legal and Regulation Challenges

Blockchain has gained attention because of its extremely strong anti-tampering technology in decentralized networks. The blockchain approach does not explicitly require peers to trust one other. However, it still has vulnerabilities [119]. Typical security risks of the blockchain approach are as follows:

7.6.1. Consensus Protocol Attacks

By obtaining a significant share of the computational resources of the whole network, attackers might crack the security hypothesis of consensus protocols. The chain can then be managed and reconstructed by such attackers. An example is an attack on the PoW blockchain, such as that used in Bitcoin [120]. Attackers who possess over half of the strength of hash can force a blockchain to accept unauthorized blocks by resolving the problem of consensus more quickly than the rest of the peers (e.g., PoW in Bitcoin). At present, 33% hash power has been shown to be adequate to resolve vulnerabilities PoW [9,120].

7.6.2. Smart Contract Vulnerabilities

A smart contract is unsafe because the blockchain technique is easy to setup and permanent. The public is open to vulnerabilities and theft, even adversaries. Moreover, because of the irreversibility of the blockchain approach, it is impossible to eliminate build-in resistance vulnerabilities from the smart contracts deployed. The 2016 attack on the decentralized autonomous organization (DAO), which culminated in a forked blockchain technology of Ethereum, is a notable illustration [9].

7.6.3. Privacy Protection

With the rapid rise of information and communication technology (ICT), privacy considerations have attracted increasing interest, particularly financial and medical data. Blockchain verification and faith mechanisms are a versatile combination of blockchain strategy and privacy security, allowing for openness of data and access privileges to be easily handled. To protect against attacks using a safe and fair method of transaction such as Sybil and anti-DoS threats, cryptocurrency is viewed as an opportunity to improve privacy. Hashing approaches and algorithms are used to encrypt information to guarantee accessibility and scalability of smart contracts. In addition, blockchain addresses the question of specific and critical data monitoring [9,121,122]. The majority of IoT applications, regardless of their critical functionality, continue to work indefinitely except for some software or hardware updates. As a result, they are more resistant to cyberattacks. Therefore, software firmware and runtime updates are critical requirements [12].

7.6.4. Legal and Regulation

Although the blockchain approach has transformed society in many respects, legal and legislative standards have also been questioned. Blockchain has experienced a variety of legal problems, notably in its initial development phase, due to the lack of legal oversight and awareness of the existence of blockchain solutions [123]. Comprehensive knowledge of blockchain functionality can help to build and strengthen legal regulations relevant to blockchain operations. Many nations are currently implementing blockchain technology

together with the enhancement of regulatory initiatives, such as e-centralization, ethical and legal studies and jurisdiction problems, real name anonymization and internet problems, issues of accessibility and termination rights, and issues of openness and privacy of personal data. Furthermore, technology and legal issues are reciprocal options in the area of local administration and social governance. If the cost of a technological solution for a social issue is less than the legal solution, the technical method will substitute the legal method as the primary means of producing orders. Blockchain approaches have facilitated the existence of smart contracts and distributed verifiable databases that have the ability to transform legal and technical limits, giving rise to new governance models. Moreover, the effects of these technical solutions, such as improved equity and justice, can also increase the degree of productivity and the certainty of the law. The best outcome in assessing the virtuous circle of the blockchain method is that technology determines everything, yet retains legal validity [9,124].

8. Conclusions

This paper investigated security and privacy issues and challenges to support the integration of blockchain technology with the Internet of Things. In particular, most IoT systems are facing security and privacy issues such as cyberattacks. Hence, we explored blockchain technologies, protocols, and properties such as distributed ledgers, smart contracts, decentralization, security, and privacy that integrate and solve IoT issues. In this paper, we discuss a blockchain for IoT thematic taxonomy focused on the most relevant considerations. Further, we explain and debate the most critical blockchain platforms that have been implemented for IoT applications, such as the Hyperledger-Fabric and Ethereum platforms. Furthermore, we emphasize blockchain technology's role in broadening the reach of IoT applications. Moreover, we explore the most current advancements and applications for the IoT world.

We believe that blockchain will be a critical technology in IoT applications. Innovations in blockchain technology and their deployment in IoT applications to increase the quality of life are common topics in today's research communities. However, there are several problems and necessary restrictions to be explored and overcome before using the blockchain approach in IoT applications. This survey will assist researchers in identifying and addressing the issues associated with designing and integrating blockchain-based technologies for IoT applications.

Author Contributions: Conceptualization, A.A. and A.I.A.A.; methodology, M.A.; software, T.A.E.E.; validation, S.A.G., F.K.K. and H.A.; formal analysis, A.A.; investigation, A.I.A.A.; resources, M.A.; data curation, T.A.E.E.; writing—original draft preparation, A.I.A.A.; writing—review and editing, A.A.; visualization, H.A.; supervision, A.A.; project administration, S.A.G.; funding acquisition, F.K.K. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Review Article, under grant number (R.A./37/43). Princess Nourah bint Abdulrahman University, Researchers Supporting Project number (PNURSP2022R300), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Review Article, under grant number (R.A./37/43). Princess Nourah bint Abdulrahman University, Researchers Supporting Project number (PNURSP2022R300), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript or in the decision to publish the results.

References

1. Ahmed, E.; Yaqoob, I.; Hashem, I.A.T.; Khan, I.; Ahmed, A.I.A.; Imran, M.; Vasilakos, A.V. The role of big data analytics in Internet of Things. *Comput. Netw.* **2017**, *129*, 459–471. [CrossRef]
2. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]
3. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
4. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Gener. Comput. Syst.* **2019**, *100*, 325–343. [CrossRef]
5. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
6. Global, T.F. History of Blockchain. 2019. Available online: https://www.tradefinanceglobal.com/blockchain/history-of-blockchain/ (accessed on 22 November 2020).
7. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–36.
8. The 5 Best Blockchain Platforms for Enterprises and What Makes Them A Good Fit. 2019. Available online: https://medium.com/swishlabs/the-5-best-blockchain-platforms-for-enterprises-and-what-makes-them-a-good-fit-1b44a9be59d4 (accessed on 7 September 2021).
9. Lu, Y. The blockchain: State-of-the-art and research challenges. *J. Ind. Inf. Integr.* **2019**, *15*, 80–90. [CrossRef]
10. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
11. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
12. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [CrossRef]
13. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
14. Cui, P.; Guin, U.; Skjellum, A.; Umphress, D. Blockchain in IoT: Current Trends, Challenges, and Future Roadmap. *J. Hardw. Syst. Secur.* **2019**, *3*, 338–364. [CrossRef]
15. Viriyasitavat, W.; Anuphaptrirong, T.; Hoonsopon, D. When blockchain meets internet of things: Characteristics, challenges, and business opportunities. *J. Ind. Inf. Integr.* **2019**, *15*, 21–28. [CrossRef]
16. Mohanta, B.K.; Jena, D.; Ramasubbareddy, S.; Daneshmand, M.; Gandomi, A.H. Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet Things J.* **2020**, *8*, 881–888. [CrossRef]
17. Lo, S.K.; Liu, Y.; Chia, S.Y.; Xu, X.; Lu, Q.; Zhu, L.; Ning, H. Analysis of blockchain solutions for IoT: A systematic literature review. *IEEE Access* **2019**, *7*, 58822–58835. [CrossRef]
18. Mohsin, A.; Zaidan, A.; Zaidan, B.; Albahri, O.; Albahri, A.; Alsalem, M.; Mohammed, K. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Comput. Stand. Interfaces* **2019**, *64*, 41–60. [CrossRef]
19. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [CrossRef]
20. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*, 100081. [CrossRef]
21. Rao, A.R.; Clarke, D. Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet Things* **2020**, *10*, 100079. [CrossRef]
22. 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]
23. Azbeg, K.; Ouchetto, O.; Andaloussi, S.; Fetjah, L. A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications. *IRBM* 2021, *in press*. [CrossRef]
24. Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [CrossRef]
25. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
26. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *Internet Things* **2018**, *1*, 1–13. [CrossRef]
27. Tasca, P.; Tessone, C.J. Taxonomy of blockchain technologies. Principles of identification and classification. *arXiv* **2017**, arXiv:1708.04872. [CrossRef]
28. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
29. Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Pautasso, C.; Rimba, P. A taxonomy of blockchain-based systems for architecture design. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017; pp. 243–252.

30. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
31. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
32. Khalilov, M.C.K.; Levi, A. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2543–2585. [CrossRef]
33. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Das, G. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [CrossRef]
34. Hyperledger Fabric. Available online: https://www.hyperledger.org/projects/fabric (accessed on 15 July 2020).
35. Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. Consortium blockchain-based malware detection in mobile devices. *IEEE Access* **2018**, *6*, 12118–12128. [CrossRef]
36. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
37. Scardovi, C. *Restructuring and Innovation in Banking*; Springer: Berlin/Heidelberg, Germany, 2016.
38. Ølnes, S.; Ubacht, J.; Janssen, M. *Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing*; Elsevier: Amsterdam, The Netherlands, 2017.
39. Arslan, S.S.; Jurdak, R.; Jelitto, J.; Krishnamachari, B. *Advancements in Distributed Ledger Technology for Internet of Things*; Elsevier: Amsterdam, The Netherlands, 2020.
40. Buntz, B. It's Time to Rethink Distributed Ledger Technologies for IoT. 2020. Available online: https://www.iotworldtoday.com/2020/01/08/its-time-to-rethink-distributed-ledger-technologies-for-iot/ (accessed on 2 October 2020).
41. Mearian, L. What's a Smart Contract (and How Does It Work)? 29 July 2019. Available online: https://www.computerworld.com/article/3412140/whats-a-smart-contract-and-how-does-it-work.html (accessed on 15 October 2020).
42. Smartz. How Blockchain and Smart Contracts Can Impact IoT. 21 August 2018. Available online: https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-impact-iot-f9e77ebe02ab#:~{}:text=With%20such%20features%2C%20a%20blockchain,execute%20automatically%20via%20smart%20contracts. (accessed on 16 October 2020).
43. Lao, L.; Dai, X.; Xiao, B.; Guo, S. G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications. In Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), New Orleans, LA, USA, 18–22 May 2020; pp. 664–673.
44. Wang, E.K.; Sun, R.; Chen, C.-M.; Liang, Z.; Kumari, S.; Khan, M.K. Proof of X-Repute Blockchain Consensus Protocol for IoT Systems. *Comput. Secur.* **2020**, *95*, 101871. [CrossRef]
45. Sharma, P.K.; Chen, M.-Y.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2017**, *6*, 115–124. [CrossRef]
46. Banafa, A. Decentralizing IoT Networks through Blockchain. 2016. Available online: https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228 (accessed on 1 October 2020).
47. Dedeoglu, V.; Jurdak, R.; Dorri, A.; Lunardi, R.; Michelin, R.; Zorzo, A.; Kanhere, S. Blockchain technologies for iot. In *Advanced Applications of Blockchain Technology*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 55–89.
48. Abdi, A.I.; Eassa, F.E.; Jambi, K.; Almarhabi, K.; AL-Ghamdi, A.S.A. Blockchain Platforms and Access Control Classification for IoT Systems. *Symmetry* **2020**, *12*, 1663. [CrossRef]
49. Victora, S. IoT Guard: Usable Transparency and Control Over Smart Home IoT Devices. Ph.D. Thesis, Technische Universität Wien, Wien, Austria, 2020.
50. Sunny, J.; Undralla, N.; Pillai, V.M. Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Comput. Ind. Eng.* **2020**, *150*, 106895. [CrossRef]
51. Cuomo, J. How Blockchain Adds Trust to AI and IoT. 5 August 2020. Available online: https://www.ibm.com/blogs/blockchain/2020/08/how-blockchain-adds-trust-to-ai-and-iot/ (accessed on 17 October 2020).
52. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
53. Kshetri, N. Blockchain and electronic healthcare records [cybertrust]. *Computer* **2018**, *51*, 59–63. [CrossRef]
54. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
55. Sun, H.; Wang, X.; Wang, X. Application of blockchain technology in online education. *Int. J. Emerg. Technol. Learn.* **2018**, *13*, 252–259. [CrossRef]
56. Rimer, S. An IoT architecture for financial services in developing countries. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, 30 May–2 June 2017; pp. 1–10.
57. Dineshreddy, V.; Gangadharan, G. Towards an "Internet of Things" framework for financial services sector. In Proceedings of the 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 3–5 March 2016; pp. 177–181.
58. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain technology in finance. *Computer* **2017**, *50*, 14–17. [CrossRef]

59. Chen, Y.; Bellavitis, C. Blockchain disruption and decentralized finance: The rise of decentralized business models. *J. Bus. Ventur. Insights* **2020**, *13*, e00151. [CrossRef]
60. Khare, A.; Merlino, G.; Longo, F.; Puliafito, A.; Vyas, O.P. Design of a trustless smart city system: The# SmartME experiment. *Internet Things* **2020**, *10*, 100126.
61. Li, Y.; Ouyang, K.; Li, N.; Rahmani, R.; Yang, H.; Pei, Y. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. *Sensors* **2020**, *20*, 2483. [CrossRef]
62. Du, X.; Gao, Y.; Wu, C.-H.; Wang, R.; Bi, D. Blockchain-Based intelligent transportation: A sustainable GCU application system. *J. Adv. Transp.* **2020**, *2020*, 5036792. [CrossRef]
63. Bitcoin Is an Innovative Payment Network and a New Kind of Money. Available online: https://bitcoin.org/en/ (accessed on 30 August 2020).
64. Ethereum Is a Global, Open-Source Platform for Decentralized Applications. Available online: https://www.ethereum.org/] (accessed on 21 August 2020).
65. Multichain. Available online: https://www.multichain.com/ (accessed on 3 July 2020).
66. Samaniego, M.; Deters, R. Internet of smart things-iost: Using blockchain and clips to make things autonomous. In Proceedings of the 2017 IEEE International Conference on Cognitive Computing (ICCC), Honolulu, HI, USA, 25–30 June 2017; pp. 9–16.
67. Quorum. Available online: https://www.jpmorgan.co.jp/global/Quorum (accessed on 15 June 2020).
68. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv* **2018**, arXiv:1809.03421.
69. Lisk. Available online: https://lisk.io/ (accessed on 3 June 2020).
70. Litecoin. Available online: https://litecoin.org/ (accessed on 25 May 2020).
71. How Litecoin Works: An Introduction to the Cryptocurrency. Available online: https://www.kompulsa.com/how-litecoin-works-an-introduction-to-the-cryptocurrency (accessed on 10 May 2020).
72. HDAC Technology. Available online: https://www.hdactech.com/ (accessed on 29 April 2020).
73. Raschendorfer, A.; Mörzinger, B.; Steinberger, E.; Pelzmann, P.; Oswald, R.; Stadler, M.; Bleicher, F. On IOTA as a potential enabler for an M2M economy in manufacturing. *Procedia CIRP* **2019**, *79*, 379–384. [CrossRef]
74. Perry, K.J.; Toueg, S. Distributed agreement in the presence of processor and communication faults. *IEEE Trans. Softw. Eng.* **1986**, *3*, 477–482. [CrossRef]
75. Wen, F.; Yang, L.; Cai, W.; Zhou, P. DP-Hybrid: A Two-Layer Consensus Protocol for High Scalability in Permissioned Blockchain. In Proceedings of the International Conference on Blockchain and Trustworthy Systems, online, 6–7 August 2020; pp. 57–71.
76. Perez, D.; Xu, J.; Livshits, B. Revisiting Transactional Statistics of High-scalability Blockchains. In Proceedings of the ACM Internet Measurement Conference, Pittsburgh, PA, USA, 27–29 October 2020; pp. 535–550.
77. Veena Pureswaran, S.P.; Nair, S.; Brody, P. Empowering the Edge-Practical Insights on a Decentralized Internet of Things. Available online: https://www.ibm.com/downloads/cas/2NZLY7XJ (accessed on 8 January 2022).
78. Shah, P.; Forester, D.; Polk, D.; Berberich, M. Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies. 2019. Available online: https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf (accessed on 23 November 2020).
79. Bernabe, J.B.; Canovas, J.L.; Hernandez-Ramos, J.L.; Moreno, R.T.; Skarmeta, A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access* **2019**, *7*, 164908–164940. [CrossRef]
80. Lee, D.; Park, N. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. *Multimed. Tools Appl.* **2020**, *80*, 34517–34534. [CrossRef]
81. Shbair, W.; Steichen, M.; François, J. Blockchain orchestration and experimentation framework: A case study of KYC. In *IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium*; IEEE: Taipei, Taiwan, 2018.
82. Pahl, C.; El Ioini, N.; Helmer, S.; Lee, B. An architecture pattern for trusted orchestration in IoT edge clouds. In Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018; pp. 63–70.
83. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **2020**, *35*, E23. [CrossRef]
84. Madine, M.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Arshad, J.; Yaqoob, I. Application-Level Interoperability for Blockchain Networks. *TechRxiv* **2021**, Preprint. [CrossRef]
85. Wang, H.; Cen, Y.; Li, X. Blockchain Router: A Cross-Chain Communication Protocol. In Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, Jeju, Korea, 29–31 March 2017; pp. 94–97.
86. Latif, S.; Idrees, Z.; Ahmad, J.; Zheng, L.; Zou, Z. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *J. Ind. Inf. Integr.* **2021**, *21*, 100190. [CrossRef]
87. Wu, X.; Liang, J. A blockchain-based trust management method for Internet of Things. *Pervasive Mob. Comput.* **2021**, *72*, 101330. [CrossRef]
88. Fan, Q.; Chen, J.; Deborah, L.J.; Luo, M. A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. *J. Syst. Archit.* **2021**, *117*, 102112. [CrossRef]
89. Zhang, H.; Tong, L.; Yu, J.; Lin, J. Blockchain Aided Privacy-Preserving Outsourcing Algorithms of Bilinear Pairings for Internet of Things Devices. *arXiv* **2021**, arXiv:2101.02341. [CrossRef]

90. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [CrossRef]
91. Singh, A.P.; Pradhan, N.R.; Agnihotri, S.; Jhanjhi, N.; Verma, S.; Ghosh, U.; Roy, D. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5779–5789. [CrossRef]
92. Latif, R.M.A.; Hussain, K.; Jhanjhi, N.; Nayyar, A.; Rizwan, O. A remix IDE: Smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimed. Tools Appl.* **2020**, 1–24. [CrossRef]
93. Lin, C.; He, D.; Huang, X.; Xie, X.; Choo, K.-K.R. Blockchain-based system for secure outsourcing of bilinear pairings. *Inf. Sci.* **2020**, *527*, 590–601. [CrossRef]
94. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Blockchain leveraged decentralized IoT eHealth framework. *Internet Things* **2020**, *9*, 100159. [CrossRef]
95. Gong, X.; Liu, E.; Wang, R. Blockchain-Based IoT Application Using Smart Contracts: Case Study of M2M Autonomous Trading. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 781–785.
96. Huang, J.-C.; Shu, M.-H.; Hsu, B.-M.; Hu, C.-M. Service architecture of IoT terminal connection based on blockchain identity authentication system. *Comput. Commun.* **2020**, *160*, 411–422. [CrossRef]
97. Zhang, J.; Wang, Z.; Shang, L.; Lu, D.; Ma, J. BTNC: A blockchain based trusted network connection protocol in IoT. *J. Parallel Distrib. Comput.* **2020**, *143*, 1–16. [CrossRef]
98. Singh, S.K.; Rathore, S.; Park, J.H. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
99. Memon, R.A.; Li, J.P.; Nazeer, M.I.; Khan, A.N.; Ahmed, J. DualFog-IoT: Additional fog layer for solving blockchain integration problem in Internet of Things. *IEEE Access* **2019**, *7*, 169073–169093. [CrossRef]
100. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT information sharing security mechanism based on blockchain technology. *Future Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [CrossRef]
101. Jiang, W.; Li, H.; Xu, G.; Wen, M.; Dong, G.; Lin, X. PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI. *Future Gener. Comput. Syst.* **2019**, *96*, 185–195. [CrossRef]
102. Casado-Vara, R.; Chamoso, P.; De la Prieta, F.; Prieto, J.; Corchado, J.M. Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. *Inf. Fusion* **2019**, *49*, 227–239. [CrossRef]
103. Bruneo, D.; Distefano, S.; Giacobbe, M.; Minnolo, A.L.; Longo, F.; Merlino, G.; Mulfari, D.; Panarello, A.; Patanè, G.; Puliafito, A. An iot service ecosystem for smart cities: The# smartme project. *Internet Things* **2019**, *5*, 12–33.
104. Rathee, G.; Sharma, A.; Kumar, R.; Iqbal, R. A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Netw.* **2019**, *94*, 101933. [CrossRef]
105. Wang, X.; Yu, G.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Zheng, K.; Niu, X. Capacity of blockchain based Internet-of-Things: Testbed and analysis. *Internet Things* **2019**, *8*, 100109. [CrossRef]
106. Huang, J.; Kong, L.; Chen, G.; Wu, M.-Y.; Liu, X.; Zeng, P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
107. Biswas, S.; Sharif, K.; Li, F.; Nour, B.; Wang, Y. A scalable blockchain framework for secure transactions in IoT. *IEEE Internet Things J.* **2018**, *6*, 4650–4659. [CrossRef]
108. Pan, J.; Wang, J.; Hester, A.; Alqerm, I.; Liu, Y.; Zhao, Y. EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. *IEEE Internet Things J.* **2018**, *6*, 4719–4732. [CrossRef]
109. Novo, O. Scalable access management in IoT using blockchain: A performance evaluation. *IEEE Internet Things J.* **2018**, *6*, 4694–4701. [CrossRef]
110. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* **2018**, *72*, 266–273. [CrossRef]
111. Agrawal, R.; Verma, P.; Sonanis, R.; Goel, U.; De, A.; Kondaveeti, S.A.; Shekhar, S. Continuous security in IoT using Blockchain. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018; pp. 6423–6427.
112. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-Peer Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]
113. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
114. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
115. Sankar, L.S.; Sindhu, M.; Sethumadhavan, M. Survey of consensus protocols on blockchain applications. In Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017; pp. 1–5.
116. Dunphy, P.; Petitcolas, F.A. A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
117. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]

118. Lin, C.; He, D.; Huang, X.; Khan, M.K.; Choo, K.-K.R. A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems. *IEEE Access* **2018**, *6*, 28203–28212. [CrossRef]
119. Conti, M.; Kumar, E.S.; Lal, C.; Ruj, S. A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3416–3452. [CrossRef]
120. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
121. Lu, Y. Blockchain: A survey on functions, applications and open issues. *J. Ind. Integr. Manag.* **2018**, *3*, 1850015. [CrossRef]
122. Sun, Y.; Zhang, L.; Feng, G.; Yang, B.; Cao, B.; Imran, M.A. Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. *IEEE Internet Things J.* **2019**, *6*, 5791–5802. [CrossRef]
123. Lu, Y. Artificial intelligence: A survey on evolution, models, applications and future trends. *J. Manag. Anal.* **2019**, *6*, 1–29. [CrossRef]
124. Kan, L.; Wei, Y.; Muhammad, A.H.; Siyuan, W.; Linchao, G.; Kai, H. A multiple blockchains architecture on inter-blockchain communication. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 139–145.