computers

MDPI

Review

Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges

Tanweer Alam

Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia; tanweer03@iu.edu.sa

Abstract: Advances in technology always had an impact on our lives. Several emerging technologies, most notably the Internet of Things (IoT) and blockchain, present transformative opportunities. The blockchain is a decentralized, transparent ledger for storing transaction data. By effectively establishing trust between nodes, it has the remarkable potential to design unique architectures for most enterprise applications. When it first appeared as a platform for anonymous cryptocurrency trading, such as Bitcoin, on a public network platform, blockchain piqued the interest of researchers. The chain is completed when each block connects to the previous block. The Internet of Things (IoT) is a network of networked devices that can exchange data and be managed and controlled via unique identifiers. Automation, wireless sensor networks, embedded systems, and control systems are just a few of the well-known technologies that power the IoT. Converging advancements in real-time analytics, machine learning, commodity sensors, and embedded systems demonstrate the rapid expansion of the IoT paradigm. The Internet of Things refers to the global networking of millions of networked smart gadgets that gather and exchange data. Integrating the IoT and blockchain technology would be a significant step toward developing a reliable, secure, and comprehensive method of storing data collected by smart devices. Internet-enabled devices in the IoT can send data to private blockchain networks, creating immutable records of all transaction history. As a result, these networks produce unchangeable logs of all transactions. This research looks at how blockchain technology and the Internet of Things interact to understand better how devices can communicate with one another. The blockchain-enabled Internet of Things architecture proposed in this article is a useful framework for integrating blockchain technology and the Internet of Things using the most cutting-edge tools and methods currently available. This article discusses the principles of blockchain-based IoT, consensus methods, reviews, difficulties, prospects, applications, trends, and communication between IoT nodes in an integrated framework.

Keywords: blockchain; smart contract; Internet of Things; security and privacy; proof of work

Citation: Alam, T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. *Computers* **2023**, *12*, 6. https://doi.org/10.3390/computers12010006

Academic Editor: Sergio Correia

Received: 1 November 2022
Revised: 13 December 2022
Accepted: 20 December 2022
Published: 26 December 2022

1. Introduction

Stuart Haber and W Scott Stornetta discovered blockchain in the early 1990s [1]. Blockchain, the major Bitcoin cryptocurrency, was initially recognized in 2009. The blockchain evolved into a cryptocurrency platform. Commercial banks are the primary institutions they regard as a new price platform. However, since 2009, the blockchain aroused tremendous interest in various businesses. Consider the power of cutting in chain management, consumer procurement restrictions, and other areas to produce income with blockchain. Blockchain is a broad term for an open, unstable, public realm that allows anyone to securely transmit data using public key authentication and proof of work (PoW) because of its power-sharing traits, resilience, confidentiality, and book research abilities. Throughout the testing, the blockchain's usage was focused on its usability and speed difficulties. The authors assumed that five scientific arches were heavily used for the experiment: IEEEXplore, Springer, ACM digital library, and Scopus. After the first round was accomplished, only 150 articles were selected. After the first round, unusual papers were

deleted, and 100 papers were selected. In the third round of paper selection, only 81 papers were selected. Blockchains, by definition, rely on a public directory. The public directory acts as a common transaction information database for many sites. The ledge was released in phases, and blocks were noted in the ledger. Blockchain is made up of blocks. Blockchain time is an indestructible database that is placed in a new time transaction and divided into a block hash chain. It details many copies of such blocks that were made and saved in the extracted device's protocol. The primary purpose is to locate a donor population known as miners. Blockchain technology Minors are linked to the current blockchain generation [2]. The technique argues that a few miners can amend a risky or inaccurate transaction at any time stamp. Various blockchain frameworks are now accessible, including public, non-public, licensing, and no blockchain authorization. Thanks to the social blockchain standard, anyone can subscribe to the series. Public blockchains are often authoritative, especially when all users have equal access rights and proportions. A personal blockchain ensures anonymity. On a personal blockchain, each player's tool is predetermined. Customers do not currently have equal access and equitable rights in the community as a result of these licenses. Bitcoin is a significant and still commonly used blockchain protocol. There may be a time constraint of up to 5 min, similar to how a new miner is normally unbiased and wants the best one to contribute or install a new blockchain device. The primary question in this circumstance is who will add the transactions and how. The same gain can be reached using two methods: send proof and process verification. Consider a case in which you want to pay. The foundation explains why signing transactions validates the use of cryptographic keys. In this scenario, community service providers or miners validate the legitimacy of digital signatures and ensure asset access. When these tasks are complete, the blockchain system delivers new enhancements [3]. Each block has its hash code, which includes the hash of the previous blocks in the series. It is also used to connect blocks in a specified manner. To build network leadership, everyone involved in mining must work hard and rapidly. Internal computing solves the problem of highlighting contradicting size computations for permanent length recordings. A leader can be elected in any situation. This leader enables several miners to attempt to rectify the problems with the person who solved the problem first and offer evidence of completion to the group. Furthermore, multiple miners must guarantee that the completed designs are ready. In contrast, confirming and picking that hole. Every node uses a blockchain verification mechanism before placing something in a blockchain device. If the nodes are authenticated blocks, they receive a pow. Every new node that joins a shared blockchain device receives a copy of the blockchain. When creating a new block, send it to all blockchain nodes remotely. Each node also validates the blocking process and ensures that the data displayed are correct. If the block is validated, it is posted to the nearby blockchain. Pos has another alternative. This is another approach. This approach selects the most useful person in the network. The Pos defines the value of the pole in the network dependent on the amount of money the miner has. This presupposes that a miner with several poles is very popular in the network [4]. All nodes eagerly greet this leader by including his block in the mining block. Only the inclusion of new in-network devices should keep the blockchain current. The research question is "what are the prospects and obstacles for a blockchain-based IoT network?".

There are various survey papers accessible on the blockchain. This study investigates opportunities, demands, and trends resulting from blockchain systems' complete functioning and behaviour. A few exam papers focus on specific features of the blockchain, such as framework, smart contracts, privacy, security, compliance agreements, applications, and IoT–blockchain integration. Few studies investigate the privacy and security challenges raised by specific blockchain topologies, such as Ethereum or Bitcoin. Table 1 displays similar studies from the same study area. The author specifies the role of blockchain in IoT, challenges in communication between blockchain and IoT, and the applications. The authors examine the characteristics of the current and future blockchain generation, significant performance difficulties, and open challenges for the future.

Table 1. Related Studies.

Reference(s)	Topics	Year	Area
[5]	Peer-to-Peer Electronic Cash System	2008	Bitcoin
[6]	Blockchain as a Service for IoT	2016	Blockchain and IoT
[7]	Blockchain Technology	2016	Blockchain
[8]	Blockchain for the Internet of Things	2016	Blockchain and IoT
[9]	Blockchain for the Internet of Things	2017	Blockchain and IoT
[10]	Internet of things and Blockchain	2016	Blockchain and IoT
[11]	Security of Blockchain	2017	Blockchain Security
[12]	Analysis of Established Blockchain Systems	2017	Blockchain
[13]	Consensus algorithms of Blockchain	2017	Blockchain
[14]	blockchain research framework	2019	Blockchain
[15]	Consensus protocols on Blockchain	2017	Blockchain
[16]	Blockchain framework	2018	Blockchain
[17]	Data processing view of Blockchain systems	2018	Blockchain
[18]	Blockchain: trends and future	2018	Blockchain
[19]	Blockchain security architecture for the Internet of Things	2018	Blockchain and IoT
[20]	Blockchain and IoT integration	2018	Blockchain and IoT
[21]	Use of Blockchain for the Internet of Things	2018	Blockchain and IoT
[22]	Blockchain meets IoT	2018	Blockchain and IoT
[23]	Blockchain technologies for the Internet of things	2018	Blockchain and IoT
[24]	The blockchain-empowered software system	2018	Blockchain
[25]	Distributed ledger technologies	2018	Blockchain
[26]	Blockchain Transactions	2018	Blockchain
[27]	Blockchain: Challenges and applications	2018	Blockchain
[28]	Blockchain applications in different domains	2020	Blockchain
[29]	Blockchain in developing countries	2018	Blockchain
[30]	Blockchain and its Role in the Internet of Things	2019	Blockchain and IoT
[31]	Blockchain applications in supply chain	2019	Blockchain
[32]	Privacy protection in blockchain system	2019	Blockchain
[33]	Blockchain in industries	2019	Blockchain
[34]	Blockchain for Internet of things	2019	Blockchain and IoT
[35]	Evolution of Blockchain	2019	Blockchain
[36]	Blockchain-based IoT	2019	Blockchain and IoT
[37]	Blockchain Technology	2019	Blockchain
[38]	Security Issues in IoT for Blockchain Healthcare	2019	Blockchain and IoT
[39]	Security issues and blockchain solutions for IoT	2020	Blockchain and IoT
[40]	Scalability of Blockchain Systems	2019	Blockchain
[41]	Security and privacy on the Blockchain	2019	Blockchain
[42]	Blockchain Applications for Industry 4.0	2019	Blockchain
[43]	Transformative effects of IoT, Blockchain and Artificial Intelligence	2019	Blockchain and IoT

Table 1. *Cont.*

Reference(s)	Topics	Year	Area
[44]	Efficiency Issues and Solutions in Blockchain	2019	Blockchain
[45]	Blockchain-based security aspects in heterogeneous Internet-of-Things	2018	Blockchain and IoT
[46]	Consensus Algorithms in Blockchain Technology	2019	Blockchain
[47]	Determining blockchain applicability	2018	Blockchain
[48]	Blockchain Applications in IoT Systems	2019	Blockchain and IoT
[49]	Aspects of Blockchain and IoT	2019	Blockchain and IoT
[50]	Blockchain characteristics and consensus	2019	Blockchain
[51]	Survey of Blockchain-Enabled Cyber-Physical Systems	2020	Cyber-Physical Systems
[52]	IoT Applications in Blockchain Systems	2020	Blockchain and IoT
[53]	Blockchain, Fog and IoT Integrated Framework	2020	Blockchain and IoT
[54]	Blockchain consensus algorithms performance evaluation	2020	Blockchain
[55]	Blockchain for 5G-enabled IoT	2020	Blockchain and IoT
[56]	Blockchain smart contracts formalization	2020	Blockchain
[57]	Blockchain for Cybersecurity in IoT	2021	Blockchain and IoT
[58]	Integration of Blockchain and Internet of Things: challenges and solutions.	2021	Blockchain and IoT
[59]	A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges	2022	Blockchain and IoT

The authors also described blockchain policy terms and changes to blockchain-related organizations. A scientific study is intended to reveal a target audience's range of behaviours and attitudes about important issues and concerns. The outcomes of qualitative research are explanatory rather than predictive. All information gathered consists of words written and uttered by people and their observed behaviours. In-depth interviews are a qualitative research approach used by researchers to collect data to acquire a more profound knowledge of the interviewee's perspective and situation. Such an interview strategy involves asking participants open-ended and screening questions to receive information that the researcher finds worthwhile. This article carefully explores how BC can benefit from the Internet of Things. The primary goal of this research is to analyze recent trends in BC-related approaches and tool usage analysis in an IoT environment. Compared to previous studies, this paper explores the novel roles of BC in IoT, finds new opportunities in various areas, for example, in the COVID-19 situation, and explores the challenges. Additionally, it shows the reader how far along numerous proposed solutions are in their advancement. We also discuss the main open questions, future research directions in the field, and the challenges the research community must overcome to integrate BC and IoT successfully.

This paper describes how blockchain technology can be applied to Internet of Things contexts to solve problems that arise. The following are some of the key contributions made by this study:

1. The paper begins with a brief introduction to the Internet of Things and blockchain. On the other side, this study reveals the numerous challenges experienced by researchers while exploring the Internet of Things.
2. This study highlights the importance of smart contracts in the Internet of Things environment.

3. Method of data storage and management, big data, cloud computing, and network security management technique are the three primary groups into which we categorize and investigate the available solutions in depth.
4. In the form of a table, we compare the categories of the offered solutions in terms of used technology, potential solutions, and implementation notes.
5. This paper covers unanswered research topics and our findings that may be applicable to the development of blockchain-based IoT systems, based on a review.

The following is how the rest of the article is organized. The authors present the broad structure and growing technology components of blockchain, including a distributed ledger, cryptography, consensus protocols, smart contracts, and standards, in Section 2. Section 3 depicts the consensus algorithms, Section 4 depicts the blockchain layered architecture, Section 5 defines current blockchain development trends, Section 6 depicts the role of blockchain in the IoT, Section 7 depicts communication among IoT nodes in the IoT–blockchain framework, Section 8 depicts challenges, and Section 9 depicts blockchain applications.

2. Blockchain

The blockchain is a public digital ledger constructed on a peer-to-peer network that may be openly distributed across varied users to generate an immutable history of timestamped and connected transactions [60]. When a group of transactions is appended, the data creates a new block in the chain. Simply put, a blockchain is a timestamped set of unchangeable data records attempted by a group of machines that a single party does not control. Each data block is encrypted and linked to the next in a chain using cryptography standards. Without relying on a centralized system, untrustworthy entities with common interests can utilize blockchain to construct a reliable, unchangeable, and open history of trading and distribution [61,62]. The numerous elements of blockchain and its reliance on encryption and distributed systems may allow for a more complex understanding.

Furthermore, each part may be clearly defined and used as a building brick to comprehend the greater complex structure. Blockchain technology can be characterized as public or private [63]. Anyone can connect to the blockchain network using the public blockchain. By confirming transactions and delivering correct services, all users contribute to the public blockchain. Public blockchains are the most extensively utilized cryptocurrencies today. Only authorized users have access to the private blockchain. The owner of the private blockchain can modify or remove entities from the blockchain network. A variety of corporate paradigms recommended the use of private blockchains. The blockchain is a distributed electronic database of digitally signed transactions that are clustered into chain blocks [13]. Each block is cryptographically connected to the preceding records after verification and consensus. When a new block is installed, reconfiguring earlier blocks is much more challenging. The new blocks are duplicated across all system copies of the ledger, and any conflicts are addressed instantly using current rules. The blockchain methods utilized to transmit data between devices are depicted in Figure 1.

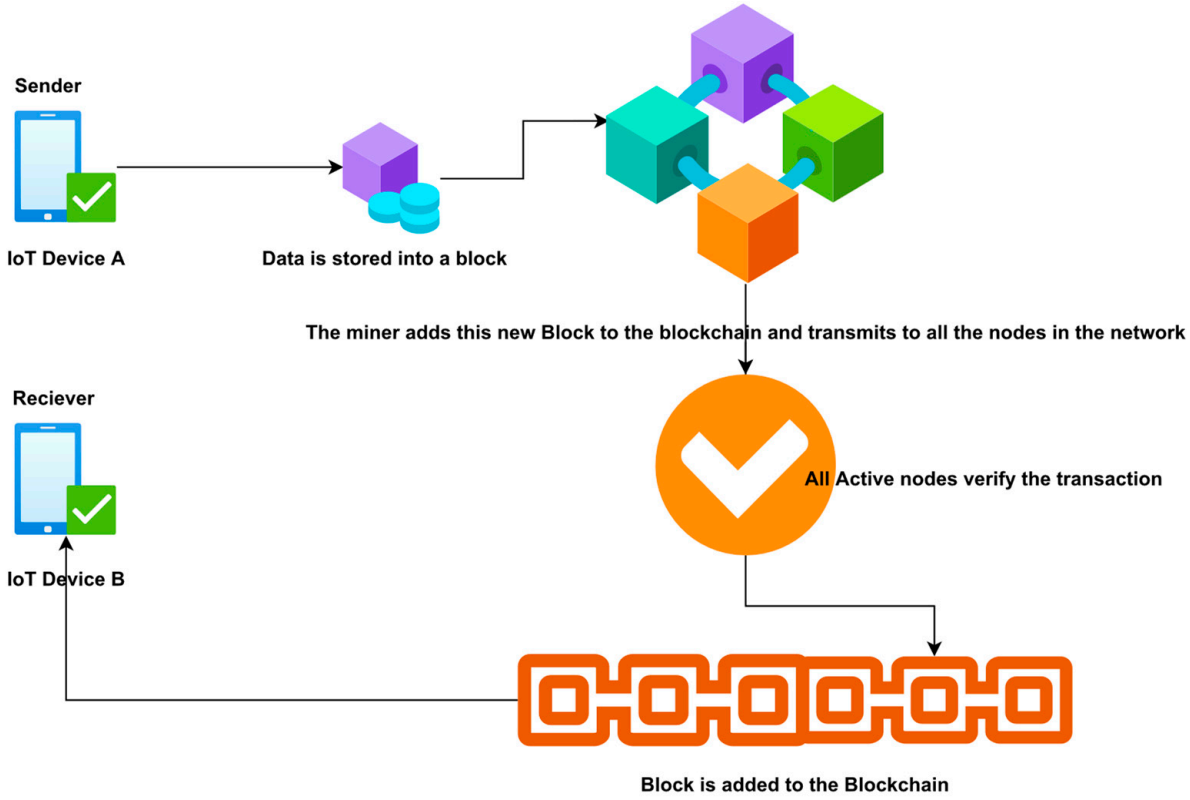

Figure 1. Blockchain process to send data between devices.

2.1. Components of Blockchain

The following are blockchain add-ons.

2.1.1. Block

A block is an information structure used to deceive a transaction group sent to all public nodes.

2.1.2. Nodes

Nodes for devices or users in the blockchain community.

2.1.3. Transactions

Transactions are the tiniest components of the blockchain framework design.

2.1.4. Miners

A miner is a particular node that executes a block authentication method on a blockchain network.

2.1.5. Chain

A chain is a sequence of blocks.

2.1.6. Consistency

Consistency refers to highly complex and fast rules that can be used to carry out blockchain operations when processing transactions. The blockchain can be represented as a collection of linked blocks. Before Bitcoin, it was known as digital ledgers in general. The blockchain is an actively distributed system that prioritizes data integrity, transparency, security, shareability and other features. To distribute processes across various locations, blockchain uses a distributed platform, often a peer-to-peer (P2P) system [64]. A consensus approach could be utilized to synchronize the saved and data gathered from each node [65].

Two prominent communication protocols are Gossip and Kademlia. Messages are sent over many endpoints to support these protocols. Gossip is the most widely used protocol in Bitcoin, and it is used to send data to the whole network, with each node only talking with its neighbours. Kademlia, on the other hand, defines the network structure using a shared hash table, and the peer list includes each node interaction.

2.2. Blockchain Versions

Table 2 depicts the evolution and versioning of blockchain technology from 1.0 to 4.0. With its first use (Bitcoin), blockchain 1.0 was introduced for distributed ledger technologies. Blockchain 2.0 introduced smart contracts, short computer programs that run automatically with verifications. Decentralized storage communication on peer-to-peer networks is possible with blockchain 3.0. Blockchain 4.0 enabled enterprises to access blockchain technology, allowing them to be employed in Industry 4.0. The current blockchain versions are listed in Table 2.

Table 2. Blockchain versions.

Year	Version	Application	Algorithms	Chaining	Execution Framework	Other Features
2008	1.0	Currency	PoW	Metachain	Bitcoin	Transparency, authentication, zminimize cost.
2013	2.0	Smart Contracts	PoW, PoS	Metachain	Ethereum	Distributed computations, Exchange the digital currencies
2015	3.0	Decentralized Apps	PoW, PoS, PoET, PBFT, etc.	A directed graph, Metachain, and sidechain.	Ethereum Swarm	Decentralized storage and communication
2018	4.0	Industry 4.0 Apps	Artificial intelligence-based Consensus	Connected chain, Divided chain	unibright.io framework	Approved workflows, financial transactions, IoT data gathering, e-health management system, etc.

2.3. Blockchain Terminologies

Blockchain terminologies vary from execution to execution—generic phrases would be utilized to communicate about the present invention. Some terminologies are defined below.

2.3.1. Blockchain

It is a distributed digital ledger.

2.3.2. Blockchain Technology

This term describes the innovation in the most generic version.

2.3.3. Blockchain Network

This term describes the network where a blockchain will be applied. It demonstrates blockchain implementation.

2.3.4. Blockchain Network User

This term describes an organization, individual, company, administration, and many others using the blockchain network system.

2.3.5. Node

A node is an individual device in the blockchain system.

2.4. Blocks in a Blockchain

Blockchain network users send transactions to the blockchain system through computer apps, smart device apps, digital wallets, web services, and other means. The apps route such transactions to a node or nodes within the blockchain system. These entire nodes could be published or unpublished. A submitted transaction would then be disseminated to other nodes in the network. However, they cannot find the transaction in the blockchain community. Because of the nature of many blockchain systems, non-time transactions must wait in a queue until a publishing node sends them to the blockchain network. Figure 2 illustrates the blockchain's blocks.

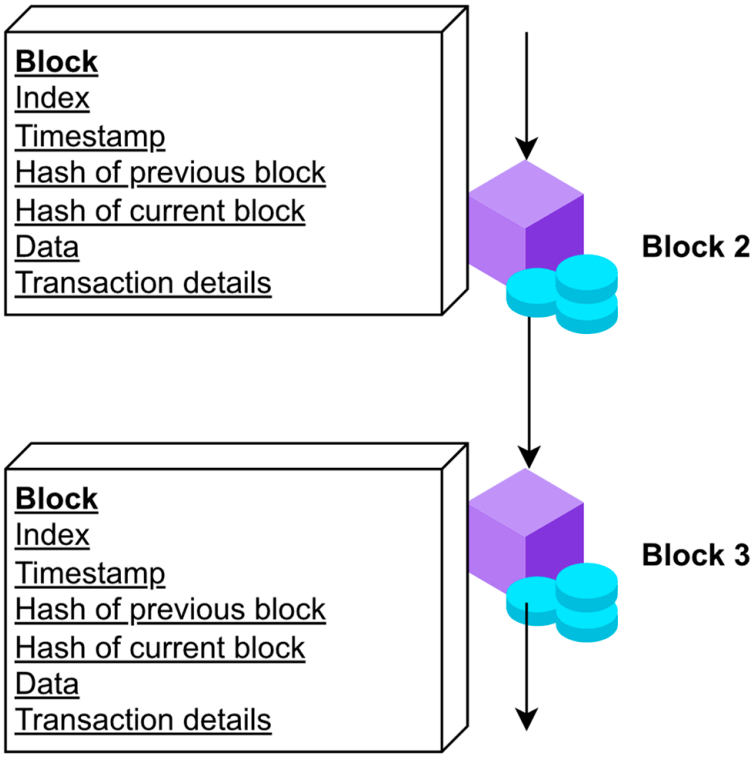

Figure 2. Blocks in blockchain.

A blockchain block might include both a header and information. This header consists of the metadata for the block. The data consists of a list of correct and confirmed transactions published in the blockchain system. Accuracy and validity are ensured by ensuring that the transaction is accurately configured and that the distributed ledger services cryptographically signed each transaction. In the blockchain implementation, there are no standard data fields for a block. They can describe their data fields in a block. However, data fields are used in a variety of blockchain implementations.

2.4.1. Block Header

In some blockchain networks, a block number is also referred to as a block height.

2.4.2. Hash Code

The hash code of the previous block pass. A hash description of the block information (this might be accomplished using a variety of approaches, such as creating a Merkle tree, processing the root hash, or utilizing a hash of all the combination block information).

2.4.3. Timestamp

A method for authenticating data and associating electronic files or events with a particular instant in time is known as timestamping, which is based on blockchain technology. A timestamp is a string of letters that serves as a unique identifier for the

document or event in consideration and the time it was formed. In the most basic form, the timestamp is a string of letters.

2.4.4. Block Size

A nonce is something that is utilized for mining and is controlled by the publishing node to solve the hash puzzle.

Figure 3 depicts the process of connecting one block to two others, a previous and the following one, which validates the chain architecture of a blockchain. However, the question is, where does that chain begin, and where does it end? The solution is that the initial block, known as the genesis block, is hardcoded into the source code. This has a hash reference with only zeros and is the first block in the chain. It also contains certain arbitrary information that can be identified within its coin base transaction. The following is the block information:

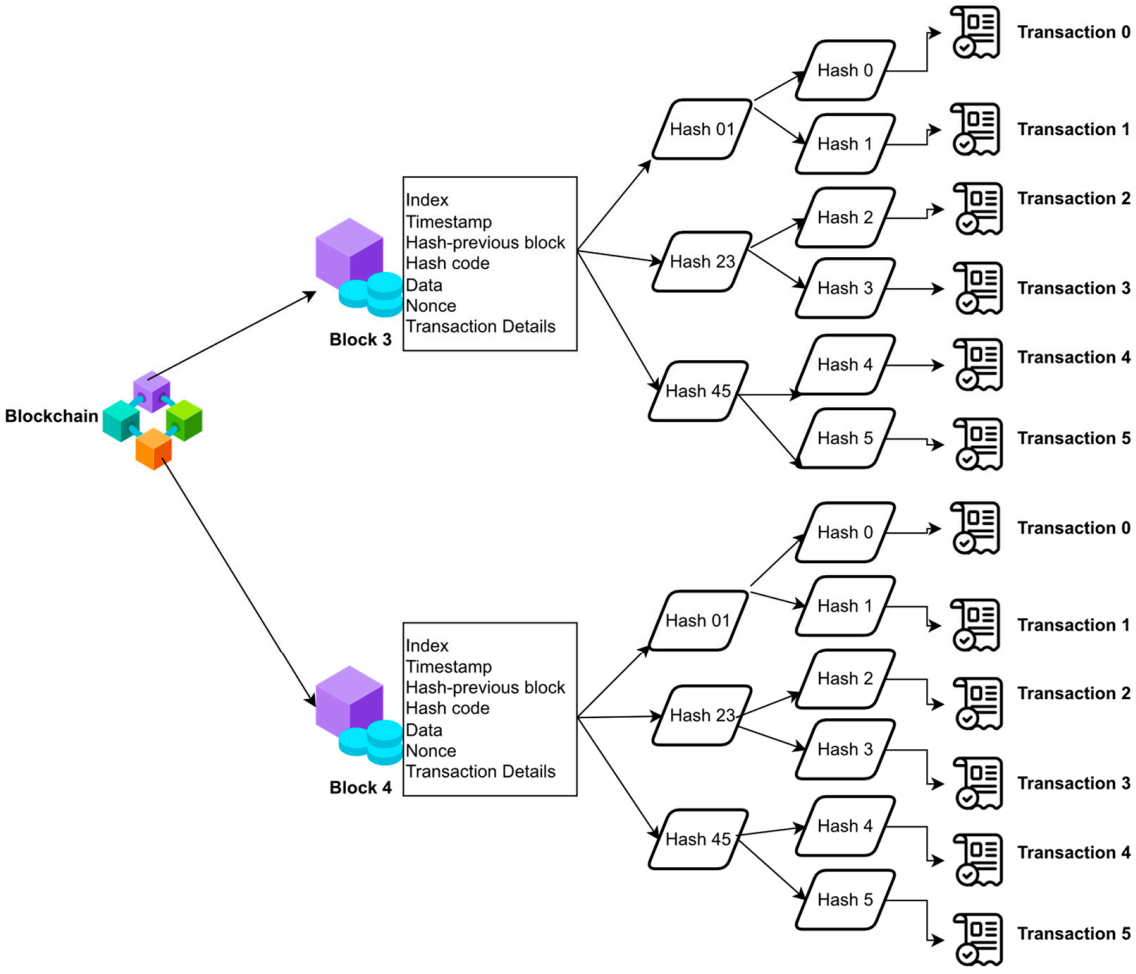

Figure 3. Blockchain structure.

2.4.5. Data

The information in the block.

2.4.6. The Ledger Transactions and Events

This section may include further information.

2.5. Transactions

A transaction is an activity that occurs between nodes. It depicts the exchange of digital currency between blockchain network nodes. In business-to-business contexts, it could be

a method of recording activities involving digital or physical assets. In a blockchain, each block may contain zero or more transactions.

2.6. Digital Signature

A digital signature is a computational procedure that is used to authenticate digital information, such as a code. The accurate digital signature ensures the receiver that the data were unquestionably generated by a known entity and was not changed during transmission (un-repudiation) [66]. The digital signature technique is based on an algorithm that generates a private key with a secure, consistent distribution from a big enough pool of possible private keys so that multiple copies are not obtained. It enables different identities to be assigned to each individual. Then it employs an asymmetric cryptographic approach to determine the appropriate public key. Each component is an algorithm that generates a digital signature and a relevant message from a private key. The digital signature operations are depicted in Figure 4.

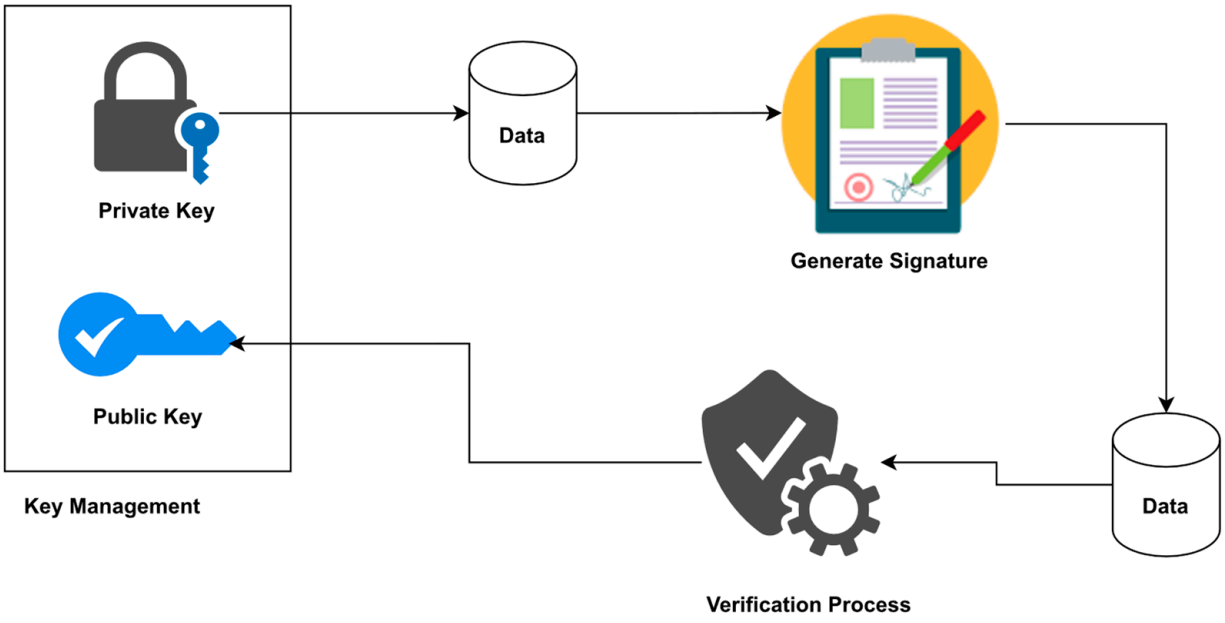

Figure 4. Digital signature process.

2.7. Sharding

The practice of splitting files in the blockchain storage process is known as sharding. Every shard is replicated to prevent data loss in the event of a communication problem. These files are encrypted with a key, making it hard for other nodes in the network to access them. These shards are globally shared via dispersed networks [67]. Nodes must be registered in the blockchain ledger in order for the blockchain network to validate and transport transactions across networks. The blockchain storage is designed to save these links forever and cannot be altered.

2.8. Smart Contracts

The smart contract is a method that is stored on the public ledger and dynamically executed while defined terms of service are met. These services carry out the developers' instructions at the most basic level. Its benefits are evident in corporate partnerships, where they are typically used to handle contracts, and all parties can be satisfied with the conclusion with the help of an intermediary [68]. The smart contract method is depicted in Figure 5.

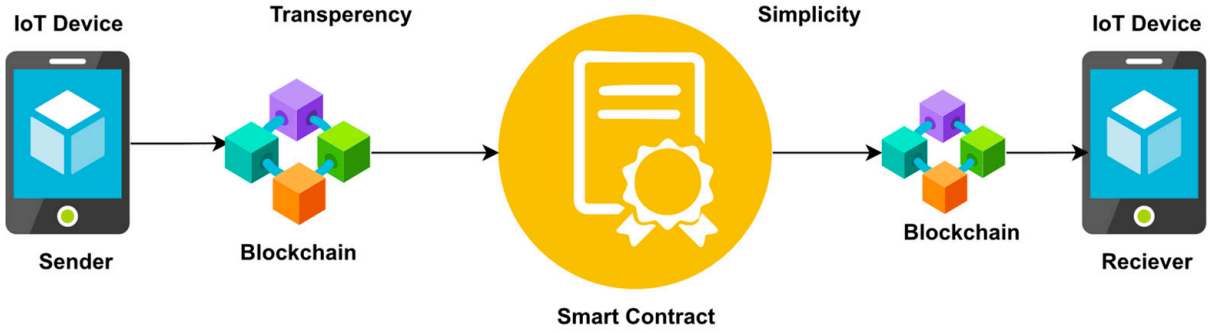

Figure 5. Smart contract.

2.9. Merkle Tree

The Merkle tree is extremely important since it was designed for blockchain. This binary hashing tree uses the SHA-256 cryptographic algorithm to encrypt the transactions and provide a list of all the transactions in the block. For instance, consider a case where the hashing value starts with "000000".

The hashing starts with "000000" in SHA-256("blockchain" + nonce).

The nonce and hashing can be combined in blockchain. A nonce can only be a numeric value. Here are some examples of measurements:

1. SHA-256("blockchain0") = 0xjhh323hhg4h43434hg4hg444j4j4j4j4ko4o4p4mh4g4hh4 d6t5l7of0g9e1
2. SHA-256("blockchain1") = 0x2hkjhfg987gjh5j3hgf98h7g5f0j0k0401hei9h0j0j6g4c4b4n 4n1m1m2f5k6a0 . . .
3. SHA-256("blockchain70346529") = 0x000000j4k3ls8n9m0h0j1k29l4hj7k9e0u0j0a0a 0387a0r8h0k4l1k3b5tt

Examples 1 and 2 are unsolvable. However, example 3 is solvable because the hashing starts with "000000".

A Merkle tree can be used to construct transaction blocks. It will, however, reduce node involvement with low computing power.

Assume A and B are two separate transactions. The hashing can be calculated using the formula below.

$$\text{SHA-256(SHA-256(A))} = \text{Hash (A)}.$$

$$\text{SHA-256(SHA-256 Hash(A) + Hash(B))} = \text{Hash (A B)}.$$

The Merkle tree is constructed from the ground up. Initially, the transactions within the leaves are hashed. The related leaf nodes are hashed into a parental node, and so forward until only one hashing remains, known as the Merkle root.

2.10. Hashing

Hashing is a mechanism for converting letter and digit data into a fixed-length encrypted response. The hashing is produced by an algorithm and is required for cryptocurrency chain operations.

3. Consensus Algorithms

The consensus algorithms are intended to offer redundancy for the device's many unstable constituents. The next block in a blockchain will almost certainly be the most accurate version of the truth. It keeps fair events from undermining the community, while also efficiently developing the chain. The most common consensus algorithms are proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), ripple, practical byzantine fault tolerance (PBFT), and delegated byzantine fault tolerance (DBFT). Based on numerous scenarios, Table 2 describes the operation and functionality of the consensus algorithms.

3.1. Proof of Work (PoW)

PoW is the most common mechanism used for cryptocurrencies such as Bitcoin and Ethereum. Before proceeding, for non-technical users, the hashing method would be a way that may be used to assign random-sized material to fixed-size content. Whether a hash function is secure or not, its performance is random.

3.2. Proof of Stake (PoS)

Because the PoS does not allow devices to perform repeated processing, it is more environmentally sustainable. It replaces miners with verifiers, who can keep a portion of the Bitcoins as a stake. The team of verifiers takes turns suggesting and participating in the next block, and the stakes' quality determines the strength of each validator's voting. When the validators discover a block that they believe can be added to the blockchain, they can verify it by placing a bet on it as well. That validator would be given credit for their stakes. Everyone who maintains a cryptocurrency blockchain foundation can become a validator by submitting a specific type of operation to safeguard it. The following are some of the benefits of PoS.

(1) Altitude: allows for faster transactions.
(2) Efficiency: uses less power.
(3) Less equipment: no need for a supercomputer.

Its downside is vulnerability: anyone with enough money to invest exclusively in the destruction of this device might accomplish it by spending only money, as opposed to PoW, where they would have to spend money, time, skills, and so on.

3.3. Delegated Proof of Stake (DPoS)

Because delegated proof of stake (DPoS) and conventional PoS differ slightly, the gap between direct democracy and representative democracy can be compared. Any account containing Bitcoins is eligible to stake in a standard PoS system. People can vote on verifying activities, reach a shared consensus, and receive coins in exchange. Each wallet containing tokens is eligible to vote for representatives throughout the DPoS scheme [69].

3.4. Leased Proof of Stake (LPoS)

This method is an upgraded version of the stake consensus algorithm, which seeks to generate a decentralized consensus to secure the blockchain platform. This approach enabled regular people with no technical skills to contribute to the security of the Waves system by leasing Waves to complete peers without losing ownership of the keys. Meanwhile, the Waves blockchain enabled performance with access to 100 TPS, which is a completely different scenario than other blockchain technologies. Expenses are modest, and there is no need to provide miners with node incentives to compensate for high energy expenses and expensive equipment.

3.5. Proof of Elapsed Time (PoET)

Every participant will be given a network-authorized timing entity that will wait for the time provided by the timestamp. Instead, each participant obtains and sends a certification proving that the system stopped the remainder of the system. This network tests how frequently the participant is a member in order to determine the members. Every member of the blockchain system will delay for a set amount of time. The first member to complete the time restriction will become a participant in the newly created block. Each new member must gain access to the blockchain joining system; once activated, the policy will produce a new key pair, which the member will present to the entire network as part of a request to participate.

3.6. Practical Byzantine Fault Tolerance (PBFT)

This algorithm vastly improves aspects of Byzantine fault tolerance (in several terms, security towards Byzantine faults). It was already implemented in some significant decentralized computer networks and certain blockchain networks. The PoET stochastic selects a specific peer group to perform demands at a given moment. Typical observers must test a uniformly distributing random function and wait for the experiment's specified period. Its shortest test peers outperform it. Deception is avoided by using a secure implementation system, identification authentication, blocklisting centred on asymmetric key encryption, and a comprehensive set of laws.

3.7. Delegated Byzantine Fault Tolerance (DBFT)

This algorithm is utilized to get a consensus, which disappoints some blockchain and cryptocurrency developers. Delegated Byzantine fault tolerance is more efficient than most other methods in dealing with unstable or insecure blockchain participants.

3.8. Direct Acyclic Graph (DAG)

This is a topologically organized directed graph data model. Its series could only occur before and after. It is also used for data analysis, organization, choosing the best routing technique, and information decoding.

3.9. Proof of Activity (PoA)

This is referred to as a blockchain consensus algorithm that verifies that transactions are valid and that miners achieve an agreement. The PoA mixes PoW and PoS and attempts to bring the most powerful of either. Throughout POA, the refining process begins as a standard PoW mechanism, with multiple miners competing with a great computational capacity to surpass one another to find a new element. When a new (extracted) block is recognized, the device switches to POS, with the newly identified block consisting of the head and data.

3.10. Proof of Importance (PoI)

This became one of the most significant breakthroughs in blockchain-based businesses. This innovative approach employs system theory to assign a value to the channel for each consideration. Several additional blockchains assign incentives using proof of work (POW) or proof of stake (POS). Anyone who can maintain the most reliable connection arrays has an advantage over many other customers when it comes to POW. Such POW buildings frequently generate excessive amounts of power, harm the environment, and burden mining firms with high electricity bills. This gives card hoarders an unfair advantage. The more coins they use in transactions, the more money they receive.

3.11. Proof of Capacity (PoC)

Blockchain miners employ software backups rather than the more common power-efficient proof of work (PoW) technique, which combines continuous computer activity. The transaction system is protected throughout the proof of work method by performing an absurd amount of processing per moment to verify every block. That is why you must employ hardware. It usually results in negatives, such as increased electricity usage, temperature, loud noises, the requirement for modern semi-reusable equipment, and huge enterprises' centralization of the refining process.

3.12. Proof of Burn (PoB)

This algorithm is more attainable than others. It reduces energy consumption. There is no need to mine the hardware equipment in this algorithm. The coin burns are essentially virtual mining equipment. The PoB algorithm allows miner nodes to make long-term commitments with other nodes in the network. In this algorithm, the supply or extraction of coins looks to grow less centralized.

3.13. Proof of Weight (PoWeight)

This blockchain consensus mechanism assigns them a 'weight' based on the amount of digital currency they own. Consumers of PoWeight play an important role in the consensus mechanism. Each consumer is assigned a "weight" based on the relevance chosen to serve the customer's commitment to the system. It safeguards against double spending and other wrongdoing on the blockchain. The high proportion of the weighted portion must pose a risk to fair customers. The number of coins determines the likelihood of PoS at risk linked to the rest of the system. PoWeight, on the other hand, might employ different weighted standards to evaluate the possibilities.

4. Blockchain–IoT Layered Architecture

The blockchain comprises numerous components that perform various functions, such as processing transactions, propagating blocks, mining, finding approval, and storing the ledger for its related coins. The blockchain contains several levels similar to the well-known TCP/IP infrastructure. These elements could be classified based on their characteristics. There are still various concepts for creating a blockchain network with a tiered design. The blockchain layered architecture is depicted in Figure 6.

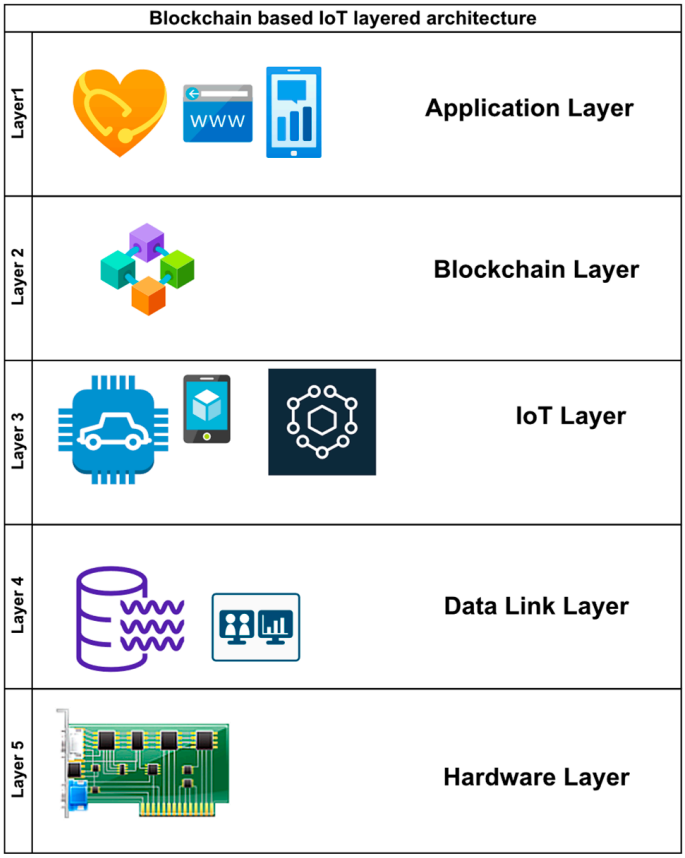

Figure 6. Blockchain layered architecture.

4.1. Application Layer

This layer includes smart contracts, chain code, and blockchain applications. This layer is divided into two sections: application and execution. In the blockchain system, end users use the applications to communicate and share information. Software, Web applications, user interfaces, and protocols are all included. For such applications, the blockchain system serves as the back-end infrastructure. These apps, however, frequently interact with the blockchain system via interfaces. The second tier is the implementation level, which includes smart contracts, basic rules, and a hybrid ledger. It follows strict coding and execution standards [70,71]. The smart contract was created in Solidity and will

be executed on Ethereum's runtime platform. To show that coding requires the use of a compiler. The bytecode becomes shorter as it is compiled. As a result, it outperforms on Ethereum. The Ethereum software is isolated from the network and file system.

4.2. Blockchain Layer

Consensus is the most fundamental and necessary level of any blockchain. A consensus mechanism creates a proven collection of entity commitments in a decentralized P2P system. According to the consensus, most of the nodes are precisely aligned. The consensus mechanisms vary depending on the type of blockchain. The consensus mechanism is defined as deterministic if preceded by an unregulated blockchain network, such as Ethereum, Bitcoin, and so on. Although there is a danger that different parties may have different viewpoints on a block in the blockchains, consensus ensures the accuracy of the ledger. Deterministic approaches are used by permitted blockchains, such as Hyperledger. Unique nodes, known as ordered endpoints, exist on specific blockchain platforms.

4.3. Network Layer

This layer is accountable for transaction discovery and block distribution in the IoT environment. This means that nodes will discover each other and will be able to connect, share, and transfer data to better the blockchain system's existing position. The P2P platform is a network in which devices are shared and system loads are redistributed. Endpoints execute blockchain transactions. Full nodes and light nodes are the two types of nodes. Full nodes provide exchange verification, authentication, processing, and compliance with consensus laws. These nodes are in charge of ensuring the system's trust. The light node can convey the blockchain's header and submit operations.

4.4. Data Link Layer

The data structure of the blockchain could be regarded as a link list of blocks where transactions are structured. Merkle's tree is a hash code binary tree. All blocks contain a hash of Merkle's root and information, such as the hashing of the previous block, timestamp, nonce, block versions, and the most recent complexity level. Merkle trees, cryptography, and consensus mechanisms are the foundation for distributed ledger technology. The root hashing might be applied to the entire tree network. Every block lists multiple transactions that occurred since the previous transaction, and when those transactions are submitted, the root hashing indicates the current state of the blockchain.

4.5. Hardware Layer

Blockchains could be used to structurally measure, verify, and store transactions in a distributed database. This database contains all important information, transactions, and facts. A P2P system considers every computer to be an endpoint. Endpoints confirm transactions, organize them into blocks, upload them to the blockchain system, and so on. Nodes add blocks to the blockchain system and upgrade the public ledger replica after reaching an agreement. A virtualized layer is used to create such a layer. Substantially, the nodes are at the centre of this layer. A computer is referred to as a node when it is connected to a blockchain system. These nodes are part of a decentralized and distributed blockchain system.

5. Roles of Blockchain in IoT

Privacy and security in IoT device communication gained much attention between 2018 and 2022. Many papers will be published between 2018 and 2022 [72–76]. In 1990, Stuart The authors published an essay on sharing a record with privacy without storing any information on timestamping services. The blockchain concept originated with, although Satoshi Nakamoto provided the first blockchains in 2008. The author gave a document in which the blocks were joined to construct a blockchain in a certain order. The IoT chain is proposed by for data authentication between two nodes in IoT networks. In addition, they

developed a set of guidelines for altering records in IoT and blockchain technology. The authors' goal is to secure the authorization component of the IoT chain device. The item researched the cloud and manet infrastructure to connect intelligent gadgets in the IoT and provide security and authentication during verbal transmission. It represents a suitable framework known as the net cloud framework, which could be useful for facilitating communication with IoT-based intelligent devices. It proposes a cloud-manet middleware system for accessing various IoT node records. The project also suggests ways to combine blockchains and the IoT. They also provide security within the blockchain–IoT to construct IoT apps using blockchain capability. The IoT enables connected physiological things in a heterogeneous system to modify their records. The Internet of Things would be divided into the following components.

5.1. Physical Things

The Internet of Things provides a unique identity for each related thing within the network device. IoT devices can exchange data with one another.

5.2. Gateways

Gateways are devices that function between physical objects and the cloud to guarantee the connection is secure and the network device is protected.

5.3. Networking

This is used to control the glide of statistics and determine the shortest path for various IoT devices.

5.4. Cloud

The cloud is used to store and compute records.

5.5. Storage

Blockchain is a collection of demonstrated and encrypted blocks of transactions stored on a network device. The records of blocks are recorded in a virtual ledger that is publicly shared, distributed, and open. Blockchain enables secure communication within the IoT community device. With extraordinary qualities, blockchain might be personal, public, or consortia.

5.6. Blockchain Ledgers

A decentralized trust model, excessive protection, extremely publicly accessible, privacy ranging from low to high, and transferable identities are all properties of blockchain ledgers [77,78]. The properties are centralized versions with low trust and public access. Privateness is an excessive and non-transferable acknowledgement. As a result, blockchain is more advanced than centralized storage systems.

5.7. Blockchains

Blockchains are a technological development that secures transactions between IoT devices. It enables decentralization, dissemination, and public peer-to-peer storage of sections of data stored or validated in an IoT network. The information recorded in the blockchain is quickly handled in a peer-to-peer setting. Blockchains are a technology that allows IoT devices to alter transactions in the blockchain device. The following summarizes blockchain's function in IoT.

5.8. Smart-Route Control Algorithm (s-RCA)

The s-RCA finds the optimal route for data traffic between a source and a destination, minimizing the total number of hops and the total amount of time it takes to transfer that data. This reliable connection can be used in medical procedures to guarantee that all instructions are received promptly and carried out without delay. This idea can enhance

m-QoS for surgical procedures performed at a distance with the help of trusted paths. The new s-RCA can be integrated into an existing routing protocol to keep tabs on the primary path and track emergency packets stored in node buffers for immediate forwarding via the demand path [79].

5.9. Decentralized Framework

Both IoT and blockchain will be utilized in this framework. A structure such as this eliminates the need for a centralized approach and even allows for a decentralized design. It increases the likelihood of the cumulative control unit failing or performing poorly. The use of blockchain firmly established decentralization. A data offloading algorithm is also being developed to distribute various processing and computing tasks to OpenFlow switches based on their current load. A traffic model is also recommended for modelling and analyzing traffic in different network nodes. The proposed algorithm is evaluated using both a testbed and a simulation. The experimental results show that the proposed framework performs better regarding latency and resource consumption.

5.10. Exchanges between Nodes in Blockchains

Exchanges between nodes in blockchains are always secure. It is a novel way to achieve relationship security. Blockchains allow IoT devices to connect with one another more efficiently.

5.11. Identification

In the IoT, all connected devices are uniquely recognized using a cryptographic hash. Each block is also clearly labelled. As a result, blockchain is a powerful innovation that gives known facts that can be processed across the database.

5.12. Consistency

The blockchain database of nodes effectively acquired information scattered across the database. The data were correct when the miners double-checked it before entering it into the blockchain. Only validated blocks may enter the blockchain.

5.13. Autonomous

Every IoT device can communicate with any other device in a network via a distributed architecture.

5.14. Optimistic

IoT devices could interact with high availability, a decentralized intelligent network communicating with the target device in real-time, or transaction data.

6. Communication among IoT Nodes in an IoT Blockchain Framework

IoT blockchains evolved into a new ledger incorporating IoT users' utilized, used, public, and real-time performance. The blockchain is organized in blocks, and each block is linked to the blocks that came before it to form a chain. Every block contains a cryptographically secure token, a front hash block, and metadata. Blockchain transactions are basic gadgets used to send data between IoT-based devices. Nodes are various kinds of physical objects.

On the other hand, smart gadgets have embedded sensors, actuators, and packaging, and can interface with other IoT devices. Its role in the IoT is to offer secure system records to IoT devices. It is a luxury that may be publicly utilized and accepted by the public. The IoT requires this time to facilitate secure communication between IoT nodes in a heterogeneous machine. Anyone with authenticated communication within the IoT platform can track and monitor blockchain transactions. The IoT blockchain can increase chat security and authentication. Throughout this work, the author investigated this technique, its possibilities and situations that require assistance, and its thoughts.

6.1. Peer-to-Peer Network

Peers are computer systems linked to one another via the internet network in the peer-to-peer (P2P) ecosystem. Without a central system, documents could be shared instantly among devices on the platform. Any device connected to the P2P platform will function as a storage server and computer. The primary goal of P2P systems would be to communicate information and assist linked devices in interacting efficiently and effectively, gaining access to critical services, or performing specified duties. P2P is a network resource exchange protocol used to trade network resources, such as compute power, networking capacity, and data storage capacity. However, the most common use case for P2P networking is file sharing via a network. Peer-to-peer networks are ideal for file sharing because they allow connected devices to receive and transmit files simultaneously. Sensor nodes with P2P networking could play an essential role in the IoT system. A lightweight encryption technique is required for IoT sensor nodes.

Blockchains offer an efficient solution to a P2P communication network problem. This technology enables the creation of a shared electronic transaction ledger distributed among device peers rather than centralized. Users are linked to blockchains to track activity. This system employs cryptography to verify and recognize the participants' peers, allowing them to attach actions to the database cryptographically. Transactions are vetted and checked by specific nodes in the process, eliminating the need for a central system. This approach might be easily applied to IoT platforms to overcome the scale issue, allowing millions of devices to use the same infrastructure without requiring professional help. Blockchains also address the issue of authority conflicts among manufacturers by establishing a standard in which everyone has equal rights and privileges.

6.2. IoT-Blockchain Integration

Each IoT tool acts as a blockchain node, capable of generating transactions, sharing them to form a block as a miner, and acting as a more straightforward transaction validation node to establish a blockchain subgroup and confirm exchanges to apply a simplified change validation approach. In spite of the limited resources available, the integration of blockchain protocols into IoT devices is being carried out. Keeping and validating a large volume of blockchain data is especially useful when limited resources require sufficient recent memories or processing. As a result, the idea is that not all of the data collected by IoT devices should be kept and stored in the blockchain network. Almost all blockchain offerings, including IoT distribution networks, are open to the public. However, if the personal blockchain is used as much as feasible, scalability will no longer be as much of an issue as it is now [80]. Because the information is of the quickest subject, the private blockchain will no longer include that many performers. Its transmission is critical for the export company, the importer, and maybe other parties in the manufacturing process. Except for performers associated with the blockchain, most cannot participate in and verify the emergence.

6.3. IoT Blockchain Communication

The Internet of Things is rapidly expanding, with applications such as smart homes and cities, e-fitness, distributed intelligence, and so on. However, it creates difficult privacy and security conditions. To connect IoT devices, decentralized networking is used. As a result, employing the same old security approaches in spoken communication among IoT devices became significantly more complicated. Blockchain is a technology that provides security in transactions between different IoT nodes. Blockchain is a distributed, decentralized, and publicly accessible shared ledger that keeps track of the blocks processed and demonstrated in an IoT network. The public ledger's information is handled automatically via a peer-to-peer network. Blockchain is a generation in which IoT device transactions are recorded as a block in the blockchain. Blocks are linked, and each tool has a tool reference that comes before it. The approaches to blockchain and IoT integration work within IoT and

cloud integration techniques. Blockchain has the potential to alter future IoT conversations. The visions of blockchain and IoT integration are outlined below.

1. The decentralized method is quite similar to IoT and blockchain technologies. This removes the centralized device and provided the power of a decentralized method. This reduces the likelihood of failure and enhances the overall performance of the framework.
2. Security: Blockchain enables secure transactions between nodes. This is a revolutionary communication strategy. The Blockchain enables IoT devices to communicate with one another in a safe environment.
3. Identifications: IoT assists all associated gadgets that are uniquely recognized with a unique id variation. Every block in a blockchain is also uniquely identified.
4. However, blockchain is a trusted era that gives uniquely recognized information kept in a shared public ledger.
5. Reliability: The IoT nodes in blockchain can authenticate the information passed over the networks. Facts are reliable because miners validate them before entering the blockchain system. However, only the most useful proved blocks can be included in the blockchain device.
6. Autonomous: The blockchain enables all IoT nodes to connect with any node in the network without relying on a centralized approach.
7. Scalability: Blockchain enables IoT devices to communicate in a distributed intelligence network. It also communicates with real-time destination tools and alternate facts.

6.4. Platforms

Several systems are used to create IoT packages using blockchain.

1. IoTa: IoTa is the new platform for blockchain and IoT, also known as next-generation blockchain. By utilizing fewer assets within the device, the platform contributes to high information integrity, overall transaction performance, and block validity. This also resolves the blockchain restrictions.
2. IoTify: this provides a web-based IoT approach to reduce the constraints of blockchain in the form of customized applications.
3. Iexec: this open-source blockchain-based device is used to assist your apps and the blockchain's decentralized cloud benefits.
4. Xage: this versatile blockchain platform for IoT allows for increased automation and more relaxed data in the machine.
5. SONM is a decentralized blockchain-based fog computing platform that simplifies cloud offerings for users.

The IoT and blockchain are extending company potential and introducing new marketplaces in which anybody or everything can connect in real-time in a decentralized device with authenticity, privacy, and security. Incorporating these revolutionary technologies will revolutionize the current world on numerous levels, with gadgets communicating without people. The framework's goal is to provide safe data at the right place, in a suitable format, and real-time on a device. Blockchain will fine-tune billions of IoT-connected concerns, coordinate this stuff, facilitate transaction processing, resolve or eliminate crises, and build a flexible environment for running physical things. Blockchain develops data privacy for clients connected to the framework by utilizing hashing procedures in information blocks.

7. Current Trends in BC-IoT Development

Due to the security method of sending transactions between numerous entities without a trusted third and monitoring information veracity, blockchain gained a lot of attention. Even though many analysts feel that blockchain is the solution to many problems in today's fundamentally insecure internet because of its privacy and security capabilities, there may not be a systematic study to examine and evaluate blockchain from various angles [81]. Blockchain made its debut in 2009, less than a decade earlier. Because of this extraordinary

innovation, the globe underwent a rapid transition. Blockchain is making inroads into various professional industries, including retail, medical care, and science.

7.1. Federated Blockchain

Federated blockchain is one of the most significant and successful recent blockchain innovations. This is an upgraded method of the basic blockchain framework, making it perfect for various relevant applications. According to experts, federated blockchain could grow in popularity since it provides a more customizable perspective for private blockchain. Federated blockchains are comparable to private blockchains in most ways, with some small advantages. These blockchains are speedier (higher scalability) and provide greater transaction privacy. Federated blockchain examples include R3 (banks), EWF (energy), B3i (insurance), Corda, and more.

7.2. Blockchain as a Service (BaaS)

BaaS is the creation and maintenance by third parties of cloud-based systems used by industries to run blockchain-based apps. Another trend that Microsoft and Amazon are utilizing is BaaS. This recent blockchain trend is currently integrated with various startups and businesses. However, such future blockchain trends may not be viable while building, sustaining, and monitoring a new blockchain technique. It is a cloud-based system that uses blockchain technology to enable users to develop online services. Such digital products could be smart contracts, apps, or other services that operate independently of the blockchain-based network.

7.3. Ricardian Contracts

The Ricardian contract was designed to identify a legally valid document that was electronically linked to an important aspect. The Ricardian contract organizes all of the legal agreement facts into a layout that the program can execute. As a result, it is both a legal contract and a mechanism that electronically integrates the agreement into digital infrastructure while providing a secure network because of cryptographic verification. It is distinct from the smart contract. Smart contracts are a type of digital agreement that was previously agreed upon and is automatically executable. On the other hand, the Ricardian contract is an agreement paradigm for recording an agreement's objectives and any behavior related to that agreement prior to the agreement being performed. Ricardian contracts could likewise be simply applied to software by utilizing hashes that describe external documentation.

7.4. Blockchain Interoperability

Interoperability refers to exchanging information and other content across many blockchain networks and infrastructures. The public could easily access information that was held on a number of different blockchains because of this function [82,83]. It enables subscribers to transfer funds easily and quickly from one blockchain to another. This functionality also adds additional functions, such as cross-chain transactions. It can also improve multi-token transactions by constructing multi-token wallet services.

7.5. Social Networking

Blockchain in social networks would be capable of resolving difficulties such as prominent debates, privacy violations, information manipulation, and the significance of the material. As a result, blockchain is a new technology trend that is being integrated into social media architecture. Tokens are used by social networks. As a result, media companies are given financial incentives to generate content and increase network productivity. Token exchanges, such as the blockchain, are finished and practically instantaneous, with no charges.

7.6. Hybrid Blockchains

The future scope of blockchain technology, which could be simplified as the blockchain, proposes using a more appropriate fraction of public and private blockchain technologies. The exchange rate is slightly lower because the network's popular nodes make validating processes simple and quick. The hybrid blockchain operates in a closed ecosystem, so all evidence on the network improves security. This also avoids more than half of all attacks, since thieves cannot gain access to the blockchain system. The user can update the rules whenever it is necessary. It also helps to keep a task secret when engaging with the outside world.

8. Opportunities within the Integrated Technique

Several excellent potentials for blockchain–IoT integration were discovered. Blockchain–IoT together opens new opportunities in several regions. Figure 7 depicts the blockchain–IoT potential. However, some of the options are listed here.

Figure 7. Blockchain–IoT opportunities.

8.1. Create Trust among Gadgets

Because of its security, blockchain-IoT technology will instill trust in some of the numerous connected devices. However, only the most basic verified devices can communicate within the community, and the miners must first validate each transaction block before it can enter the blockchain [84].

8.2. Reduce the Expenses

It will save money because it communicates instantly using an online platform. This removes all third-party nodes. It also allows direct communication among IoT nodes.

8.3. Reduce Time

It may drastically shorten the time. Blockchain-IoT cuts transaction time from days to seconds.

8.4. Security and Privacy

Blockchain-IoT provides devices with security and anonymity, and data are exchanged between devices [85].

8.5. Social Services

Blockchain-IoT provides public and social services to connected nodes. Each connected gadget can communicate and exchange data [86].

8.6. Financial Services

It can safely transfer payments without the involvement of other parties. Blockchain-IoT enables a quick, secure, and private financial services system. It also decreases transfer costs and time, among other things [87].

8.7. Risk Management

It played a critical role in analyzing and mitigating the risk of system resources and transactions failing [88].

9. Challenges

Many difficulties, including measurement, storage, services, and discovery, could be addressed by blockchain–IoT. The blockchain–IoT challenges are depicted in Figure 8. The integrated strategy faces the following challenges.

Figure 8. Blockchain–IoT challenges.

9.1. Scalability

Because of its high transaction volume, blockchain can become blocked. On 10 July 2022, Bitcoin had more than 406 GB of storage space [89]. Weight can be considerably more significant than the best blockchain when IoT joins blockchain.

9.2. Storage

All IoT devices will store the given ledger. However, it will increase with its storage size in the form of being challenging to work with and a significant weight on every connected tool.

9.3. Inadequate Abilities

Most researchers are unaware of the blockchain phenomenon, which is increasingly mainstream. It is also an initiative to teach people nearly every technology.

9.4. Exploration and Integration

Blockchain is not intended for IoT applications. It is quite tricky for associated devices to locate another tool within the blockchain and IoT systems. As a result, IoT nodes can access all other nodes while detecting and integrating blockchain and other nodes.

9.5. Confidentiality

The shared ledger is broadcast to all connected devices. These gadgets are capable of viewing ledger transactions in real-time. As a result, maintaining privacy in an embedded system is a difficult task [90].

9.6. Interaction

Blockchain might be public, private, or in the form of a consortium. As a result, the interaction between public and private blockchains is also a blockchain IoT agreement.

9.7. Rules and Regulations

Because the IoT blockchain will function internationally, numerous norms and laws will be enforced globally.

This research looks on a novel approach known as blockchain-IoT. The article [91] discusses numerous possibilities and challenges. Similarly, this article lists the platforms that are available to implement Blockchain-IoT technique. Blockchain-IoT has the potential to lead the internet by redesigning and replacing it with a new internet service in which each smart device connects to other peer-to-peer devices. This can save both money and time while providing precise data to the relevant device. As a result, it has the potential to be a very useful strategy in the future.

10. Applications

The modern internet is concerned with the availability and security of connected resources. These resources might be encrypted on a network-to-network chain known as the blockchain or ledger, where each user knows with whom they transact. Because it simplifies the business, speeds up the process, eliminates failures, and saves it, it may safeguard commercial connections and avoid fraud. The distributed blockchain technology will transform people's life by allowing them to execute trades or control money via phones, vote, rent a car, and even prove their identity.

10.1. Smart Devices

A smart device connects wirelessly and gives users more excellent knowledge and control than ever before. For instance, if your washing machine stops working, a code associated with your device can connect to the internet and warn you. Such alerts keep the devices in good working order, saving them money on energy efficiency and allowing you to monitor the gadgets while on the road to work. Accessing such gadgets via the blockchain would safeguard the assets while allowing for information flow.

10.2. Sensors for the Supply Chain

A sensor is a device that detects and responds to a specific sort of input derived from physical infrastructure. Light, wind, movement, humidity, strain, or any other environmental changes may provide critical information. Sensors in the supply chain aid in the location of vehicle temperatures, pressures, and so on. When supply chain executives need to watch product or vehicle situations and determine precisely where they are and where they are heading, such inputs are used. The value of sensors in the supply chain is based on their ability to provide real-time activity information.

10.3. The Smart Contract

The smart contract evolved into a digital machine designed to electronically encourage, test, or execute the arrangement and execution of an agreement. Smart contracts allow for the performance of trustworthy exchanges without the use of third-party providers.

10.4. Keeping Track of Prescription Medications

Blockchains could improve the patient experience by allowing them to scan a barcode and instantaneously determine whether a prescription is counterfeit, according to the release. Its innovation could also determine when pharmaceuticals were gathered and transferred across the production process at the required temperature changes.

10.5. Voting through Electronic Means

In any country, the security of a vote is a matter of national security. Computer security is investigating the prospect of using an online voting system to lower the cost of hosting a federal election while meeting and increasing security criteria. Since the inception of democratic politicians, the voting mechanism was based on paper and pen. It is critical to replace the current pen-and-paper procedure with modern election technology to reduce fraud and make voting verifiable and trackable. Blockchains enable a wide range of applications that profit from the exchange. Blockchain has the potential to play a significant role in implementing shared electronic voting systems as a service. However, establishing electronic voting systems and using blockchain to implement these structures is fraught with difficulties.

10.6. Healthcare on the Blockchain

The blockchain can revolutionize healthcare data, place the patient at the centre of health infrastructure, and improve healthcare security, privacy, transparency, and connectivity. Such innovation has the potential to create a new architecture for health information sharing by making electronic records more influential, without an intermediary, and secure. This modern, continuously changing environment is ideal for innovation, research, and proof of concept testing.

10.7. Blockchain Music

In some cases, blockchain technology may be advantageous in music. It could increase availability or incentivize and share revenue with viewers through special edition electronic releases. However, employing it for a music service is unjust, and claiming it is a solution to any of the most pressing issues musicians confront is false.

10.8. Blockchain Identification

Identity verification is now an important aspect of our daily life. Visiting another nation, purchasing a new automobile, and enrolling in a university necessitate identification checks. Creating a new social media account also necessitates mobile authorization. Bringing personal belongings may not always be practical or even possible. That is where the blockchain's effective confidentiality control comes into play.

10.9. Passports

The idea behind a blockchain-based passport is that citizens can control electronic transport identification using provable information, such as biometrics, travel history, or any other related information gathered at checkpoints by trusted public authorities and other contact points. Instead of keeping the details to themselves, each authority or agency decides to rely on each other's data. Blockchain passport enables partnership members to obtain verifiable traveller-identifying information claims to assess validity, streamline passenger processing, and reduce risks. People can also use blockchain passport to retain their identification and acquire personal information, and digital attestations choose which

data to transmit. The more attestations a traveller possesses, the more alliance members, governments, and other parties may be able to guarantee smooth and secure travel.

10.10. Certificates of Birth, Marriage, and Death

Some things are more significant than showing the paperwork, such as birth certificates, marriage certificates, and expiry certificates that give you access to various benefits (such as elections, employment, and residency), but ineptitude is becoming more widespread. According to UNICEF, more than one-third of children under five do not have a birth certificate. The Blockchain can make records more secure by obtaining birth and death certificates and allowing users to access this vital information.

10.11. Processing of Insurance Claims

Smart contracts on the blockchain network might be used to handle insurance claims. In this case, all parties to an insurance policy may have access to the shared insurance ledger to view policy details. When a claim is applied, a claimant can submit evidence such as insurance papers, claim documents, and supporting claims proof to the distributed ledger. For statements, policyholders must interact directly with distributors. This activity is recorded on a private blockchain, with smart contracts enabling a workflow claim. Blockchain financial services and tariff plans need to be scrutinized. The active policy and smart contracts will be placed on the blockchain for policyholders with preset claim requirements.

10.12. Data Exchange

Blockchain is primarily concerned with improving the efficiency of data exchange across the supply chain, including producers, shipping providers, distributors, governments, suppliers, fulfilment centres, and consumers. Blockchains will allow the corporation to track the source of degradation much more quickly, reducing the impact of tainted products. Regarding customer refunds, blockchains can give end-to-end information traceability, the best right to examine the product's background, and real-time position and condition.

10.13. Copyright and Royalties Are Protected

Blockchains could be game changers for copyright holders looking to defend their rights electronically. Without question, it began to make its presence known to copyright holders. It remains to be seen whether the compliance procedures recommended for such networks will be implemented. However, the outlook remains positive. It is difficult to imagine blockchain being utilized to secure copyright in the coming months. This technique must first be broadly adopted before it can be widely used to defend copyright.

10.14. Property Registration, Real Estate, and Land Registration

Blockchains can profoundly alter the real estate market, from property acquisition to title management. It can transform the relationship between taxpayers and tax authorities and change how tax returns are submitted, taxes are paid, and data are handled. Blockchain technology can disrupt and restructure finance and streamline transaction, exchange, and property registration processes.

10.15. In a Catastrophic Situation (COVID-19)

The COVID-19 pandemic emphasizes global interconnectedness. This also highlights a complex reality: vast amounts of critical information stay trapped in fortified information storage facilities and reputation mechanisms when we require swift, collective action or cooperation. The blockchain–IoT integrated solutions aid in the resolution of the most difficult issues confronting us between 2019 and 22.

11. Conclusions

A critical component of this decentralization strategy was the blockchain design, which included hash-based proof of work, shared key encryption, and peer-to-peer networks. Complexity, limited compatibility, resource constraints, privacy and security concerns, and vulnerabilities hamper current IoT solutions. The rapid advancement of blockchain technology provides solutions to problems such as increased connectivity, privacy, security, transparency, and stability. Academics investigate the intersection of blockchain and the IoT throughout this post. They also discussed and presented literature on blockchain and the IoT. The issues and applications for developing a stable and interoperable communication infrastructure for blockchain and the IoT are discussed. This article examines current blockchain trends. The integration of blockchain and IoT architecture is investigated, as are the advantages and disadvantages of the combined strategy.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

IoT	Internet of Things
P2P	Peer-to-peer
PoS	Proof of stake
PoW	Proof of work
R3	An enterprise blockchain technology company
EWF	Energy web foundation
B3i	The blockchain insurance industry initiative
Corda	Open-source blockchain platform for business
Chain	A sequence of blocks
DPoS	Delegated proof of stake
PBFT	Practical Byzantine fault tolerance
dBFT	Delegated Byzantine fault tolerance
LPoS	Leased proof of stake
PoET	Proof of elapsed time
DBFT	Delegated Byzantine fault tolerance
DAG	Direct acyclic graph
POA	Proof of activity
PoI	Proof of importance
PoC	Proof of capacity
PoB	Proof of burn
PoWeight	Proof of weight
IOTA	The next generation of distributed ledger technology
IoTIFY	Online cloud-based MQTT/HTTP network simulator
iExec	Blockchain-based decentralized cloud computing
Xage	Blockchain cybersecurity system
SONM	Decentralized fog computing platform

References

1. Haber, S.; Stornetta, W.S. How to timestamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Aarhus, Denmark, 21–24 May 1990; Springer: Berlin/Heidelberg, Germany, 1990; pp. 437–455. [CrossRef]
2. 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]
3. Alangot, B.; Achuthan, K. Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud. In Proceedings of the International Conference on Ubiquitous Communications and Network Computing, Bangalore, India, 3–5 August 2017; Springer: Cham, Switzerland, 2017; pp. 189–195. [CrossRef]
4. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]

5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 23 October 2022).
6. Samaniego, M.; Jamsrandorj, U.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 433–436. [CrossRef]
7. Ammous, S. *Blockchain Technology: What is it good for?* SSRN: Rochester, NY, USA, 2016. [CrossRef]
8. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [CrossRef]
9. Risius, M.; Spohrer, K. A blockchain research framework. *Bus. Inf. Syst. Eng.* **2017**, *59*, 385–409. [CrossRef]
10. Huckle, S.; Bhattacharya, R.; White, M.; Beloff, N. Internet of things, Blockchain and shared economy applications. *Procedia Comput. Sci.* **2016**, *98*, 461–466. [CrossRef]
11. Xia, B.; Ji, D.; Yao, G. Enhanced tls handshake authentication with blockchain and smart contract (short paper). In *International Workshop on Security*; Springer: Cham, Switzerland, 2017; pp. 56–66. [CrossRef]
12. Haffke, F. Technical Analysis of Established Blockchain Systems. Master's Thesis, Technical University of Munich, SW Engineering for Business Informatics, München, Germany, 2017.
13. Mingxiao, D.; Xiaofeng, M.; Zhe, Z.; Xiangwei, W.; Qijun, C. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. [CrossRef]
14. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
15. 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. [CrossRef]
16. Marsal-Llacuna, M.L. Future living framework: Is Blockchain the next enabling network? Technol. *Forecast. Soc. Change* **2018**, *128*, 226–234. [CrossRef]
17. 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]
18. Yang, W.; Garg, S.; Raza, A.; Herbert, D.; Kang, B. Blockchain: Trends and future. In *Pacific Rim Knowledge Acquisition Workshop*; Springer: Cham, Switzerland, 2018; pp. 201–210. [CrossRef]
19. Alphand, O.; Amoretti, M.; Claeys, T.; Dall'Asta, S.; Duda, A.; Ferrari, G.; Rousseau, F.; Tourancheau, B.; Veltri, L.; Zanichelli, F. IoTChain: A blockchain security architecture for the Internet of Things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6. [CrossRef]
20. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
21. 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]
22. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
23. 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]
24. Cai, W.; Wang, Z.; Ernst, J.B.; Hong, Z.; Feng, C.; Leung, V.C. Decentralized applications: The blockchain-empowered software system. *IEEE Access* **2018**, *6*, 53019–53033. [CrossRef]
25. El Ioini, N.; Pahl, C. A review of distributed ledger technologies. In Proceedings of the OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", Valletta, Malta, 22–26 October 2018; Springer: Cham, Switzerland, 2018; pp. 277–288. [CrossRef]
26. Shrestha, A.K.; Vassileva, J. Bitcoin Blockchain Transactions Visualization. In Proceedings of the 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), Fuzhou, China, 15–17 November 2018; pp. 1–6. [CrossRef]
27. Tasatanattakool, P.; Techapanupreeda, C. Blockchain: Challenges and applications. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 473–475. [CrossRef]
28. Chang, M.C.; Park, D. How can Blockchain help people in the event of pandemics such as the COVID-19? *J. Med. Syst.* **2020**, *44*, 102. [CrossRef] [PubMed]
29. Kshetri, N.; Voas, J. Blockchain in developing countries. *It Prof.* **2018**, *20*, 11–14. [CrossRef]
30. Alam, T. IoT-Fog: A Communication Framework using Blockchain in the Internet of Things. *Int. J. Recent Technol. Eng.* **2019**, *7*. [CrossRef]
31. Dujak, D.; Sajter, D. Blockchain applications in supply chain. In *SMART Supply Network*; Springer: Cham, Switzerland, 2019; pp. 21–46. [CrossRef]

32. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
33. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
34. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
35. Dabbagh, M.; Sookhak, M.; Safa, N.S. The evolution of Blockchain: A bibliometric study. *IEEE Access* **2019**, *7*, 19212–19221. [CrossRef]
36. Thakore, R.; Vaghashiya, R.; Patel, C.; Doshi, N. Blockchain-based IoT: A survey. *Procedia Comput. Sci.* **2019**, *155*, 704–709. [CrossRef]
37. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* **2019**, *8*, 100107. [CrossRef]
38. Devibala, A. A Survey on Security Issues in IoT for Blockchain Healthcare. In Proceedings of the 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 20–22 February 2019; pp. 1–7. [CrossRef]
39. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
40. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A survey on the scalability of blockchain systems. *IEEE Network* **2019**, *33*, 166–173. [CrossRef]
41. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34. [CrossRef]
42. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.K.R. Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access* **2019**, *7*, 176935–176951. [CrossRef]
43. Gill, S.S.; Tuli, S.; Xu, M.; Singh, I.; Singh, K.V.; Lindsay, D.; Tuli, S.; Smirnova, D.; Singh, M.; Jain, U.; et al. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet Things* **2019**, *8*, 100118. [CrossRef]
44. Odiljon, A.; Gai, K. Efficiency Issues and Solutions in Blockchain: A Survey. In Proceedings of the International Conference on Smart Blockchain, Birmingham, UK, 11–13 October 2019; Springer: Cham, Switzerland, 2019; pp. 76–86. [CrossRef]
45. Pohrmen, F.H.; Das, R.K.; Khongbuh, W.; Saha, G. Blockchain-based security aspects in Internet of Things network. In Proceedings of the International Conference on Advanced Informatics for Computing Research, Shimla, India, 14–15 July 2018; Springer: Singapore, 2018; pp. 346–357. [CrossRef]
46. Sharma, K.; Jain, D. Consensus algorithms in blockchain technology: A survey. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; pp. 1–7. [CrossRef]
47. Scriber, B.A. A framework for determining blockchain applicability. *IEEE Softw.* **2018**, *35*, 70–77. [CrossRef]
48. Noby, D.A.; Khattab, A. A Survey of Blockchain Applications in IoT Systems. In Proceedings of the 2019 14th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 17–18 December 2019; pp. 83–87. [CrossRef]
49. Atlam, H.F.; Wills, G.B. Technical aspects of Blockchain and IoT. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2019; Volume 115, pp. 1–39. [CrossRef]
50. Viriyasitavat, W.; Hoonsopon, D. Blockchain characteristics and consensus in modern business processes. *J. Ind. Inf. Integr.* **2019**, *13*, 32–39. [CrossRef]
51. Rathore, H.; Mohamed, A.; Guizani, M. A survey of Blockchain enabled cyber-physical systems. *Sensors* **2020**, *20*, 282. [CrossRef]
52. Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Comput. Surv.* **2020**, *53*, 18. [CrossRef]
53. Alam, T.; Benaida, M. CICS: Cloud-internet communication security framework for the internet of smart devices. *Int. J. Interact. Mob. Technol.* **2018**, 12. [CrossRef]
54. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
55. 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]
56. Singh, A.; Parizi, R.M.; Zhang, Q.; Choo KK, R.; Dehghantanha, A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Comput. Secur.* **2020**, *88*, 101654. [CrossRef]
57. Chentouf, F.Z.; Bouchkaren, S. Blockchain for Cybersecurity in IoT. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 61–83. [CrossRef]
58. Zafar, S.; Bhatti, K.M.; Shabbir, M.; Hashmat, F.; Akbar, A.H. Integration of blockchain and Internet of Things: Challenges and solutions. *Ann. Telecommun.* **2022**, *77*, 13–32. [CrossRef]
59. Huo, R.; Zeng, S.; Wang, Z.; Shang, J.; Chen, W.; Huang, T.; Wang, S.; Yu, F.R.; Liu, Y. A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 88–122. [CrossRef]
60. Bansod, S.; Ragha, L. Blockchain Technology: Applications and Research Challenges. In Proceedings of the 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 5–7 June 2020; pp. 1–6. [CrossRef]

61. Cervone, L.; Palmirani, M.; Vitali, F. The Intelligible Contract. In Proceedings of the HICSS, Maui, HI, USA, 7–10 January 2020; pp. 1–10. [CrossRef]
62. Cui, Z.; Fei XU, E.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A hybrid BlockChain-based identity authentication scheme for multi-WSN. *IEEE Trans. Serv. Comput.* **2020**, *13*, 241–251. [CrossRef]
63. 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]
64. Dunphy, P.; Petitcolas, F.A. A first look at identity management schemes on the Blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
65. Ekramifard, A.; Amintoosi, H.; Seno, A.H.; Dehghantanha, A.; Parizi, R.M. A systematic literature review of integration of Blockchain and artificial intelligence. In *Blockchain Cybersecurity, Trust and Privacy*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 147–160. [CrossRef]
66. Guidi, B. When Blockchain meets online social networks. *Pervasive Mob. Comput.* **2020**, *62*, 101131. [CrossRef]
67. Kshetri, N.; Voas, J. Blockchain-enabled e-voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
68. Lu, Y. The Blockchain: State-of-the-art and research challenges. *J. Ind. Inf. Integr.* **2019**, *15*, 80–90. [CrossRef]
69. Notheisen, B.; Cholewa, J.B.; Shanmugam, A.P. Trading real-world assets on Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 425–440. [CrossRef]
70. Oham, C.; Jurdak, R.; Kanhere, S.S.; Dorri, A.; Jha, S. B-fica: Blockchain based framework for auto-insurance claim and adjudication. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1171–1180. [CrossRef]
71. Perrons, R.K.; Cosby, T. Applying Blockchain in the geoenergy domain: The road to interoperability and standards. *Appl. Energy* **2020**, *262*, 114545. [CrossRef]
72. Alam, T. Blockchain-based big data integrity service framework for IoT devices data processing in smart cities. *Mindanao J. Sci. Technol.* 2021. [CrossRef]
73. Alam, T. Blockchain-Enabled Deep Reinforcement Learning Approach for Performance Optimization on the Internet of Things. *Wirel. Pers. Commun.* **2022**, *126*, 995–1011. [CrossRef]
74. Alam, T. Cloud-based IoT applications and their roles in smart cities. *Smart Cities* **2021**, *4*, 1196–1219. [CrossRef]
75. Alam, T. IoT-fog-blockchain framework: Opportunities and challenges. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*; IGI Global: Hershey, PA, USA, 2023; pp. 258–277. [CrossRef]
76. Alam, T.; Ullah, A.; Benaida, M. Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems. *J. Ambient Intell. Humaniz. Comput.* **2022**, 1–14. [CrossRef]
77. Tang, B.; Kang, H.; Fan, J.; Li, Q.; Sandhu, R. IoT passport: A blockchain-based trust framework for collaborative internet-of-things. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, Toronto, ON, Canada, 3–6 June 2019; pp. 83–92. [CrossRef]
78. Uriarte, R.B.; DeNicola, R. Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards. *IEEE Commun. Stand. Mag.* **2018**, *2*, 22–28. [CrossRef]
79. Abujassar, R.S.; Yaseen, H.; Al-Adwan, A.S. A Highly Effective Route for Real-Time Traffic Using an IoT Smart Algorithm for Tele-Surgery Using 5G Networks. *J. Sens. Actuator Netw.* **2021**, *10*, 30. [CrossRef]
80. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
81. Salah, K.; Rehman MH, U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
82. Savelyev, A. Copyright in the blockchain era: Promises and challenges. *Comput. Law Secur. Rev.* **2018**, *34*, 550–561. [CrossRef]
83. Sullivan, C.; Burger, E. E-residency and Blockchain. *Comput. Law Secur. Rev.* **2017**, *33*, 470–481. [CrossRef]
84. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C. Blockchain and machine learning for communications and networking systems. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1392–1431. [CrossRef]
85. Vashisht, S.; Gaba, S.; Dahiya, S.; Kaushik, K. Security and Privacy Issues in IoT Systems Using Blockchain. In *Sustainable and Advanced Applications of Blockchain in Smart Computational Technologies*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2022; pp. 113–127. [CrossRef]
86. Dahiya, A.; Gupta, B.B.; Alhalabi, W.; Ulrichd, K. A comprehensive analysis of Blockchain and its applications in intelligent systems based on IoT, cloud and social media. *Int. J. Intell. Syst.* 2022. [CrossRef]
87. Elngar, A.A.; Kayed, M.; Emira, H.H.A. The role of Blockchain in financial applications: Architecture, benefit, and challenges. In *Artificial Intelligence and Big Data for Financial Risk Management*; Routledge: London, UK, 2022; pp. 140–159. [CrossRef]
88. Choudhary, T.; Virmani, C.; Juneja, D. Convergence of Blockchain and IoT: An Edge Over Technologies. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*; Springer: Cham, Switzerland, 2020; pp. 299–316. [CrossRef]
89. Statista. Size of the Bitcoin Blockchain from January 2009 to 11 July 2022. 2022. Available online: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (accessed on 21 October 2022).

90. Ebrahim, M.; Hafid, A.; Elie, E. Blockchain as privacy and security solution for smart environments: A Survey. *arXiv* **2022**, arXiv:2203.08901.
91. 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]