Review

Not peer-reviewed version

Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions

Muath A. Obaidat * , Majdi Rawashdeh , Mohammad Alja'afreh , Meryem Abouali , Kutub Thakur , Ali Karime

Posted Date: 16 September 2024

doi: 10.20944/preprints202409.1193.v1

Keywords: Blockchain integration; I T security; Security; privacy; cyber-attacks; smart devices; distributed ledger technologv

Article

Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions

Muath A. Obaidat [1,*], Majdi Rawashdeh [2], Mohammad Alja'afreh [3], Meryem Abouali [4], Kutub Thakur [5] and Ali Karime [6]

[1] Department of Computer Science, John Jay College and the Graduate School and University Center of the City University of New York, New York, NY 10016
[2] Department of Business Information Technology, Princess Sumaya University for Technology, Amman, Jordan, College of Engineering and Architecture, Department of Software Engineering, Al Yamamah University, Riyadh, Kingdom of Saudi Arabia; m.rawashdeh@psut.edu.jo
[3] Department Communication Engineering, IoT Program, Princess Sumaya University for Technology Amman, Jordan; m.aljaafreh@psut.edu.jo
[4] Department of Computer Science, John Jay College, New York NY 10019; mabouali@jjay.cuny.edu
[5] Department of Professional Security Studies, New Jersey City University, Jersey City, NJ 07305, USA; kthakur@njcu.edu
[6] Electrical and Computer Engineering. Royal Military College of Canada. PO Box 17000, Station Forces. Kingston, Ontario, Canada; ali.karime@rmc-cmr.ca
* Correspondence: muobaidat@ccny.cuny.edu or mobaidat@jjay.cuny.edu

Abstract: The emergence of the Internet of Things (IoT) has led to remarkable advancements in various sectors such as urbanization, manufacturing, and healthcare, intending to enhance the quality of life and contribute to the world economy. However, by the conclusion of 2024, it is projected that the global network of the Internet of Things (IoT) will encompass over 207 billion interconnected devices. The immense data collected and exchanged are often stored in centralized servers, leading to vulnerabilities such as data breaches. Blockchain technology, originally developed for cryptocurrency transactions, provides a possible solution for these challenges with its decentralized, immutable, and encrypted features. This survey provides a comprehensive discussion regarding the fusion of Blockchain technology and the IoT, covering architectural alignment, application, security, and limitations. The contributions of this survey include an overview of Blockchain technology and its secure applications, the integration of Blockchain into IoT, an examination of suitable methods for IoT-Blockchain integration, and a taxonomy of security and limitations of IoT and Blockchain integration.

Keywords: blockchain integration; IoT security; Security; privacy; cyber-attacks; smart devices; distributed ledger technology

1. Introduction

The Internet of Things has grown significantly in The Internet of Things (IoT) has seen remarkable growth in recent years, with its application covering various services globally, including urban management, production, and healthcare[1,2]. The purpose of IoT technology goes beyond improving people's day-to-day experiences; it also aims to strengthen the global economy by advancing multiple sectors[3-5]. However, the rapid increase in IoT devices has brought about significant privacy and security challenges[6-9]. By 2024, the total number of IoT devices is projected to exceed 207 billion [9,10]. These devices gather a wide array of data, typically stored on centralized servers, which, in turn, raises issues about data security and trustworthiness[11-15]. years and is used in various services around the world, such as cities, manufacturing, and healthcare[1,2]. The goal of IoT technology is not only to improve people's lives but also to contribute to the global economy by enhancing various sectors[3-5]. However, the exponential growth of IoT devices has caused numerous privacy and security issues[6-9]. By the end of 2024, the number of IoT devices is expected to surpass 207 billion devices by the end of the year 2024[9, 10]. These devices collect diverse data, which is stored in centralized servers, raising concerns about data security and trust[11-15].

IoT devices face several challenges, including the need for management by multiple administrators and the risk of unencrypted serves, which can lead to data breaches[16-18]. Blockchain technology offers a new way to serve decentralized storage and manage data. It uses a shared, secured, and distributed ledge to store and protect data without a centralized system, eliminating the need for third-party collectors[9-20]. Furthermore, blockchain allows devices to communicate and exchange technology's decentralized, immutable, and shared nature, along with its use of encrypted databases, which helps secure against various attacks[20-25]. One of the classic ways to collect data from IoT devices is storing in certain centralized servers such as cloud servers that are used often[1, 2, 4, 12]. The storage of data in the cloud has caused people not to trust IoT devices, which pushed for the development of trusted decentralized servers so that sensitive and private data are stored safely on these servers [13-15]. Some IoT devices can face challenges, while others need to be managed by more than one manager simultaneously; another issue is that these IoT devices can have an unencrypted server [16] which can lead to data being hacked and from this hackers can publish sensitive personal information [17, 18].

When it comes to protection Blockchain technology is the new way to secure decentralized storage and data management, the concept with which it works is the one of a shared, secured, and distributed ledger where it stores and keeps safe all the records and data without there being a centralized system and removes the third party collector[19, 20]. What Blockchain helps is that it allows two or devices to communicate and exchange information, resources, and all sorts of data in a network which is decentralized which is known as a peer-to-peer network[21-23]. Blockchain technology is decentralized, immutable, and shared it uses a database ledger that stores and registers data and transactions in the network [20, 24].

Blockchain also helps to protect against different attacks, as the goal is to control a centralized system and what to do with leaked personal information and other valuable data [20, 25]. Another advantage of using Blockchain in IoT devices is that the Blockchain network is encrypted, which means in a P2P network every node is equipped with two different keys where one is public and is used by other nodes to encrypt the messages[2, 12] and the other one is the private key which is used to decrypt the received message[2, 12, 20, 26]. Despite its origins in cryptocurrency, blockchain technology is increasingly being used in IoT applications due to its security features[27,28] .

1.1. Contributions

The contribution of this paper is a comprehensive discussion of recent advances in IoT and Blockchain technology. This survey highlights the role of blockchain technology in integrating into the IoT infrastructure to provide secure authentication. The main contributions of this paper are as follows.

- An overview of Blockchain technologies, including components features, and characteristics of Blockchain, and secure application methods
- A focuses on how blockchain can be integrated into the Internet of Things (IoT) infrastructure, discussing recent methods and examples.
- A summary of blockchain application into IoT, implementation methods, and the requirements for integration.
- A discussion on Blockchain security, and how it can protect IoT from cyber-attacks, with suggestions and protective measures.
- An exploration of the most suitable methods for IoT- Blockchain integration, architectural challenges, and issues, along with an overview of consensus protocols and algorithms.
- A taxonomy detailing the security considerations and constraints involved in the IoT and blockchain integration process aiming at establishing a secure authentication framework.

1.2. Organization of the Paper

The paper follows a structured organization, beginning with an in-depth introduction to the topic. It then proceeds to discuss the research methodology and related work in Section two, providing insights into the research approach and reviewing existing literature. Section three elaborates on the characteristics and features of blockchain technology, while Section four summarizes how blockchain can enhance security in IoT applications. The integration of blockchain with IoT is thoroughly explored in Section five, which highlights the requirements and development of this integration. Moving forward, Section six explains the challenges and potential security threats associated with integrating Blockchain into IoT systems. Section seven offers a discussion on countermeasures against attacks, Blockchain privacy, IoT trust issues, and solutions based on Blockchain technology for IoT, including consensus algorithms. Furthermore, Section eight provides a taxonomy of security research in IoT with Blockchain, concluding with research directions and open issues. Finally, section nine concludes the paper, wrapping up the main discoveries and implications discussed throughout the paper. The organization and layout of the paper are visualized in Figure 1.

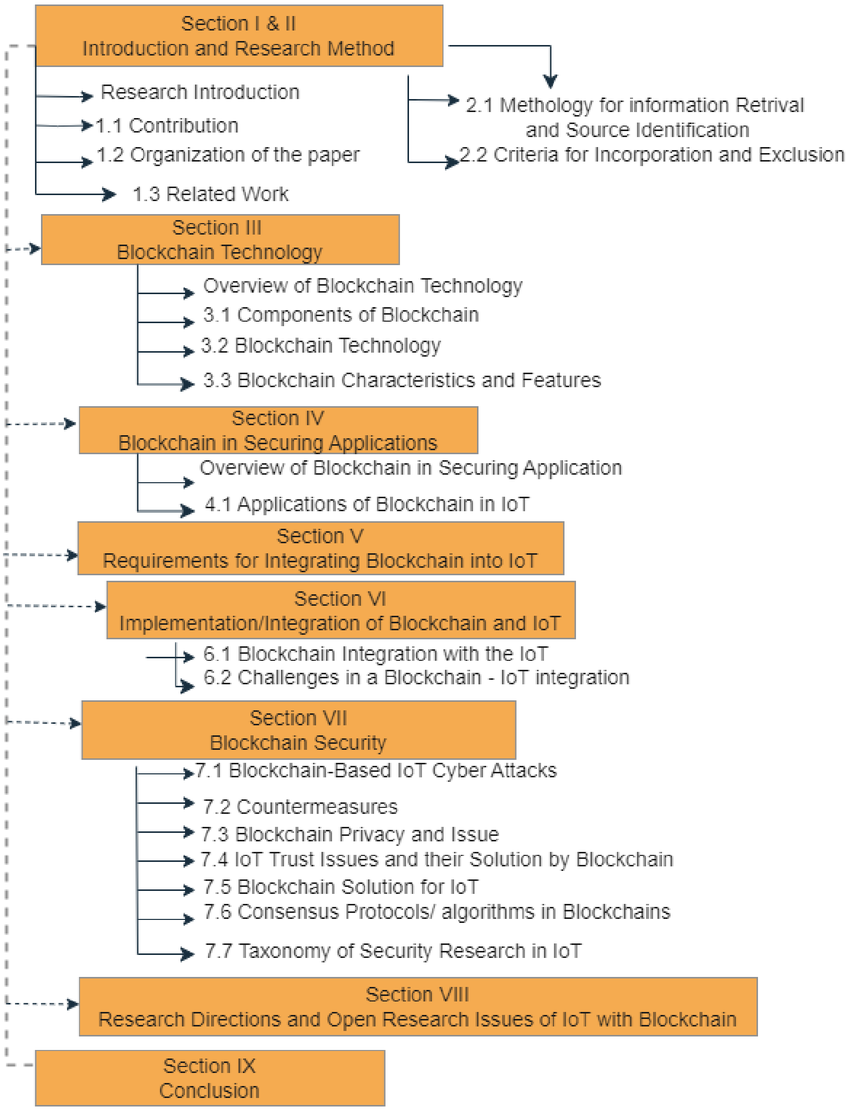
Section I & II
Introduction and Research Method
Research Introduction
1.1 Contribution
1.2 Organization of the paper
1.3 Related Work
2.1 Methology for information Retrival and Source Identification
2.2 Criteria for Incorporation and Exclusion
Section III
Blockchain Technology
Overview of Blockchain Technology
3.1 Components of Blockchain
3.2 Blockchain Technology
3.3 Blockchain Characteristics and Features
Section IV
Blockchain in Securing Applications
Overview of Blockchain in Securing Application
4.1 Applications of Blockchain in IoT
Section V
Requirements for Integrating Blockchain into IoT
Section VI
Implementation/Integration of Blockchain and IoT
6.1 Blockchain Integration with the IoT
6.2 Challenges in a Blockchain - IoT integration
Section VII
Blockchain Security
7.1 Blockchain-Based IoT Cyber Attacks
7.2 Countermeasures
7.3 Blockchain Privacy and Issue
7.4 IoT Trust Issues and their Solution by Blockchain
7.5 Blockchain Solution for IoT
7.6 Consensus Protocols/ algorithms in Blockchains
7.7 Taxonomy of Security Research in IoT
Section VIII
Research Directions and Open Research Issues of IoT with Blockchain
Section IX
Conclusion

Figure 1. Paper organization.

1.3. Related work

Various surveys have examined the integration of blockchain and IoT, primarily focusing on security aspects. In this section, several surveys are discussed and categorized into three groups [3, 11, 21, 25, 26, 29-43], and we will separate them into three categories. The first category reviews technical details and blockchain applications. One survey focuses on the technologies and applications of blockchain, discussing taxonomy, consensus algorithm, and security vulnerabilities[29]. Another survey examines blockchain's security features and its applications in business, education, IoT, finance, and other fields. Moreover, it talks more about security attacks and what kind of vulnerabilities Blockchain offers since it is still a new technology[30]. Additional surveys explore privacy protection techniques within IoT and blockchain and how blockchain addresses privacy and security threats in IoT devices[31, 34].

One survey highlights the use of blockchain for security authentication and maintenance through decentralization, recommending its integration into IoT frameworks. Furthermore, the use of Blockchain technology as a solution to address privacy and security threats has emerged due to the widespread use of IoT devices that offer the mentioned features. The article recommends integrating blockchain into the IoT framework for an efficient and secure system to prevent negative impacts on various aspects of our environment and society [11]. Other surveys [3], discuss communication protocols and the relationship between IoT and blockchain, including fog and cloud computing applications [35]. In the above section, the survey was about Blockchain and the Internet of Things, but other research has gone through Blockchain applications that can help improve or create a better system for the Internet of Things. One survey published [26] has been working on how to optimize blockchain for IoT, focused on consensus algorithms, architecture, cryptography, etc. [36].

In addition, we have another survey that has worked with security issues that come from the Internet of Things. They have explored how Blockchain can enhance IoT security issues [32]. Some surveys have reviewed blockchain-enabled IoT applications from two main perspectives: data management and things management, which are mainly related to IoT [37, 38]. Daily advances in Blockchain technology and its impact on the future of IoT applications primarily related to security have gotten the attention of many researchers [39]. Also, an author is interested in integrating Blockchain in IoT since it is considered a vast security player in IoT[33] and has reviewed security issues using Blockchain for IoT applications [40]. Finally, since Blockchain is a field of broad study, we have a lot of surveys and researchers working on the theoretical sites of Blockchain, such as edge computing, summarizing how integration is done, as well as how the applications of Blockchain for IoT are viewed from a system design perspective [40, 42].

Another paper that has been developed has been authored that focuses on the connection between Blockchain and cybersecurity. Their article has shown the research about Blockchain applications for cybersecurity purposes divided into multiple domains. The paper demonstrates that over half of the literature is focused on Blockchain to secure domains for the Internet and IoT [43]. One of the authors, Taylor, recommended viewing all other opportunities using different Blockchain systems like Ethereum, which can help develop and find other possible solutions that can secure cybersecurity and IoT in securing our devices [43]. The other author examines the special difficulties and remedies related to protecting blockchain-based Internet of Things systems, emphasizing the use of anonymous auditing to strengthen security and privacy while preserving the integrity and openness of Blockchain transactions. The authors suggest a brand-new architecture that blends cutting-edge security mechanisms designed for Internet of Things scenarios with the decentralized nature of Blockchain technology [21]. As we mentioned, security and Blockchain are areas that most researchers focus on. Furthermore, papers by K. Salah and M.A Khan provide more details about layered taxonomy, what characterizes IoT security issues, and what countermeasures can be taken. This paper also discusses and analyzes the characteristics of Blockchain security solutions and their effectiveness in securing IoT [36].

researchers also emphasize the potential of blockchain in IoT security and its role in addressing security issues. Moreover, the main solution is based on smart contracts, which are the first step to take or ensure security, which is discussed in more depth in the research by F. Casino [25]. In his research paper, the author reviews blockchain-based applications in different domains. The point is to classify blockchain-based applications in various domains that move from the supply chain to the Internet of Things. Through this, what are the limitations of blockchain and how can blockchain be adopted in those domains [25]

All of the examined research has attempted to address inquiries regarding the broader application of Blockchain. All those papers whose primary goal is to use blockchain technology for security, and for sure this field of research is advancing quickly and is gaining more attention by researchers because of promising implications as well. However, they do not analyze or investigate the suitability of Blockchain Smart Contracts to achieve a level of security in all areas of the Internet, especially on the Internet of Things. Thus, it is good to provide the most recent results from this research area because it motivates new researchers to develop further advanced approaches by ensuring security using Blockchain.

2. Research Methodology

2.1. Methodology for Information Retrieval and Source Identification

The research methodology for securing IoT devices through the integration of blockchain technology is designed to ensure a robust and thorough investigation. The methodology of PRISMA (preferred reporting elements for systematic reviews and meta-analysis) is adopted as the foundation of the approach, widely considered a gold standard framework for conducting systematic reviews, providing a structured and transparent process to identify, evaluate, and synthesize relevant studies [44]. To begin the research, a meticulous search process is undertaken across a diverse array of scientific databases, including Science Direct, Google Scholar, IEEE, and ACM. This expansive search strategy allows for casting a wide net and gathering a comprehensive selection of scholarly articles about IoT security and Blockchain integration. Temporal limitations on the search are avoided, allowing the capture of relevant literature spanning from 2019 to 2024. [45].

2.2. Criteria for Incorporation and Exclusion

Keyword selection is a crucial aspect of the search strategy, employing a carefully considered set of keywords such as "' IoT security, 'Blockchain integration,' cybersecurity,' 'smart devices, 'and 'distributed ledger technology.' These keywords are chosen to encapsulate the core themes and concepts relevant to the research inquiry. The identification process returned a total of 925,573. Titles identified during the search process will undergo screening based on established criteria outlined in the PRISMA checklist. Duplicate articles will be removed using EndNote 21.1 reference management software. Articles that meet the screening criteria will proceed to title and abstract screening, resulting in the exclusion of 17,590 articles. The study is meticulously structured and executed following the scoping and systematic review guidelines, guided by the Population, Context, and Concept(PCC) framework. This framework offers a systematic method for crafting research questions and identifying relevant study components, ensuring the analysis is comprehensive and extensive. In implementing the search strategy, the titles and abstracts of the retrieved articles are rigorously screened based on the predefined criteria established in the PRISMA checklist, which equates to 17,890 articles. Duplicate articles are identified and removed using reference management software to streamline the screening process. Furthermore, 168,270 articles that meet the screening criteria are submitted for full-text evaluation.

During the full-text assessment, each article undergoes a detailed evaluation of relevance, duplication, and availability of full text. Only English-language papers meeting inclusion criteria are considered for further analysis. Journal-wise statistics are analyzed to acquire insights into the distribution of relevant literature across different publication sources, providing valuable context to the findings. In addition to the systematic review, a comprehensive analysis of existing literature is conducted to identify relevant studies on IoT security, Blockchain integration, and related domains. This synthesis offers a holistic evaluation of the application of blockchain technology in securing IoT devices. Exclusion criteria are used to guarantee the integrity and focus of the analysis. Articles containing duplicated information, irrelevant content, or not directly related to IoT security and Blockchain integration are excluded from consideration amounting to 148,450 articles. In addition, resources such as case series, reports, brief communications, and editorial comments are omitted from the final selection of articles, preserving the scholarly rigor of the study. Through this comprehensive and methodical approach, a distinctive understanding of the integration of Blockchain technology for securing IoT devices is aimed. Keeping in mind established methodologies and guidelines, the objective is to produce research outcomes that are rigorous, reliable, and actionable.Figure.2

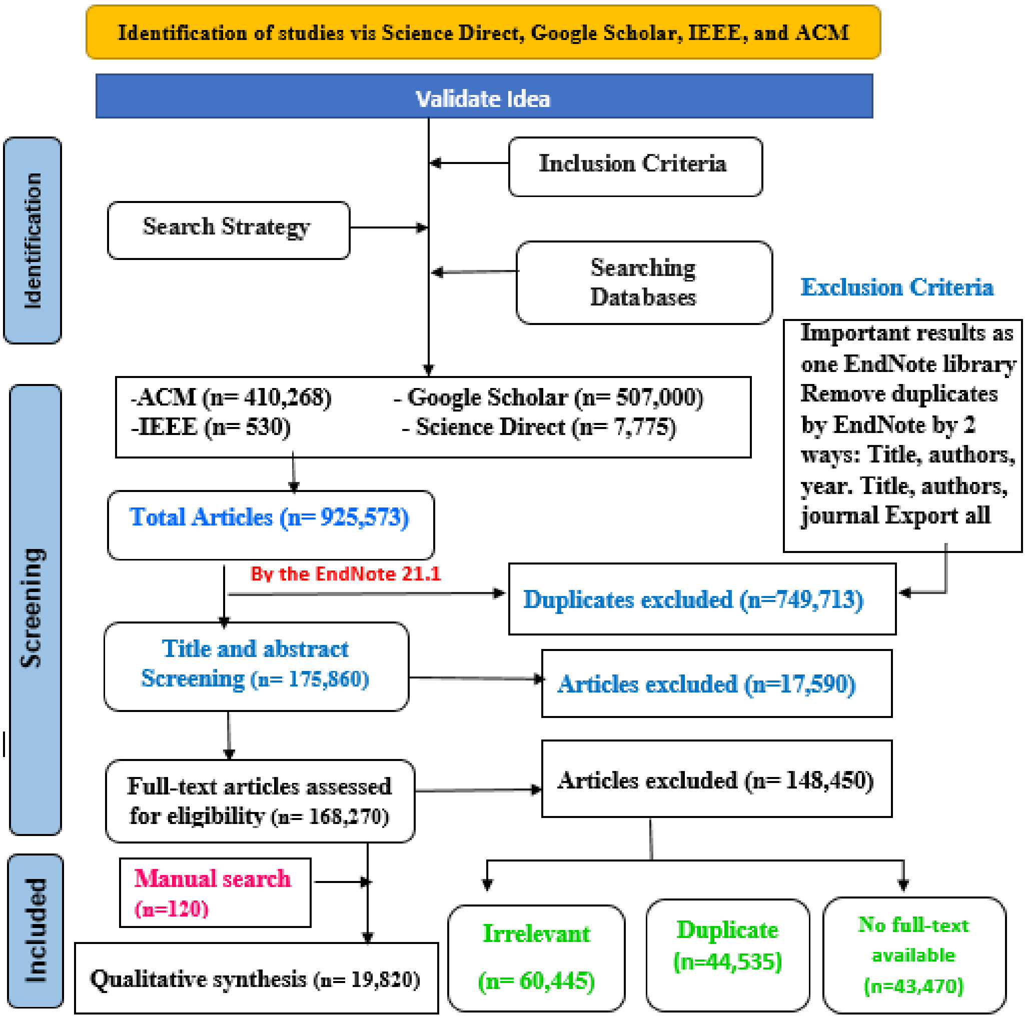
Identification of studies vis Science Direct, Google Scholar, IEEE, and ACM
Validate Idea
Identification
Inclusion Criteria
Search Strategy
Searching Databases
Exclusion Criteria
Important results as one EndNote library Remove duplicates by EndNote by 2 ways: Title, authors, year. Title, authors, journal Export all
Screening
-ACM (n= 410,268)
-IEEE (n= 530)
- Google Scholar (n= 507,000)
- Science Direct (n= 7,775)
Total Articles (n= 925,573)
By the EndNote 21.1
Duplicates excluded (n=749,713)
Title and abstract Screening (n= 175,860)
Articles excluded (n=17,590)
Full-text articles assessed for eligibility (n= 168,270)
Articles excluded (n= 148,450)
Included
Manual search (n=120)
Qualitative synthesis (n= 19,820)
Irrelevant (n= 60,445)
Duplicate (n=44,535)
No full-text available (n=43,470)

Figure 2. The PRISMA model guiding the article selection process.

3. Blockchain Technology

Satoshi Nakamoto first presented Blockchain, but it is still unknown whether a person or a group of people anonymously created Bitcoin. Often, people mistake Blockchain for Bitcoin [38]. Bitcoin is a digital currency based on Blockchain technology that permits trading freely worldwide without requiring a financial institution as a guarantor Bitcoin is merely a monetary application of blockchain technology. Blockchain is characterized as an unchanging, auditable, timestamp and tamper resistant block ledger that shares, stores, and uses information in a peer-to-peer (P2P) way [45-47]. Figure 3 shows the types of decentralized ledger technology, categorized into data structure ledges and permission and accessibility ledgers.

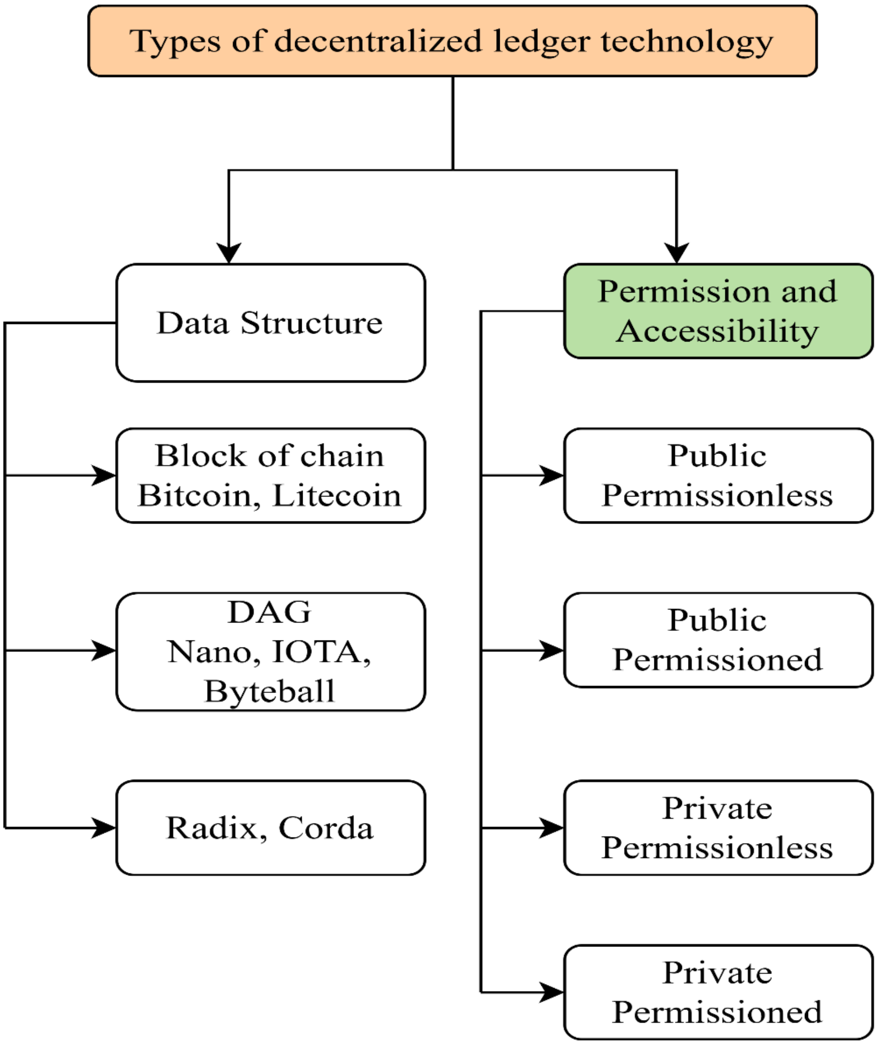

Figure 3. Types of Decentralized Ledger Technology.

The data stored in the blockchain can vary, including payment history and personal information. Blockchain stores information in blocks, which are then connected in a chain. When new information is added, it is placed into a new block, which, once filled, is secured to the previous block, maintaining the information in sequential order [44-46, 48,49]. Figure 4 depicts the types of blockchain networks, including structured networks, unstructured networks, and hybrid networks.

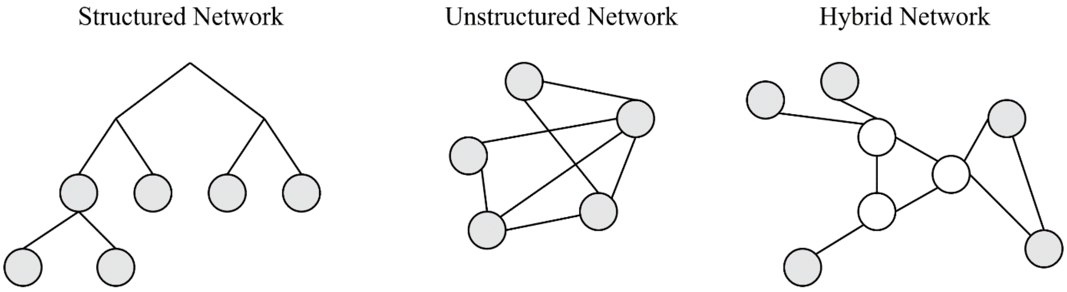

Figure 4. Structure of Blockchain Network.

3.1. Components of Blockchain

Blockchain technology can convey a few benefits over today's arrangements, as those components make Blockchain technology different from other technologies used until now. There are many elementary features of blockchain technology: ledger, block, minor, hashing, consensus mechanism, and transaction [46, 50, 51]. The primary elements of the Blockchain are shown in Figure 5.

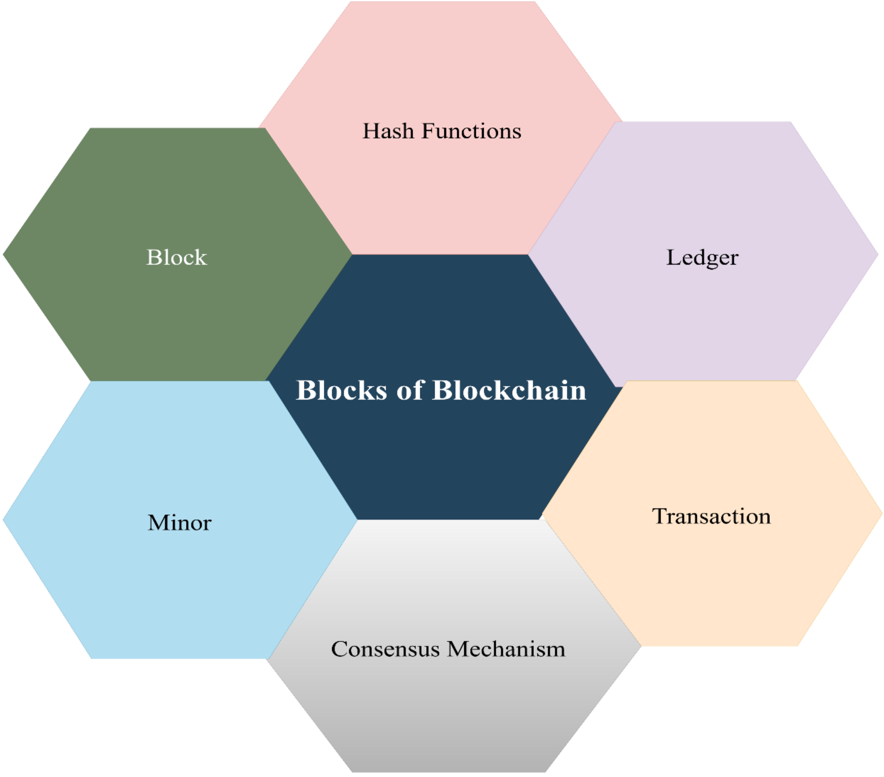

Figure 5. Main Components of Blockchain.

The Ledger: A ledger is a data structure used to store various types of information [46, 50]. It functions similarly to a traditional database but with notable differences. Unlike a database that typically organizes data into tables with rows and columns and employs a relational model for querying and data collection from multiple sources [52-54], a ledger records all transactions made by participating users in a network, both past and present. This ledger is distributed among the network nodes, ensuring that each participant has a copy [39, 46, 50, 52].

Block: A block contains a group of transactions and is linked to the previous block by storing its hash value, creating a chain of blocks [38, 52]. Each block has a unique hash that helps validate its content by ensuring data integrity [46, 53, 55]. The hash function is collision-resistant, meaning it's almost impossible to generate the same hash for different sets of data. This feature is essential for assigning and verifying the hash values of each block [46, 52, 54].

Transaction: A transaction represents the smallest unit of processing, involving a set of transactions between participants that are aggregated and stored in a block [38, 44, 54]. For a transaction to be recorded in a block, it must be approved by most nodes in the network [56]. The size of a transaction affects miners, as smaller transactions are less resource-intensive and easier to validate compared to larger ones. A miner is a computer or entity that solves mathematical problems, primarily hash functions, to generate new blocks [38, 44, 46, 52].

3.2. Blockchain Technologies

Blockchain technology is a distributed decentralized ledger that operates in a trustless environment[50, 56]. It became popular with the development of applications such as Bitcoin. Years later, Ethereum emerged as the second most popular cryptocurrency and application of blockchain technology. Numerous research articles [48, 50, 56] point out that blockchain technology is based on different layers. The primary layers of blockchain technology include the data, application, consensus, and network layers.

- Data Layer: This layer consists of transactions based on a hash function, block, Merkle tree, and digital signature [33, 55]. The data block is divided into two parts as transaction records, organized in a Merkle tree, a binary tree structure that summarizes and securely checks content within a large data set[33.50]. Figure 6 illustrates the structure of the Merkle tree.

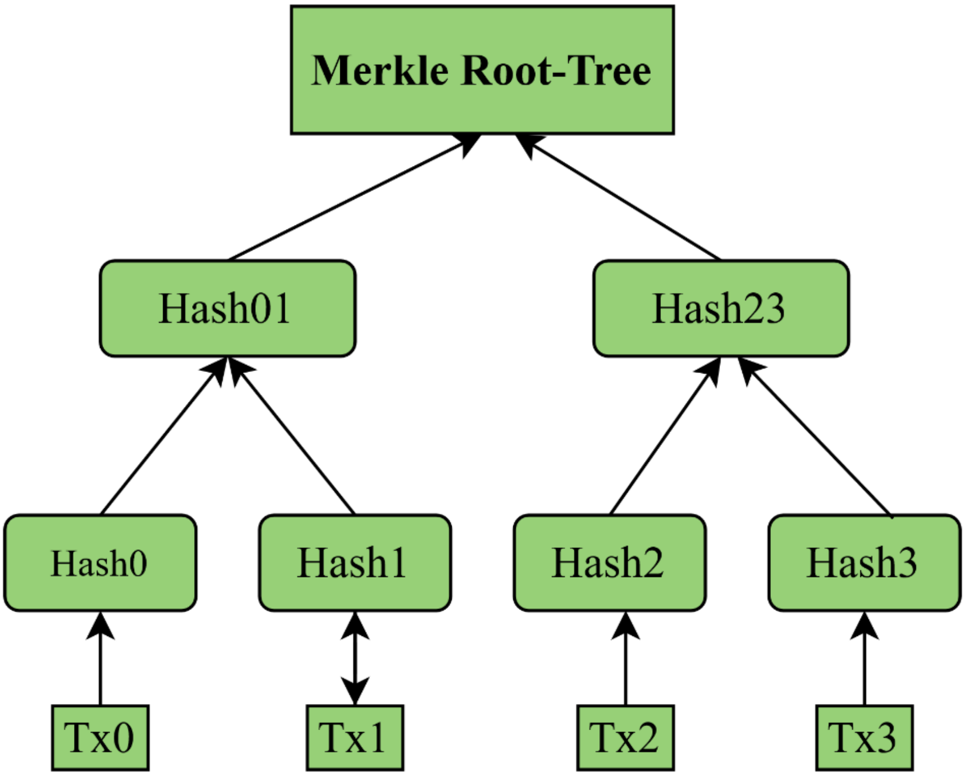

Figure 6. Merkle Tree Structure.

Those Merkle trees are generated by hashing nodes in a kind of for-loop function until one hash is left, called the root hash. Lastly, another component of the data layer is the digital signature which is authenticated digital content that guarantees the integrity of the transaction [33, 47, 48, 50]. It is sometimes complicated to understand the architecture of IoT with Blockchain, Figure 7 visualizes the architecture of IoT and Blockchain in different layers and what are their characteristics in each layer, whereas the bottom of the figure shows the IoT and Blockchain layer and their function in the network.

- Application Layer: known for smart contrast, dApps, and chain code, this layer includes the presentation layer(scripts, user interface, APIs) and the execution layer (smart contracts, chain code). Each transaction in the chain is run from the execution layer, which follows instructions given by the presentation layer [48, 57]. See Figure 7.

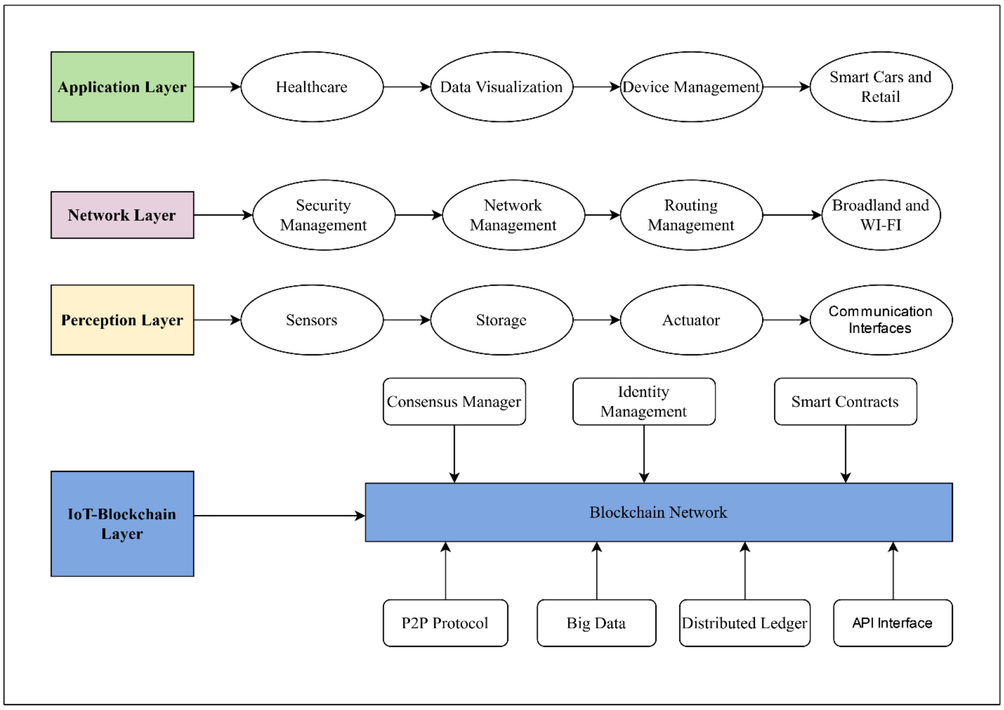

Figure 7. The architecture of IoT with Blockchain.

- Consensus Layer: serves a crucial function in maintaining the reliability of the Blockchain platform [50]. Consensus is a set of rules enforced by this layer itself, which each participant must follow to ensure that generation is done smoothly, making the transactions/block valid [48, 57, 58]. There are different kinds of consensus ways to guarantee Blockchain consistency, including probabilistic and deterministic methodologies. This layer ensures the reliability of the blockchain platform. Consensus rules enforced by this layer guarantee smoother transaction and block generation and validation[48, 50, 57]. Consensus methods include probabilistic and deterministic methodologies[48,50,57].
- Network Layer: Establishes communication between nodes, also known as a peer-to-peer network(P2P)[59]. This layer ensures all nodes are connected to propagate blocks through the network and synchronize the valid state of the blockchain. Figure 8 illustrates the P2P network architecture using six nodes.

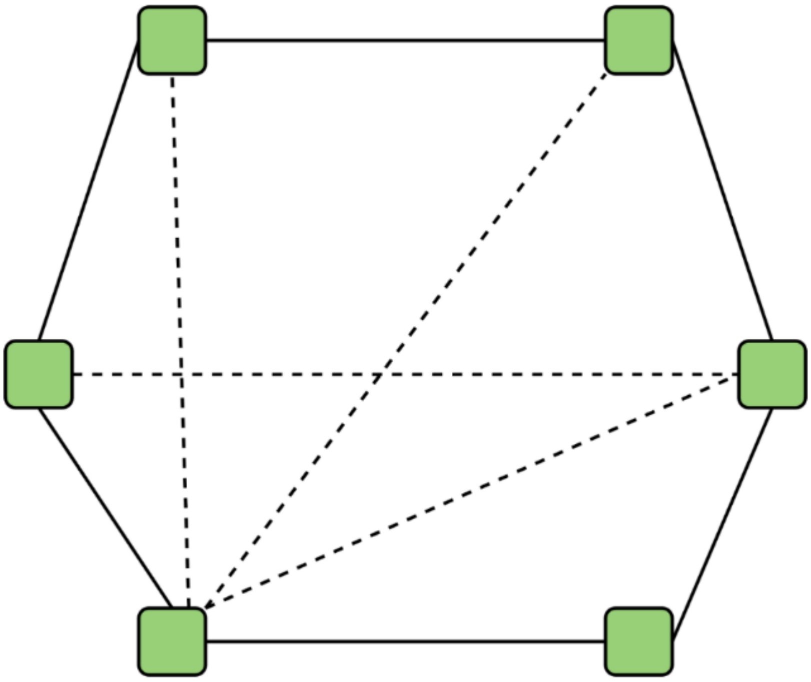

Figure 8. Architecture of Peer-to-Peer Network using six nodes.

This network can be defined as a network of computers where those computers or nodes are shared, and the workload of the network has also been shared with other nodes to achieve the final nodes of the Blockchain, which dose processes transactions and blocks[48, 50, 57-59]. The nodes distributed in this layer are light nodes that store just a header or keys of the Blockchain, which send transactions to the other nodes, called full nodes, which check and validate transactions and store the finished distributed ledger. Table 1 gives an overview of the use of nodes, storage, and validation of transactions.

Table 1. Types of Nodes in Blockchain Network.

Nodes	Full Node	Light Node	Transaction Issue
Storage	Full Blockchain	Block Headers	None
Validator	Yes	No	No

3.2.1. Blockchain Tokenization: A Digital Transformation

Figure 9 illustrates a fundamental concept in the evolving landscape of digital assets: blockchain tokenization, a process of converting real-world assets into digital tokens on a blockchain network,

3.2.2. Key Components of Blockchain Tokenization

There are two key components of blockchain tokenization which categorize the assets of value concerning their properties, into tangible and intangible assets. Further details have been discussed in the upcoming sections for clarity.

- Tangible assets: These include physical items of value such as gold, real estate, and art. Tokenizing these assets on a blockchain offers advantages such as enhanced liquidity, increased transparency, reduced fraud risks, and improved accessibility.
- Intangible assets: These refer to intellectual property, voting rights, and licensing agreements. Tokenization facilitates royalty management, ownership transfer processes fractional ownership, regulatory compliance, and liquidity.

- Tokenization offers range of services such as facilitating royalty management and distribution, streamlining the ownership and transfer processes, and enabling fractional ownership of intellectual property. It can also democratize investments by allowing smaller investments, improving regulatory compliance through transparent record-keeping, and enhancing liquidity for previously illiquid assets. There are different types of tokenization categories available to cater to tokenize different domains such as security Tokens which represent ownership stakes in a company or asset, akin to traditional securities. Crypto and tokenization encompassed two primary types of token, namely utility tokens and currency tokens, as shown in Figure 9. Utility tokens offer access to a product or service, usually on a specific blockchain network. They function similarly to loyalty points or vouchers. Currency Tokens serve as a medium of exchange within a specific ecosystem. They have huge implications for a wide range of sectors in terms of increasing liquidity, improving transaction efficiency, and enhancing the transparency and provability of assets.
- Fungible tokens are based on the ERC-20 standards, which are identical and interchangeable, similar to traditional fiat currencies. Nonfungible tokens are based on the ERC-721 standard and represent unique assets with distinct properties, such as digital art or collectibles. The main quality of the ERC721 token is that many tokens can be maintained by a single smart contract unlikely ERC20 for which one smart contract is required for each token. Examples of NFTs include Ethereum's Cryptokitties and the digital art and collectibles available for purchase on NFT marketplaces such as Nifty Gateway, OpenSea, and NBA Top Shot.

Blockchain Tokenization offers benefits in terms of increased liquidity and accessibility for various assets. Enhance transparency and security through the blockchain's immutable records that cannot be tampered with or changed once posted on the blockchain network. There are fractional ownership opportunities for investors that can be vital in the case of tangible asset ownership. The streamlined processes for asset management and transfer consider currency tokens, while there is huge potential for new business models and financial instruments Figure 9.

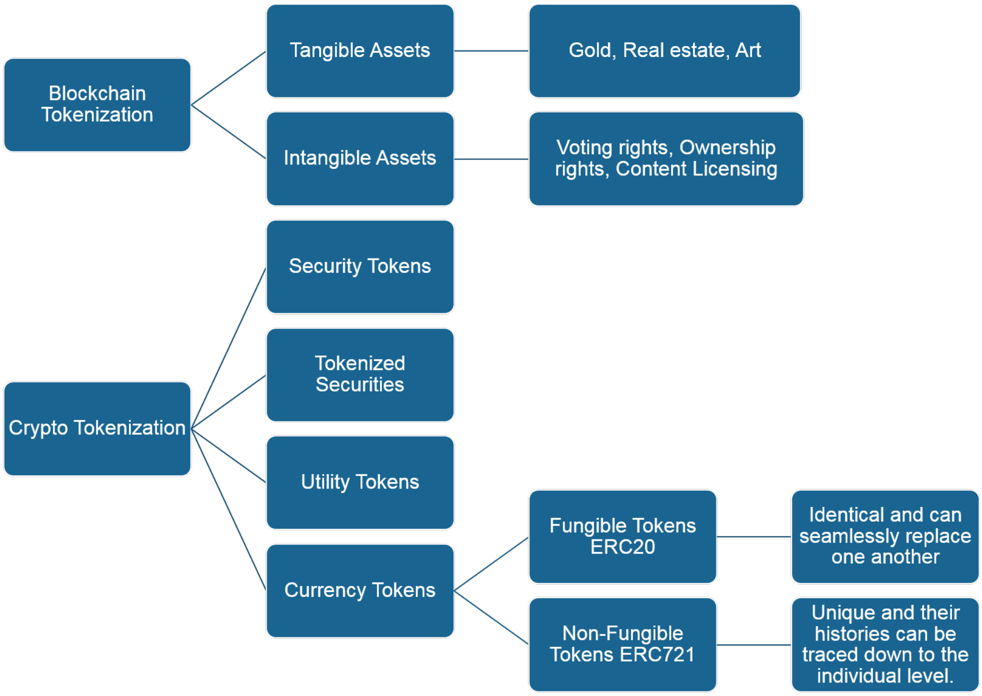
Blockchain Tokenization
Tangible Assets
Gold, Real estate, Art
Intangible Assets
Voting rights, Ownership rights, Content Licensing
Security Tokens
Tokenized Securities
Crypto Tokenization
Utility Tokens
Currency Tokens
Fungible Tokens ERC20
Identical and can seamlessly replace one another
Non-Fungible Tokens ERC721
Unique and their histories can be traced down to the individual level.

Figure 9. Blockchain Tokenization for Assets over Blockchain Network.

3.3. Blockchain Characteristics and Features

Blockchain technology has a robust structure with valuable characteristics such as decentralization, immutability, identity, non-repudiation, transparency, traceability, pseudonymity, anonymity, and security. Figure 10 highlights these salient features.

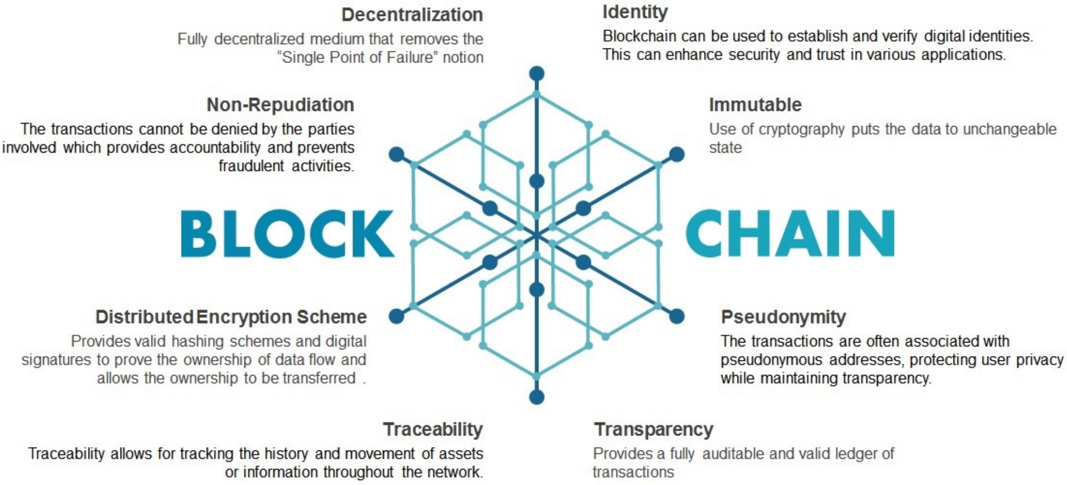
Decentralization
Fully decentralized medium that removes the "Single Point of Failure" notion
Identity
Blockchain can be used to establish and verify digital identities. This can enhance security and trust in various applications.
Non-Repudiation
The transactions cannot be denied by the parties involved which provides accountability and prevents fraudulent activities.
Immutable
Use of cryptography puts the data to unchangeable state
BLOCK
CHAIN
Distributed Encryption Scheme
Provides valid hashing schemes and digital signatures to prove the ownership of data flow and allows the ownership to be transferred .
Pseudonymity
The transactions are often associated with pseudonymous addresses, protecting user privacy while maintaining transparency.
Traceability
Traceability allows for tracking the history and movement of assets or information throughout the network.
Transparency
Provides a fully auditable and valid ledger of transactions

Figure 10. Salient features of Blockchain Technology.

1. Decentralization: This is among the features that characterize Blockchain because it is a decentralized and distributed environment done through P2P communication between nodes as shown in Figure 10 [59, 60]. Decentralization utilizes all users' processing power, decreasing latency and deleting the single-point failure[39, 46, 47, 51, 59]. The network participants can access all data records without being controlled by a central authority [33, 55]. Furthermore, Blockchain utilizes P2p communication, decreasing latency and eliminating single-point failure.
2. Immutability: As shown in Figure 10, a key feature of Blockchain is its ability to maintain transaction integrity through immutable ledgers [51]. Unlike a central authority where data integrity is controlled and maintained by a single entity, Blockchain employs collision-free hash functions to link each block to the previous one, ensuring the integrity of each block's content [33, 47]. Another aspect of immutability is that the blocks in the ledger cannot be altered unless all users agree to the change [39, 46, 47, 51]. Additionally, Blockchain maintains data integrity via collision-free hash functions, making blocks unmodifiable without user approval.
3. Identity: The ownership of an Internet of Things device may shift throughout its life cycle, necessitating an identity management system that is both efficient and secure. There are a lot of characteristics associated with the Internet of Things devices, such as the manufacturer, GPS coordinates, serial number, and kind, all of which require an administration that is trustworthy and secure [91]. In every phase of the life of Internet of Things devices, Blockchain has the potential to be a viable solution that may help reduce the issues that have been discussed above. Through the use of a decentralized and distributed ledger, blockchain can offer approved and trustworthy identity management of linked Internet of Things devices, together with information on their intricate qualities and relationships. At every stage of the Internet of Things device's life cycle, beginning with the manufacturer, the supplier, and the customer, it can monitor the item [90]. Overall, blockchain provides secure identity management for IoT devices through their lifecycle.
4. Non-repudiation: the process of validating is done by using the private keys to utilize the signature of the transactions, which helps in confirming other participants with the equivalent public key. Therefore, each transaction that is signed cannot be refused by the transaction originator [33, 46, 47]. See Table 2 for more details about the decentralized and centralized system and their features.

Furthermore, blockchain uses private key for transaction validation, confirming participant authenticity.

Table 2. A comparison between Centralized Decentralized System.

Features	Decentralized	Centralized
Transaction Mode	Decentralization	Centralization
Resource Consuming	Low	NHigh
Transaction Cost	Low	High
Flexibility	Not Supervised	Supervised
Data Privacy	High	Low
Data Storage	Decentralized ledger	Centralized Database
Information Transparency	High	Low
Cost	Low	High

5. Transparency: all the data encapsulated in the block can be viewed by all participants in the Blockchain, which means every user can access and interact with the Blockchain network while all users have equal rights [46, 47, 51, 56]. Overall, blockchain allows all participants to view data encapsulated in blocks.
6. Traceability: all the transactions saved in the Blockchain are attached with the timestamp, which is recorded when the transaction is executed. This allows each user to quickly verify and trace the origins of historical data items after analyzing the Blockchain data with current timestamps. This enables users to trace back to the original transaction [47, 51]. Furthermore, blockchain records timestamps for each transaction, enabling users to trace data origins.
7. Pseudonymity: each transaction in Blockchain uses a certain level of privacy by making Blockchain addresses anonymous[47]. Blockchain information can help identify scams and illegal transactions that may appear[33, 47]. However, Blockchain can only provide a certain level of privacy since Blockchain addresses are traceable. Overall, blockchain maintains privacy by making blockchain addresses anonymous.
8. Anonymity: All the nodes in the Blockchain interact with the network using the public key that it uses to address the node on the entire network but do not know the real identities[55]. One point is that Blockchain cannot provide proper confidentiality protection because of critical limitations [47, 55]. Overall, blockchain uses public keys for network interaction without revealing real identities.
9. Security: Another advantage of Blockchain technology is its provision of better protection for existing solutions [55, 56]. Using the public key infrastructure, Blockchain offers a secure environment from any attacks. The consensus component provides a trusted method that improves Blockchain security[26, 46, 47]. Overall, blockchain provides better protection through public key infrastructure and consensus mechanisms.

4. Blockchain in Securing Applications

Blockchain technology has gained a lot of attention with a decentralized architecture due to its security, anonymity, centralization, and traceability [26]. The progression of blockchain technology from its inception in 2008 to its anticipated future in 2030 highlights key milestones, influential figures, and emerging trends within the blockchain ecosystem. Blockchain 1.0 was introduced by Satoshi Nakamoto in the year 2008 for the concept of Bitcoin. It was described in a white paper as a peer-to-peer electronic cash system that focused on decentralized transactions without a central authority. The idea led to further implementation of it in its operational form, which gave birth to Blockchain 2.0. Bitcoin's core component was implemented as a public ledger for all transactions in the year 2009 and the era lasted until the year 2011. The foundation was established for blockchain as a technology beyond cryptocurrency.

Vitalik Buterin later proposed the Ethereum platform in 2013, which expanded the potential of the blockchain. It was referred to as Blockchain 3.0 which enabled the creation of decentralized applications (dApps) and smart contracts. His innovation laid the groundwork for various industries to adopt blockchain technology. Blockchain 4.0 in year 2018 later focused on distributed ledger technology and its applications in industries such as finance, supply chain, and healthcare. The emphasis on interoperability, cloud node access, and middleware for seamless integration kicked off the integration of decentralized ledger technology in domains apart from cryptocurrency.

With the emergence of the visionary stage since 2021, the technology encompassing the Metaverse, industrial infrastructure, and a robust blockchain ecosystem leading to Blockchain version 5.0 that focuses on advancements in identity and access control, trust mechanisms, and communication technology that must be anticipated to adapt the security and privacy concerns in the future era. The timeline depicted in Figure 11 highlights the increasing complexity and sophistication of blockchain technology over time. Each stage builds on the previous one, demonstrating the evolutionary nature of blockchain development. The involvement of key figures like Satoshi Nakamoto and Vitalik Buterin underscores the importance of individual contributions to the field.[26, 45, 51]. Blockchain offers high security by using the public key, which offers much more protection against possible attacks. All communications between other devices are done and secured cryptographically, which is provided by Blockchain technology [33, 46]. The cryptography structure on the Blockchain is based on hashing each block and including it in the previous block. This process of hashing blocks forms a virtual chain that connects them and grants a name to the Blockchain [26, 45, 46, 51].

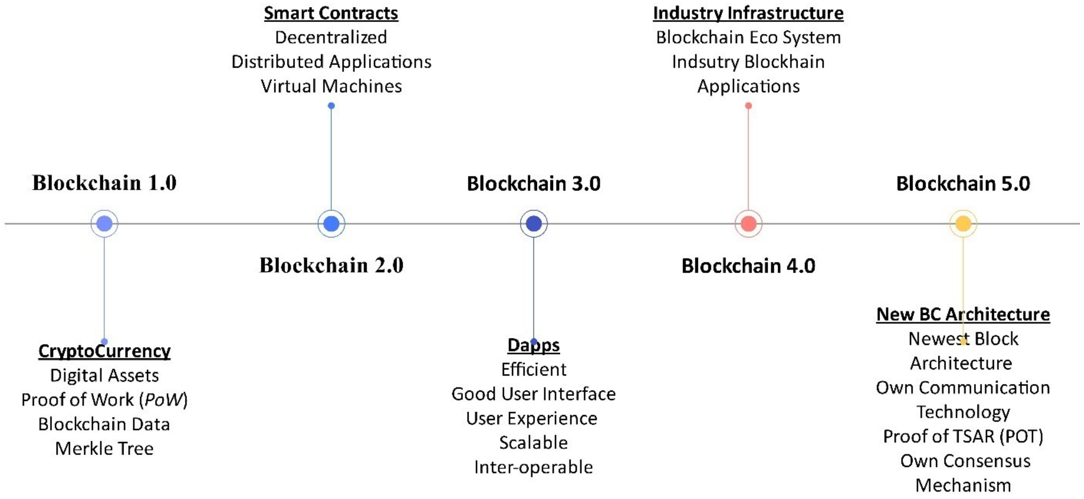

Figure 11. Development of Blockchain.

Blockchain technology can also enhance low-level security, improving remote attestation, where the process verifies whether a device's Trusted Computer Base (TCB) can be trusted. Different proposed Blockchain-IoT applications are related to smart cities and industrial processes. The framework securely integrates intelligent devices and applications, providing smart city applications[26, 33, 61]. Blockchain in securing applications is connected to IoT networks that are promised to address existing technologies; one of the technologies is Blockchain because it first confirms the stored data in the network against all kinds of attacks. Secondly, it provides a secure platform for all devices within the same network, which they can communicate with each other without asking for trust from a central server [39, 46, 56, 62, 63].

Today, we can see that blockchain is being used in many applications, as blockchain technology can improve and help all applications, especially IoT [36, 60]. Blockchain plays a fundamental key in preserving confidentiality when using different applications. This confidentiality is managed by their user key, which for an attacker would be impossible to steal because if he does, it can be used as the public key to steal anything from the user. This excellent management system frees users from managing their encrypted keys. Using the key makes the user feel safer from attacks, as the blockchain offers better security when using the applications [26, 36, 39, 60]. Another essential feature in securing applications is transaction and digital signatures. Transactions in a Blockchain network require a public-private key pair. Peers use their private keys to sign a transaction and the recipient's Blockchain address to deliver it. One transaction example is Bitcoin which uses SHA-256 encryption to drive user addresses [51, 58, 62]. The marketing can also be done between two different blockchains via side-chaining. A sidechain can be defined as a synchronized blockchain running in parallel with an existing blockchain, which we call the main chain [61, 64]. Security and privacy are crucial parts of developing applications. Since IoT is based on Blockchain privacy and security, it is essential to the entire network and platform use[65].

Blockchain is a promising solution when it comes to security applications such that applications with the help of Blockchain enable a much higher security level than the other technologies they have offered up to now [61, 65, 66]. Some of the ideas that have been presented [36, 66] are being proposed as a Blockchain solution to secure applications based on IoT device control and configuration supported by Ethereum. So, we need to remember that devices support those applications when talking about applications. In this case, the private key should be stored on the device, and the public key should be registered as a regular transaction on the Ethereum blockchain. When this enables access, the application on the device can be accessed through Ethernet while using its public key. This proposed approach for using IoT has proved that these features and security can be done using Blockchain [36, 62, 64-66]. Similarly to IoT systems, blockchain also solves problems in securing applications. The structure of a cryptographic blockchain is based on hashing each block attached to another block, which makes that promising for the future.

Blockchain technology improves and secures applications with the help of encryption, and lately, digital signatures have brought blockchain to the market because security is a primary concern for IoT and applications[33, 61, 64]. Establishing a wireless network is increasing in the industrial environment, causing an increase for the measurability and increased chances of wireless communications in the organization [47]. Open wireless channels create issues in IoT and blockchain applications due to safety violations such as jamming, overhearing, and the growth of repeat attacks. However, Blockchain schemes still have security vulnerabilities such as program deficiencies of smart contracts. For the future of secure applications, blockchain nodes should be resource-constrained, as weighted encryption techniques may not be feasible in IoT [39, 47, 56, 62].

4.1. Applications of Blockchain in IoT

There is an increased number of applications for Blockchain in IoT. This is happening because Blockchain technology can help overcome different IoT challenges Blockchain and the Internet of Things (IoT) are two emerging technologies that offer unique capabilities and solutions, when combined, for various industries as shown in Figure 9. When IoT devices record data on a blockchain, it becomes tamperproof, where data integrity is essential, such as healthcare, supply chain, and industrial processes, and therefore a blockchain can create an immutable ledger. On the other hand, IoT devices can share data with other devices securely, and data can only be accessed or modified by authorized parties. Traditional IoT systems depend on centralized servers or cloud platforms, whereas using blockchain, the data can be distributed across a decentralized network, and the risk of system failures can be reduced as well as the need for intermediaries.

The blockchain can establish clear ownership and control over the massive amounts of data generated by IoT devices, and users can also grant temporary access to their data. IoT sensors can update the blockchain with data related to the location, condition, and provenance of products transparently. IoT devices can be used to perform automated microtransactions on blockchain networks.

For example, a connected car could automatically pay parking fees, or electricity bills at charging stations using blockchain-based micro-payments. In addition, blockchain can help establish and manage secure identities for IoT devices, which is crucial because only authorized devices should interact with each other and access specific data or services [26, 33, 48]. On the other hand, the cooperation between blockchain and IoT generates huge amounts of data, which causes an issue of scalability in integrating those technologies at a large scale, in addition to a challenge in the latency of blockchain transactions. Figure 12.

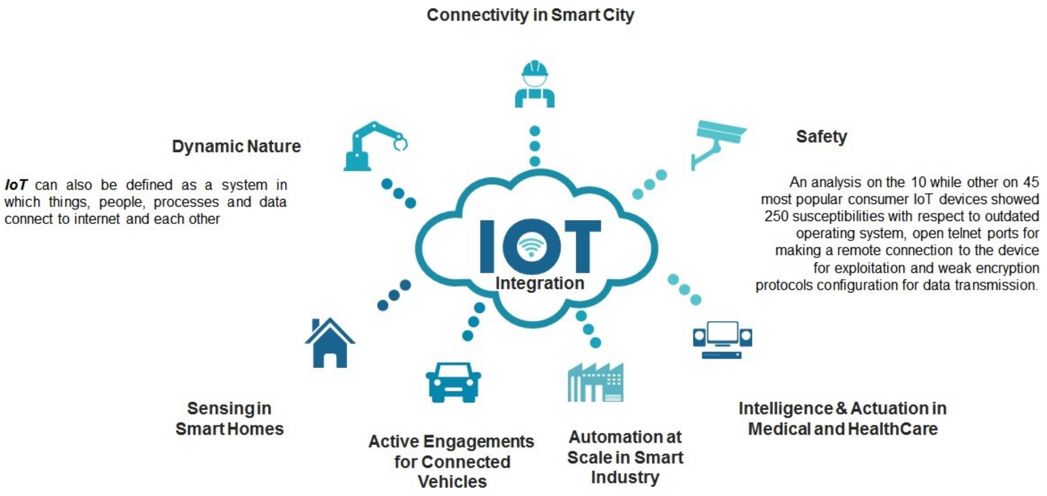
Connectivity in Smart City
Dynamic Nature
IoT can also be defined as a system in which things, people, processes and data connect to internet and each other
Safety
An analysis on the 10 while other on 45 most popular consumer IoT devices showed 250 susceptibilities with respect to outdated operating system, open telnet ports for making a remote connection to the device for exploitation and weak encryption protocols configuration for data transmission.
IOT
Integration
Sensing in Smart Homes
Active Engagements for Connected Vehicles
Automation at Scale in Smart Industry
Intelligence & Actuation in Medical and HealthCare

Figure 12. Internet of Things Applications.

Blockchain technology enhances IoT applications by addressing various challenges, such as tamper-proof data recording, securing data sharing, decentralized data distribution, clear ownership and control, automated microtransactions, and secured identity. Figure 12 illustrates IoT applications and their integration with blockchain. Furthermore, there is a wide range of use cases of Blockchain platforms across various industries such as cryptocurrencies and digital payments (Bitcoin), and smart contracts, whereas blockchain can be used to track the origin and movement of products, supply chain management companies like IBM Food Trust and VeChain are some examples. Other include the food industry, identity verification, voting systems, healthcare data management, intellectual property and copyright protection, tokenization of assets, cross-border payments and remittances, notary services, smart grids and energy trading, digital identity and Know Your Customer (KYC), tokenized securities and investment, insurance and claims processing, gaming and Non-Fungible Tokens (NFTs), and education and credential verification.

1. Smart Manufacturing

   The manufacturing industry is changing a lot and is moving from automated manufacturing to what is called smart manufacturing [25, 26]. Data plays one of the most significant roles in this transmission. There is a vast amount of data generated from different phases of manufacturing, known as the product life cycle and supply, retail, distribution, raw materials, designing, and the sale service[25, 26, 33]. This tells us that all of these cycles provide a substantial amount of data, making data aggregation and analytics more difficult. That is why Blockchain can address the interoperability problem by connecting IoT systems using a P2P network which allows data sharing in all industrial sectors[26, 33, 48]. Blockchain also helps improve security in smart manufacturing since most IoT systems have been centralized. Nodes in Blockchain can install and import the hashes with the help of smart contracts, which are implemented by design. Automated manufacturing is often integrated with decentralized Blockchain, which provides security and confidentiality compared to the centralized system [26, 33, 47, 48]. Overall, blockchain improves security and data sharing in smart manufacturing through decentralized systems and smart contracts.

2. Supply Chain

   The supply chain can be defined as a set of activities, components, and resources that must deliver a product or service to the customers [26, 33]. The final product sent across countries using different manufacturers also consists of forged components. Going through the various manufacturing processes makes those products risky[33, 48]. In this case, deploying an anti-fraud technology in the supply chain costs a lot, but the Blockchain is more affordable and can solve this problem. Blockchain and IoT affect supply chain goals such as speed, quality, costs, risk reduction, flexibility, and more [25, 26, 33, 47, 48, 67]. The trading contains a lawful contract [47] between those who buy and those who sell, with a thriving trade achievement as the product. That situation can be found in the appropriate transport technique for goods, where in this case there is a third party to check the trading procedure [47, 48]. In some cases, there will be an argument that trading the regulatory entity will solve their problems [33, 47, 48]. Overall, blockchain improves traceability and reduces fraud in the supply chain by recording each step of the product lifecycle on the blockchain.

3. Food Industry

   When discussing Blockchain's role in the food sector, we must consider the traceability of food products in ensuring food protection [47, 48]. Having the current IoT is challenging to provide food traceability within the food supply chain. Numerous providers can stipulate different food-producing organizations. Therefore, a need exists to digitize materials from sources in the manufacturing sector. Blockchain technology helps ensure the food's origin and tracking ability [26, 33, 47]. Different sources claim that there is a need for Blockchain to establish a supply chain from farming to food manufacturers, which guarantees the food supply-chain data tractability[25, 47]. Blockchain, combined with food supply chain calls, allows consumers to track the total amount of food manufacturing procedures. The Colombian natural coffee industry is also using Blockchain technology. Also, there is encouragement by the Electronic Product Code to use IoT tags and Blockchain, which can stop information interference and confidentiality revelation [25, 26, 33, 47, 67]. Overall, blockchain ensures food traceability and safety.

4. Healthcare

   Healthcare is rapidly evolving with the integration of digital technologies, which promise to revolutionize clinical data management and improve both outcomes and processes effectively [47, 48]. As one of the most pressing socioeconomic issues due to population growth [26, 68, 69], the healthcare sector faces significant challenges, particularly with limited hospital resources. One key advancement is the use of wearable devices, which enhances remote healthcare services both in clinics and at home [26, 33, 47]. For example, patients can now remain at home while using wearable devices that monitor metrics like heart rate and blood pressure [26, 33, 48]. These devices enable doctors and nurses to access healthcare data anytime and anywhere via the network. However, this data also raises concerns regarding security and privacy [26, 47, 48]. Blockchain technology offers a potential solution by ensuring the privacy and security of healthcare data stored on cloud servers and managing this data effectively [68, 69]. Medical sensor data can be collected and transmitted automatically to the system through smart contracts, enabling real-time patient monitoring [26, 33, 47, 48, 67]. By implementing these measures, Blockchain can address privacy and security issues in healthcare data management.

5. Internet of Vehicles

   Internet of Vehicles integrates vehicle-to-vehicle networks, vehicle-to-infrastructure, vehicle-to-roadside networks, and vehicle-to-pedestrian networks [33, 48]. The automotive sector is leading technically superior branches by scaling from electric, hybrid, and self-driving smart cars in the Industrial Internet of Things in combination with IoT-linked cars[26, 33, 47]. Securing message transmission and execution are some of the challenges that come with the decentralization, heterogeneity, and trustworthiness in the Internet of Vehicles. If Blockchain and the Internet of Vehicles are integrated is going to solve those challenges[25, 26, 47]. Blockchain technology conserves the energy and information interactions between electric and hybrid electric vehicles using a smart grid. Unmanned Aerial vehicles today have a communication network that lacks a wireless communication network that is used to deliver product items and acquire real-time traffic flow data. Integrating Blockchain technology with the UAV network will help the confidence in UAVs[25, 26, 33, 47]. Much development on an autonomous platform based on the Ethereum Blockchain is used to provide trust management on UAVs. They are a developer working on developing a blockchain-based system to serve privacy and security for UAV data[33, 67, 70]. In general, blockchain integration will secure communication and data exchange in vehicular networks.

6. Smart Grid

   Renewable Energy resources, the role of which is the energy consumers from the pure ones to prosumers who can generate energy and not just consume [33, 47]. The energy traded between consumers and prosumers is called P2P energy trading or between peers [26, 47]. With regard to energy trading, the challenge is to ensure and trust that energy trading between two trading parties in the environment has been distributed. Blockchain plays an essential role in ensuring P2P energy trading[47, 68]. One of the suggestions is to develop secure trading energy based on the blockchain consortium. This can reduce the trading cost because we do not go through a central broker via the distributed consensus of Blockchain[26, 33, 47, 67, 68]. They also received more suggestions on how to use blockchain to protect confidentiality in energy trading using decentralized smart grid systems. In general, blockchain secures P2P energy trading and protects confidentiality in decentralized smart grids.

4.2. AI in Blockchain

Artificial intelligence (AI) can be applied to various aspects of blockchain technology to enhance its functionality and utility. [80] AI algorithms can analyze smart contracts deployed on a blockchain to identify vulnerabilities and potential problems. It can monitor blockchain transactions in real time to detect fraudulent activities, such as double-spending, phishing attacks, or suspicious transaction patterns. AI can be used to develop advanced cryptographic techniques that enhance privacy on blockchain networks. AI algorithms can validate data stored on the blockchain by cross-referencing it with external sources to ensure the accuracy and integrity of data entries.

AI can analyze transaction patterns and user behavior on the blockchain to detect unusual or fraudulent activities. Its algorithms can provide insights and recommendations for decision-making within Decentralized Autonomous Organizations (DAOs). It can optimize consensus mechanisms and network protocols to address scalability challenges in blockchain networks. Natural Language Processing (NLP) algorithms powered by AI can analyze text data on the blockchain, such as transaction memos, which is useful for sentiment analysis. AI can optimize resource allocation and also ensure efficient use of computing power and energy. Predictive AI models can analyze market data and predict the price movements of cryptocurrencies and tokens. In general, AI can enhance various aspects of blockchain technology, including smart contract analysis, transaction monitoring, advanced cryptographic techniques, data validation, fraud detection, decision making in DAOs, resource optimization, and price prediction. The convergence of AI and blockchain drives significant technology advancements and various industries.

1. Convergence of AI and Blockchain;

   The convergence of AI and blockchain [81] represents a powerful synergy that has the potential to drive significant advances in technology and various industries.

- AI can improve several aspects of blockchain technology, such as security, supply chain, data storage, authenticity validation, healthcare, and financial services. ;
- AI protocols can be integrated into blockchain in several formats:

  Smart contracts on blockchain platforms can be used to automate and execute AI-related tasks to manage AI training, data transactions, and payments. Table 3 presents protocols and platforms for smart contracts in AI applications.

Table 3. Protocols and Platforms for Smart Contracts in AI Applications.

Protocols and Platforms	Specific Use Cases for Smart Contracts in AI Applications
Ethereum (ERC-20 and ERC-721)	Use ERC-20 tokens to represent access to AI services or datasets. Create decentralized AI data marketplaces where data providers tokenize their datasets as ERC-721 NFT
Binance Smart Chain (BEP-20)	Allow token holders to vote on AI model updates, data access policies, and funding decisions. Issue BEP-20 tokens to represent AI services
Chainlink	Allow token holders to vote on AI model updates, data access policies, and funding decisions. Issue BEP-20 tokens to represent AI services
Avalanche (AVAX)	Integrate Chainlink's decentralized oracles to fetch real-world data for AI applications.
Harmony (ONE)	Avalanche (AVAX) Utilizing AVAX tokens for transactions. Smart contracts ensure secure data exchange and compensation
Polygon (formerly Matic)	Create decentralized governance structures on Polygon for AI decision-making

Blockchain-based AI data marketplaces are designed to facilitate secure and transparent data sharing for AI development and research. Table 4 presents some protocols and platforms commonly used for creating blockchain-based AI data marketplaces.

Table 4. Blockchain-based AI Data Market Places for AI Applications.

Blockchain-based AI data Market Places	Specifications
Ocean Protocol	It allows data providers to publish datasets as "data assets" and provides tools for data access control and pricing
Bluzelle	It allows data owners to share encrypted data securely.
IoTeX	It provides a scalable and secure solution for storing and accessing data in blockchain-based AI applications.
IOTA	It is designed for the Internet of Things (IoT) but can be adapted for AI data marketplaces.
Streamr	It provides a scalable and seamless environment for data transactions.
Polygon (formerly Matic)	It is built on Ethereum, and Streamr's DATAcoin (DATA) is used for transactions.

4.3. Blockchain Tokenization for IoT-Enabled Smart Assets (IoT)

The application of blockchain technology to create unique digital representations, or tokens, for Internet of Things (IoT) devices is a hot research topic these days. By tokenizing IoT assets, the aim is to enhance their management, security, and value proposition. This approach takes advantage of the decentralized and immutable nature of blockchain to establish secure ownership, track asset lifecycle, and facilitate efficient data exchange between IoT devices and other systems. In general, tokenization of IoT assets improves their management, security, and value proposition by leveraging the decentralized and immutable nature of blockchain.

doi:10.20944/preprints202409.1193.v

4.4. Non-Fungible Tokens (NFTs)

Unlike their fungible counterparts, non-fungible tokens (NFTs) possess distinct, indivisible characteristics. Each NFT carries unique properties or metadata differentiating it from others. Although commonly associated with tangible assets such as art, real estate, or collectibles, NFTs can theoretically represent currency. However, the inherent divisibility and interchangeability required for monetary transactions pose challenges for NFT-based currencies. To function as a currency, NFTs improve specialized mechanisms for fractional ownership and divisible units, an area currently underexplored. In general, NFTs have unique properties and can represent tangible and intangible assets. Although challenges remain, they offer potential security and authentication in IoT applications.

4.5. NFTs in Security and Authentication

The distinctive traits of NFTs, including unique digital identities and immutable records, position them as potential game-changers in security and authentication. Their application in domains such as supply chain management, access control, and decentralized identity verification is evident. Nevertheless, while the potential of NFTs for enhancing IoT security is recognized, a significant research gap persists.

5. Requirements for Integrating Blockchain into IoT

Integration of Blockchain into IoT can solve many security problems. Securing data transfer in the IoT network is the primary challenge, which is why Blockchain has an advantage over it [33, 39]. As discussed in the previous section, blockchain provides an ultimate solution to trust and many security problems [39, 68, 70]. Even though it offers many solutions, since it is still a new technology, integrating Blockchain into IoT systems is still challenging, and that's why some requirements must be met. Those requirements must be fulfilled to provide high distribution performance and scalable IoT networks[51, 53, 71, 72]. In general, to successfully integrate blockchain into IoT, several requirements must be met, including privacy, access control, security, efficiency, data integrity, authenticity, adaptability, decentralized data storage, low latency, resilience, and ease of deployment. The goal of all of this is to successfully integrate blockchain into IoT. Table 5 compares IoT and blockchain technology based on these characteristics.

Table 5. A Comparison Between IoT and Blockchain Technology.

Items	IoT	Blockchain
Privacy	Lack of Privacy	Ensures the privacy of the participating nodes
Scalability	Large number of devices	Scales poorly with Large network
Bandwidth	Limited resources and bandwidth	High consumption
Resources	Resources restricted	Consumes lots of resources
Latency	Low Latency	Block mining it consumes lots of time
Security	Security is an issue	It is more secure

- Privacy: Privacy is one of the basic requirements for this integration to be possible. The blockchain should guarantee the privacy of the user's data when integration is performed [33, 51]. This makes a huge difference in the network as users are guaranteed that their information and data are not being tracked and stored in a decentralized environment[39, 51, 70].
- Access control: For the users, we should ensure that access policies and regulations in-network and outside of it must be regulated in viewing and sharing the users' data[51, 53, 71]. This ensures that any user who wants to access that information should go through some rules and regulations.
- Security: The leading reason for integrating blockchain into IoT is to enhance the security of the IoT network through new design architectures. Data confidentiality and security must be

addressed when integrating an IoT system [39, 51, 70]. Since blockchain is decentralized, it is promising that it will make a massive change in IoT development.

- Efficiency: The integration system should offer minimal performance even though the nodes are present in various sub-systems within devices [51, 53, 71]. This minimal performance certainly increases the efficiency of the device in the system.
- Data integrity: Keeping the data safe and secure is among the issues IoT devices are mostly facing [39]. Integrating Blockchain into the system should have reliable data to ensure that data consistency, accuracy, and security can stay in the decentralized environment[39, 51, 53]. As we have said before, blockchain technology fulfills the requirement.
- Authenticity: Data Transfer in the network is one vulnerability that each user can be exposed to. Data transactions must go through authentication and validation in the system and decentralized computing environment[39, 51, 70, 72].
- Adaptability: Network architecture should be flexible and adapt to the changes happening in the environment. It is done by matching the customers' pools and their demands [39, 51, 53]. This also can raise several complexities in future applications by maintaining acceptable system throughput levels, security, and delays.
- Decentralized Data: The integration architecture should extend the storage size of IoT devices based on the storage capabilities of blockchain technology, which is more accessible in handles[51, 53, 70].
- Low Latency: The integration of the system should consider delays during computation processes, the same as data transmission from one node to another[39, 53]. To keep low latency, it is essential to identify what computation tasks are involved, such as from architecture. It should be decided whether they should be performed at the end of devices, in the dew server, or another layer [39, 51, 72].

Other requirements should be fulfilled, such as resilience, where tests, if a node fails, should not affect all of the system[70]. Another is the deployment, which says that all nodes in the system must join the network without complications other than configurations. Blockchain technology gives a better solution to the problems faced by IoT systems[39, 68, 70, 71]. In addition, smart contracts can be important in the integration of blockchain in the IoT. Smart contracts can be defined as self-executing codes that enable the system to enforce a contract using certain trigger events, while a computerized process is performed in Blockchain[39, 51, 70, 72]. This blockchain is automatically triggered when a pre-set is agreed on data recorded as a transaction in the blocks. Those characteristics of operating in a digital environment show the ability to create different algorithms and programs that can be executed that perform a specific action without humans following certain pre-set terms where all parties agree.

Smart contracts are programs that have unique addresses and are embedded in the blockchain [39, 51, 68, 71]. Smart contracts are independently and automatically executed on every node on the blockchain. All nodes run as a virtual machine in the blockchain network while the whole system operates as a single computer[33, 39]. The blockchain consensus protocol enforces the execution of the nodes. Smart contracts by many Blockchain but first has been adopted in Ethereum Blockchain. Ethereum is a public, distributed operating system and Blockchain-based computing platform and the second-largest cryptocurrency in Blockchain after Bitcoin [49, 51]. Ethereum was launched in 2015 as a programmable blockchain, which means that programs can use it to build new types of decentralized applications[39, 49, 51, 70].

The decentralized programs built on the Ethereum blockchain are predictable, reliable, and combined with the benefits of blockchain technology and cryptocurrency [51]. First, smart contracts are uploaded to Ethereum, which runs automatically as a program. Then, the node used in the smart contract must pay an execution fee, also known as a 'gas fee' to perform the execution. The smart contract also has associated code and data storage[33, 39, 51]; the code is written in a high-level language called "Solidity" that is used to support Ethereum execution and to write smart contracts. Smart contracts were first proposed as a solution in a comprehensive system combining IoT and

Blockchain[33, 39, 51, 68, 70, 71]. The result is an autonomous system that pays for whatever is consumed and provides IoT resources. Another aspect of smart contracts is managing and recording all IoT interactions while delivering reliable and secure processing tools that make an action trusted. That's why smart contracts can securely model the logic in supporting IoT applications[49, 51, 68].

6. Implementation/ Integration of Blockchain and IoT

Blockchain technology is a tool that allows each transaction to be verified in a secure, distributed, and transparent ledger [63, 70]. Compared to cloud computing Blockchain, it uses the P2P setting, which is decentralized, where it keeps and processes the information, and it does not use the usual client-server architecture. As we know, Blockchain has protocols to construct knowledge as chain blocks [39, 63, 68, 70]. In the P2P architecture of blockchain, each peer in the network must depend on four functionalities: wallet, routing, services, and storage [62, 73]. The blockchain technology for each transaction uses nodes, which makes the blockchain technology secure. In Table 6 below, we illustrate the analysis of the most common type of Bitcoin. In this case, routing is an integral part of the Bitcoin network, each node in the P2P network must have a function for each transaction and block propagation [63, 70, 71, 74].

Table 6. Functionalities Node in the Bitcoin Network.

Node	Storage	Wallet	Routing	Mining
Bitcoin Core	Yes	Yes	Yes	Yes
Solo Minor	Yes	No	Yes	Yes
Full Node	Yes	No	Yes	No
Light Wallet	No	Yes	Yes	No

In some of the nodes in Table 5, in this case, the Bitcoin example, the storage function is needed to keep a copy of the chain, whereas the entire chain is stored in the case of full nodes. To do the transaction for a different reason, we must use the wallet service, which plays an important role in providing security in the transaction [62, 73]. Lastly, it is mining, its main characteristic being the building of new blocks utilizing PoW. Proof of work, also known as mining, is performed by some nodes, they are called miners. Moreover, miners receive rewards for each newly generated Bitcoins, and they charge fees for each transaction[39, 63, 70]. The main objective of mining is to strengthen trust in the blockchain network. When the miner finishes their job, the new block gets the right to be published in the network. The position of peers in the network is to verify the validity of the block before it is added to the chain. Also, blockchain can be divided into different branches. The reason why this happens is that the blocks in the network are generated simultaneously[39, 51, 62, 63, 68, 70, 73]. The objective of applying Blockchain technology in IoT is been illustrated in Figure 13.

The concurrency and the intensity of block generation create a unique, distributed technique. Blockchain is secure because the malicious node that intends to corrupt or modify the block in the Blockchain would run out of resources by the trusted miners. After all, the complexity is very high in block generation; that's why the trusted branch of blocks would invalidate the block generated by the intruder. This complicates the life of a hacker. The reason is that adding a modified or corrupted block to the chain is needed to solve the PoW before the rest of the miners in the network [39, 49, 51, 68, 70].

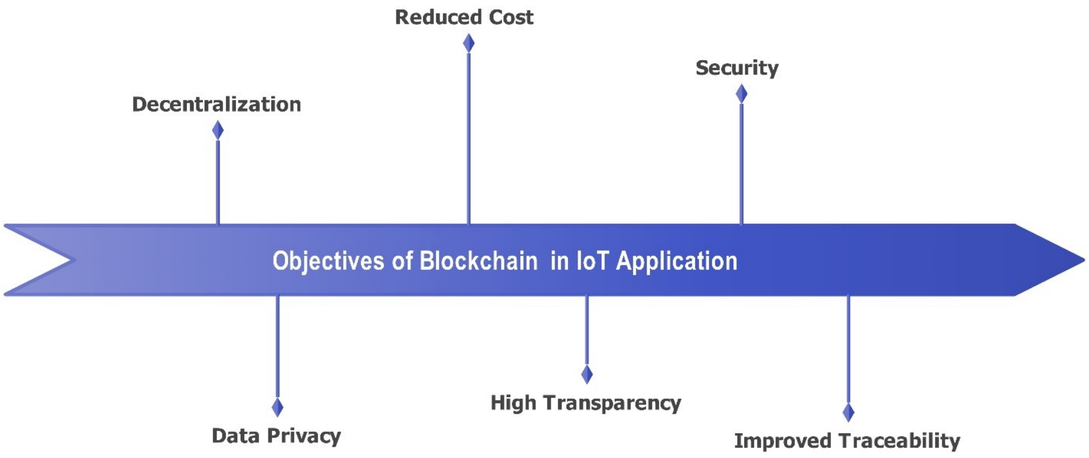

Figure 13. The Objective of Blockchain in the Internet of Things.

6.1. Blockchain Integration with the IoT

The IoT is revolutionizing the world by creating more interconnected devices that automate and optimize manual procedures, generating increasing amounts of data that automated and optimize manual procedures, generating increasing amounts of data that improve people's lives[63,70]. Previously, cloud computing was the only option that provided IoT devices with essential services, allowing them to process and analyze information and convert it into real-time services. with the growth of IoT devices, challenges such as the open data paradigm, centralized architecture, and lack of confidence have emerged[71,74,75].

Blockchain improves IoT technology by providing shared resources in a reliable, reliable and traceable manner. Data sources can be securely specified and kept unchanged, as many IoT devices share information securely[39,63,70]. This knowledge or information can help people build smart applications that improve management and lifestyles. Figure 14 illustrates the model for integrating Blockchain into IoT. Overall, blockchain technology is a tool that allows each transaction to be verified in a secure, distributed, and transparent ledger. Compared to cloud computing, blockchain uses a P2p setting, which is decentralized, keeps, and processes information without the usual client-server architecture. Blockchain protocols construct knowledge as chain blocks. In the P2P architecture of the blockchain, each peer in the network relies on four functionalities: wallet, routing services, storage, and mining.

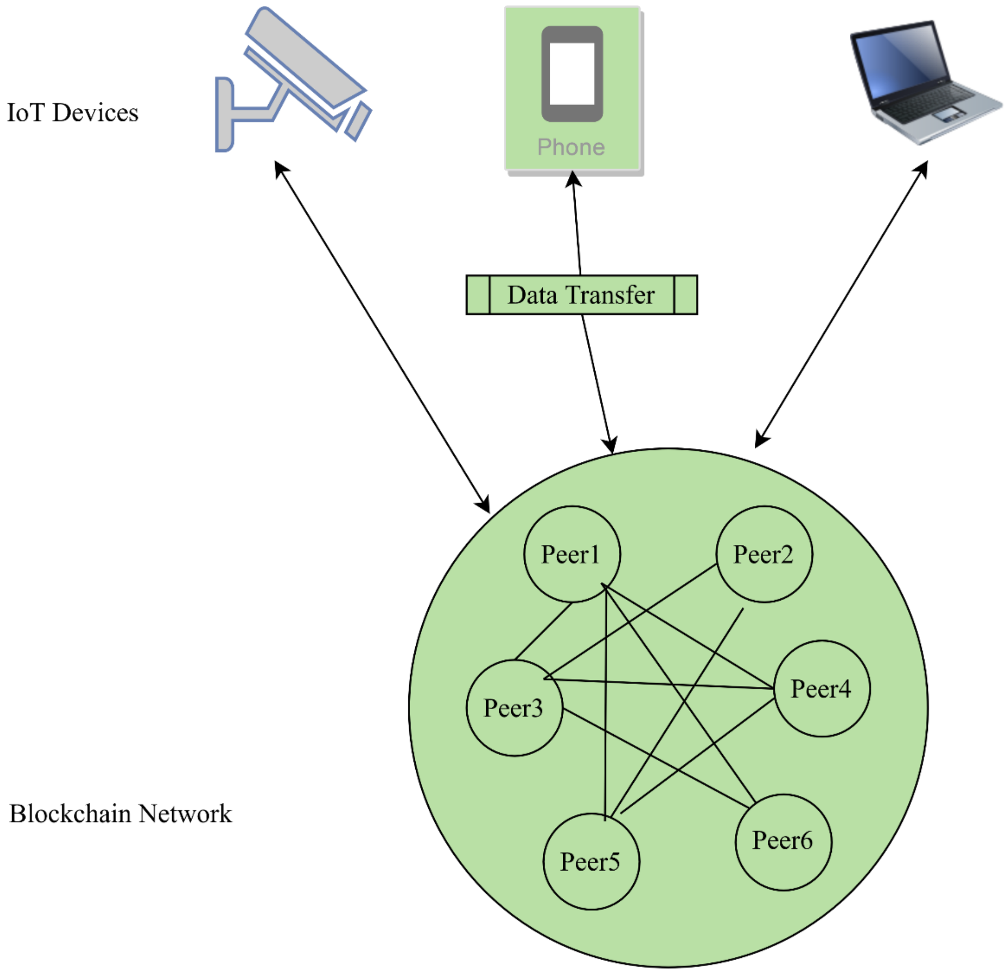

Figure 14. Blockchain-IoT Integration Model.

Additionally, Blockchain actively enhances IoT services through the following methods:

- Security – The way the IoT devices will be able to achieve full benefits by storing information and securing communications in the way they do it is through using transaction property in introducing Blockchain technology[63, 70]. Also, another critical method in the Blockchain is used to validate the message exchange through different devices. The way how this is done is by using smart contracts. Expect smart contracts, which play an essential role in Blockchain technology. Also, the optimization of security of protocols that are applied to IoT applications [39, 63, 68, 70]. Overall, IoT devices achieve full benefits by storing information and secure communications using transaction properties in blockchain. Validating message exchanges through smart contracts plays a crucial role. Security protocols optimized for IoT applications also help.
- Traceability and reliability – Blockchain can improve IoT applications and devices by distributing information and keeping it unchanged[63]. Moreover, Blockchain also can help us to verify data authenticity and ensure the data presented remains untouched while data is in transit. The data is traced to identify and protect it. Blockchain technology enables sensor data accountability and traceability[49, 51, 68, 71]. Reliability is one of the key aspects to bring to IoT. Overall, blockchain improves IoT applications distributing information and keeping it unchanged. It verifies data authenticity, ensuring data remains untouched during transit. Sensor data accountability and traceability are enabled through blockchain.
- Decentralization and scalability – The main point that leads to failure phenomena and bottlenecks happens in the client-server architecture. That is why cloud computing will be eliminated

once it is shifted to P2P, decentralized, and server for utilizing Blockchain technology[63, 70]. Additionally, controlling information generated by IoT applications storage and processing by powerful is prevented. Each shift done by Blockchain by default improves fault tolerance and permits idealistic IoT scalability [49, 51, 63, 70]. Overall, blockchain P2P decentralized and server-less architecture prevents failures and bottlenecks common in client-server models. This shift improves fault tolerance and allows ideal IoT scalability.

- Identity – Each device in Blockchain technology is identified uniquely. Every additional frame sent and used to the network is immutable; this includes the sender's address, making it hard to spoof the Blockchain devices[39, 68]. This is a good advantage since it will prevent spoofing attacks that may be present in IoT and other wireless devices[39, 51, 68]. Overall, every device in blockchain is uniquely identified. Immutable frames sent to the network include the sender's address, preventing spoofing attacks.
- Service market – Transactions in Blockchain technology are done anonymously, and those transactions are done between peers because they are decentralized; they can eliminate the authorities, which would speed up the creation and the sharing of newly created business applications. In addition, it is not convenient to deploy microservices to allow the dispatching of small payments safely [62, 63, 70]. Overall, blockchain's anonymous transactions between peers eliminate authorities, speeding up business application creation and microservices deployment.
- Autonomy – Internet of Things applications and devices can also benefit from Blockchain, which eliminates the dependency on the servers, spreading decoupled device-agnostic applications[49, 51, 70]. Overall, IoT applications and devices benefit from blockchain's elimination of server dependency, spreading decoupled device-agnostic applications.

Integrating Blockchain requires deciding where interactions occur, choosing between insider IoT, hybrid design, or solely blockchain[71, 74]. For computing, a new layer between cloud computing and IoT devices, plays a significant role in hybrid approaches. Below is the discussion of the three alternatives:

1. Inside IoT – The Inside IoT approach can be the fastest regarding latency and security because you can use it even offline, and Internet of Things devices can communicate with each other, including routing mechanisms and discovery. Not all Internet of Things data is stored in Blockchain, but IoT communicates with each other without using Blockchain. This can be an excellent example because it can be helpful to reliable IoT data where IoT interacts with each other using low latency [39, 63, 70]. Overall, this approach offers low latency and security, enabling offline communication between IoT devices, Data is not stored in blockchain but directly shared among IoT devices.
2. Hybrid – The hybrid design is where only part of the interactions and data occur in the Blockchain, and the other part is directly shared between the IoT devices. A challenge in the hybrid method is choosing which intersection to go to using Blockchain, which provides a way to decide the run time [62, 73]. An excellent example of this approach is integrating Blockchain and the Internet of Things technologies because it makes use of all the benefits of Blockchain and of real-time IoT interactions. Using the hybrid approach combines fog computing and cloud computing to complete the limitations of Blockchain and the IoT [39, 63, 68, 70]. One of the examples is fog computing, which includes fewer computationally limited devices such as gateways. It has the potential where mining can take place like the other initiatives using IoT devices. Figure 15 explains in detail the infrastructure of the Internet of Things and how that works. On one hand, the cloud's features make communication possible and on the other hand, it is the end users who can communicate with the cloud. Overall, part of data and interactions occur in blockchain, while the rest are shared real-time IoT interactions. Fog computing and cloud computing complement the limitations of blockchain and IoT.

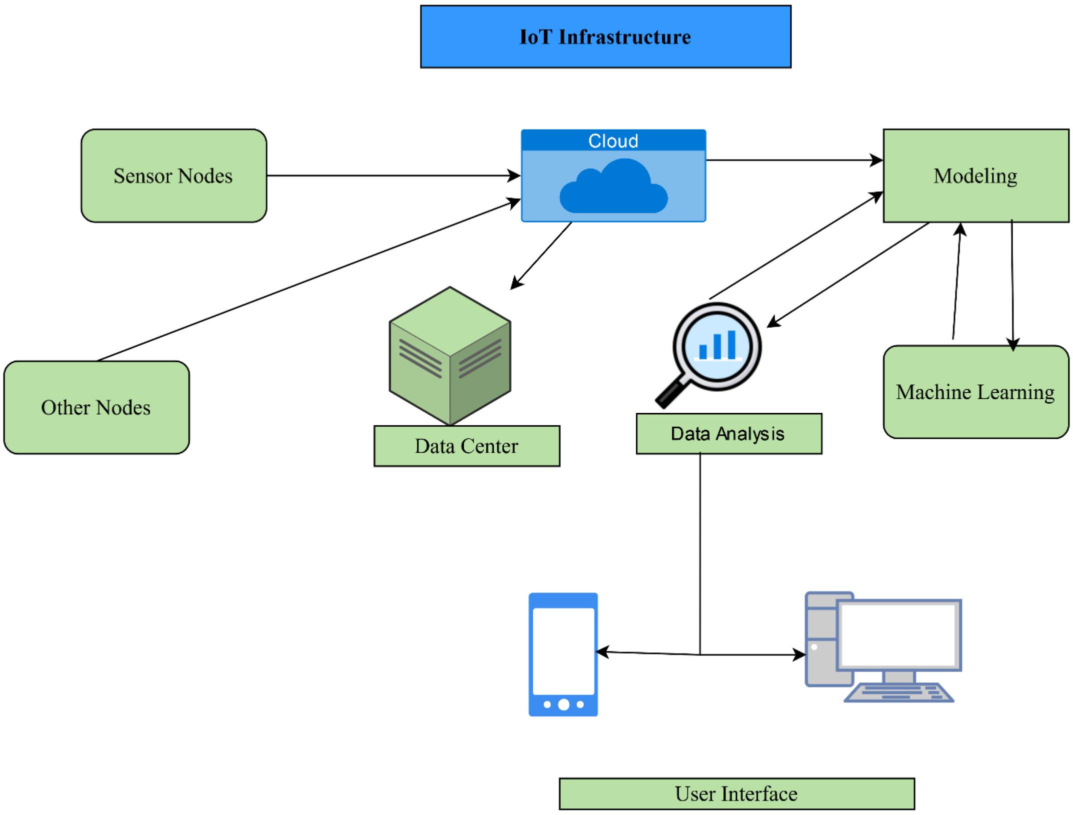

Figure 15. Internet of Things infrastructures.

3. Blockchain-IoT – All transactions are recorded on the blockchain, enabling an immutable record of interactions [68]. This method provides the right to choose an exchange that can be traceable because your details would be queried on the Blockchain, which can increase the autonomy and presence of IoT [51, 63, 68, 70]. The IoT takes advantage of this approach because it fulfills its services. On the other hand, recording all the interactions in the Blockchain can involve changing and increasing bandwidth and data, which is the biggest challenge for Blockchain. Compared to the blockchain, the data in the IoT associated with these transactions are stored in the blockchain [39, 68, 70]. In general, all interactions occur via blockchain, providing an immutable record. This method ensures traceability and autonomy, but requires increased bandwidth and data handling capabilities.

6.2. Challenges in a Blockchain–IoT integration

Integrating Blockchain into IoT is challenging due to the differing sizes of blockchain data and IoT user data. The size of blockchain data, such as Ethereum and Bitcoin, ranges from 250 GB to 1 TB, which is large compared to IoT devices[68, 74]. This discrepancy poses challenges to fully implement blockchain in IoT devices. One solution is using cloud computing to store block data, with only hash chains stored in IoT devices. Furthermore, the use of applications in IoT technology motivates society to use Blockchain to secure data transfer in IoT networks and to use it as an advantage, as it solves many security-related problems[34, 68, 76]. In addition, a transaction on a blockchain network is signed digitally. Furthermore, it is necessary to equip IoT devices to operate and use a Blockchain because of its advantages[51, 68, 74]. Before deeper analyzing the integration of Blockchain in IoT is good to go over the challenges and concerns that come from this integration. Figure 17 Some of the challenges are:

- Size of Blockchain: There is a significant difference between the size, the fixed and operational size of user data, between what Blockchain offers and the Internet of Things [34, 68, 76]. The size of Blockchain examples varies based on the Blockchain we are using; for example, the size of Blockchain-based technology like Ethereum and Bitcoin have the size of 250 GB or 1 TB until now, which is a large size if we compare it with IoT devices [38, 68, 70, 74]. This can be a challenge between those technologies since there is a vast difference in the size they offer. With space or storage, IoT devices impossible to process data, which can be challenging when integrating Blockchain in IoT [38]. Moreover, size can be an issue when blockchain is integrated into IoT and becomes an obstacle to fully deploying Blockchain in IoT devices [34, 68, 70, 76]. However, there are many ideas on how challenges can be solved. To Solve these challenges, one of the promised ways is cloud computing [38, 68] can be used to solve the problem with storage. The way to do it is by storing block data on the cloud, where only some parts and light data as the hash chain would be held in IoT devices [39, 68, 70, 71]. Thus, this is the best solution regarding the size of Blockchain and IoT, even though this can become a conflict since cloud computing is centrally controlled and alternatively, Blockchain is decentralized [34, 51, 68]. Figure 16.

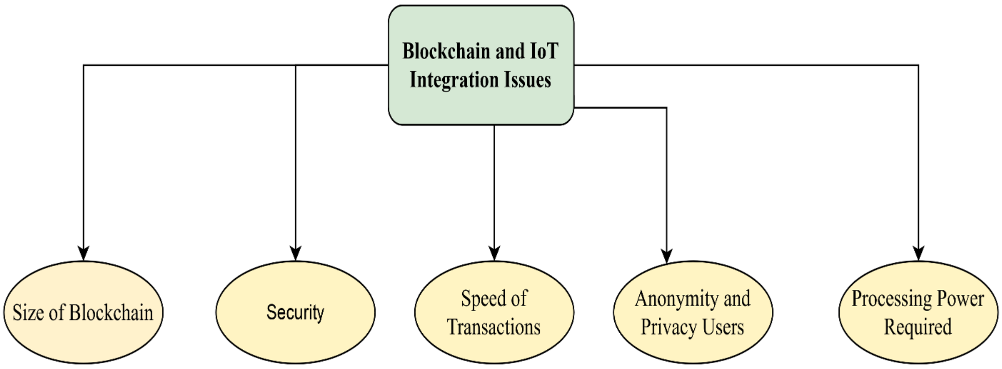
Blockchain and IoT Integration Issues
Size of Blockchain
Security
Speed of Transactions
Anonymity and Privacy Users
Processing Power Required

Figure 16. Integration issues of IoT and Blockchain.

- Security: IoT applications face security issues, including device performance and high heterogeneity. Blockchain is viewed as a solution, but integration brings reliability concerns for IoT-generated data. Blockchain guarantees data integrity unless corrupted data originates from IoT devices[38, 70]. Moreover, there is an increased number of attacks on IoT networks, and all those attacks have a terrible effect, making it necessary to develop and use technology that makes devices more secure. Many experts [68, 70, 76], see Blockchain technology as the solution to security in IoT. Since this integration is needed for IoT, there are some issues that the integration also brings [68, 70, 74]. One of the first challenges is the reliability of IoT-generated data. Blockchain can guarantee the unchangeability of data within the chain and track their modifications; however, if data becomes corrupted in the Blockchain, it stays unchangeable. IoT data can be corrupted[34, 39, 51, 70]. Furthermore, Blockchain can guarantee the integrity of data that will be processed through it unless there is no malicious data from IoT devices [34, 68, 71]. As mentioned, corrupted data is an issue, and this corruption can happen because devices can fail, Hacked or fake IoT devices pose significant risks.[34, 68, 70, 76].
- Anonymity and Privacy: Many IoT applications handle sensitive data, and when a device is linked to an individual, as seen in e-health applications, protecting data privacy and anonymity becomes a fundamental concern [39, 68, 70]. Blockchain technology offers a potential solution to this issue; for example, Bitcoin guarantees anonymity for its users [34, 70, 71]. However, ensuring data privacy in IoT is more complex, involving secure data collection, communication, and application levels. Protecting devices where data is stored and ensuring unauthorized access is prevented requires integrating cryptographic security software into these devices [34, 70]. Utilizing cryptographic hardware in the cloud can alleviate the burden of complex security software and expedite cryptographic processes [38, 68, 70, 76]. Various international laws, such as the EU's data protection regulations [34, 51, 70], govern data privacy. Therefore, adopting

Blockchain technology must align with these regulations and adhere to legal standards [34, 70, 76]. Ensuring data privacy and building trust are critical challenges for IoT. Blockchain can address identity management issues in IoT, maintaining data integrity while managing large volumes of data and providing efficient, controlled access. Compliance with global data protection laws is essential for implementing Blockchain technology effectively [34, 70, 76].Figure 17.

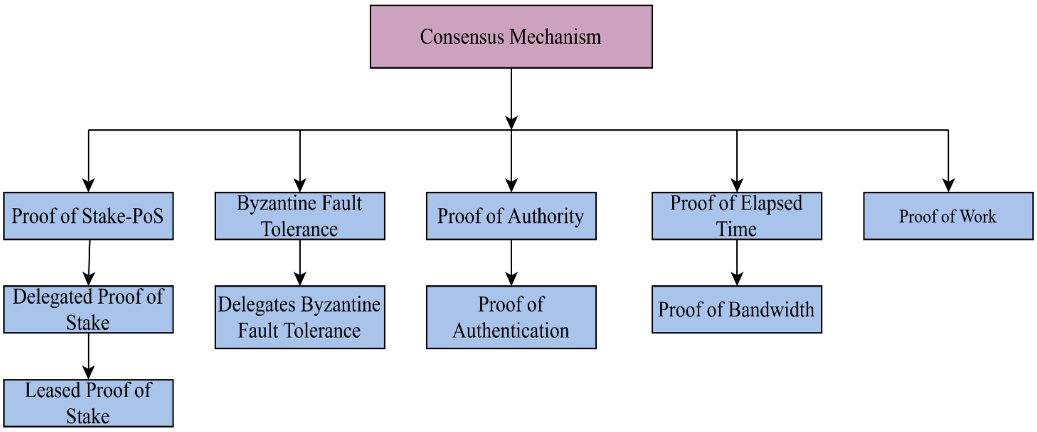

Figure 17. Taxonomy of Consensus Mechanism.

- Speed of Transaction: In Blockchain technology, the transaction rate is one of the ways to make a difference between the Blockchain. Transaction speed is one of the biggest problems of integrating Blockchain with IoT [34, 68]. The rate of Blockchain systems such as Ethereum and Bitcoin is not more than 4 to 5 transactions happening per second, at least up to now. Those systems which are integrated with IoT are slower than the other ones. IoT systems generate a large amount of data in real-time, which cannot synchronize with the speed of Blockchain [39, 68, 70, 74, 76] since it is faster. Blockchain is not originated for holding and processing the data that IoT can produce the issue is the gap in the transaction speed. Overall, blockchain's transaction rate, such as Ethereum and Bitcoin, is limited to 4-5 transactions per second, slower than ioT's data generation rate. This discrepancy poses challenges for real-time IoT integration.
- Legal Issues: The unregulated nature of Blockchain is a key aspect of its design and partly contributes to Bitcoin's success in the financial system [34, 71, 76]. However, Blockchain, particularly virtual currencies, has prompted numerous legal questions [39, 68, 70, 76]. The introduction of control mechanisms in the network, such as permissioned, private, and consortium Blockchains, reflects this concern. Similarly, the IoT sector is impacted by national laws and regulations related to data privacy and usage [70, 71, 74]. Many existing regulations are becoming outdated due to rapid technological advancements, such as those in Blockchain technology. Developing new laws and regulations can help certify the security features of devices, contributing to a more secure and trustworthy IoT network [38, 70, 76]. Despite regulatory changes, challenges remain in managing information privacy and handling [70, 71]. Some IoT devices utilize a global, unique Blockchain for machines, although it is unclear whether such networks can be managed by manufacturers or open users [34, 39, 51, 68, 70, 76]. Continuously updating laws and regulations will impact the future of Blockchain and IoT, potentially disrupting Blockchain's decentralized and free nature by introducing centralized control from governments or regions [70]. Overall, Blockchain's unregulated status raises legal issues, especially concerning virtual currencies. Both IoT and Blockchain are affected by data privacy laws, necessitating regulatory updates to keep pace with technological progress.

7. Blockchain Security

Although blockchain is considered secure, recent studies have shown vulnerabilities to various cyber-attacks affecting availability and integrity. Exploiting these vulnerabilities can compromise data recorded in the ledger, negatively impacting the blockchain state[26, 33, 39, 45, 56]. In addition, many programs are exposed to vulnerabilities that attackers can exploit. They can gain unauthorized access to the blockchain and harm it because there is a way to perform a malicious operation [33, 56, 60]. The downside of exploiting vulnerabilities in the Blockchain is that the data can be compromised. However, all data recorded in the ledger could negatively impact the state of the Blockchain [26, 39, 45, 56, 61, 76]. When it comes to Blockchain security, the Blockchain uses a 160-bit address space which is hashed by a public key generated by the Elliptic Curve Digital Signature Algorithm (ECDSA)[33, 39, 58], where it develops and allocates a large number of particular addresses and each of them is unique to be assigned in IoT devices[34, 45, 58, 60].

Since Blockchain provides a unique address, all transactions done in the Blockchain cannot be altered and can be backtracked to guarantee data reliability [26, 33, 58]. Another advantage of blockchain using smart contracts is that they provide decentralized authentication logic that is not complex and hardcoded, making it easier to authorize IoT devices[33, 45, 58, 60, 76]. Using smart contracts, we can set different rules to update software in IoT, establish new key pairs, and change ownership [45, 58]. Since this section gives an overview of blockchain security, we will learn more about blockchain-based IoT cyberattacks and countermeasures.

7.1. Blockchain-Based IoT Cyberattacks

Cyber-attacks on blockchain-based IoT systems can originate from inside or outside the network. External attacks come from attackers unfamiliar with cryptographic keys, while internal attacks involve trusted insiders. can come from inside or outside the network. The outside network is an external attack that occurs when an attacker does not know much about the cryptographic network keys and starts to attack from outside the network [45]. In contrast to an external attack, in an internal attack, the attacker controls and is trusted on the web [34, 45]. This section discusses common cyber-attacks, including Sybil, Eclipse, and DDOS attacks.

1. Sybil Attack: This attack involves a malicious party controlling a blockchain network by owning multiple malicious nodes[45, 56, 58, 74]. Sybil attacks manipulate transactions or flood the network with bad transactions, causing problems. PoW makes Sybil attacks expensive to execute, requiring significant computational resources[45, 74, 77, 78]. Some blockchain networks use consensus protocols alongside PoW to prevent Sybil attacks. Furthermore, to launch this attack, the attacker should use many computational resources to produce a block. Sybil's attack, same as PoW, is expensive to launch. The attacker must have many native cryptocurrency coins to add a new block to the Blockchain[56, 74]. When an attacker uses this kind of attack, they can compromise the entire network by manipulating a large number of virtual nodes in the network; that is the reason that they used several Blockchain which use consensus protocol in conjunction with PoW to avoid Sybil attacks[56, 58, 74, 78], in this case, PoW is conducted after every 100 blocks [34, 42, 45, 74]. Some solutions are offered to prevent Sybil's attack[45]. An IoT trust model is proposed for each user permission Blockchain with smart contracts to evaluate the trustworthiness of IoT device identities. Sybil attacks occur due to confusion some nodes can experience after a hard fork, which often happens within insecure cryptocurrency-based protocols. One of the cryptocurrencies still vulnerable to Sybil attacks is Ethereum [42, 56, 74, 77], which still has weak restrictions on the node generation process [34, 56, 78].
2. Eclipse Attack: In an eclipse attack, an attacker isolates victim nodes from the normal blockchain network by stealing routing tables and adding fake nodes as neighbors[34, 42, 56, 77]. Eclipse attacks can lead to various issues such as route fraud, storage squeeze, and denial of service. This attack is closely associated with Sybil attacks, often requiring multiple malicious nodes. Research on eclipse attacks has shown their severe impact on network topology and resource-sharing

efficiency. Furthermore, when the eclipse attacks the victim node, most of its external route paths are controlled by the attacker nodes [74, 77]. When the nodes are attacked, they can be dangerous because they can take various actions, such as route fraud, storage squeeze, denial of service, and others. So based on the discussion, an eclipse attack stands as one of the most severe threats to the blockchain network [45, 74, 77]. The eclipse attack is closely associated with the Sybil attack, where multiple malicious nodes are forged. It usually needs more Sybil nodes to mount an attack[34, 42, 56, 78]. Two main studies have been done to study eclipse attacks. One introduces the eclipse attack in Bitcoins' P2P networks. The eclipse attack destroys the topology of the networks, which reduces the number of nodes and the efficiency of resource sharing [34, 45, 74, 78]. A consequence is that the attacker hijacks all Blockchain network requests, and most of the replies they receive are falsified, and normal sharing or downloading cannot be performed[34].Figure 18.

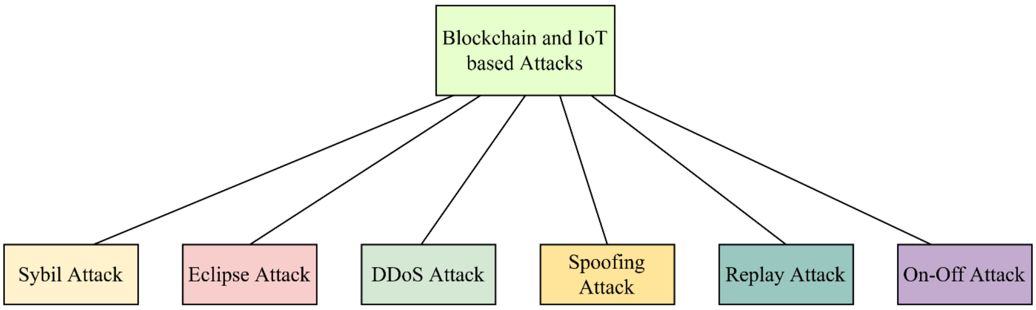

Figure 18. Blockchain and IoT-Based Cyber-Attacks.

3. DDoS Attack: Distributed denial of service (DDoS) attacks are a major threat to blockchain networks, closely connected to IoT devices[34, 45, 77, 78]. In a DDoS attack, the attackers use a client/server model to combine multiple computers, amplifying the power of denial-of-service attacks. This multiplication of resources target multiple nodes simultaneously, using blockchain as a DDoS attack engine[34, 42, 56]. This causes multiplying the power of denial-of-service attacks. This happens because many concurrent online nodes (millions of them) hold many resources in storage and bandwidth, and a Blockchain node needs to keep a copy of the whole network. A Blockchain network, in this case, is used as a DDoS attack engine[34, 56, 77, 78]. DDoS attacks can be divided into active and passive attacks. Active DDoS attack works in this way.

   The attacker actively sends a large amount of false information to the network node because the subsequent visits to this information will be forwarded to the victim to achieve the effect of a DDoS attack. Passive DDoS attacks push a based mechanism in the Blockchain network protocol [34, 42, 74]. From this, there will be a lot of information within a short period, which is not easy to record and analyze. This allows IP checks to be avoided by using fake source addresses, making it difficult to track and locate attack sources [34, 42, 45, 77, 78]. Blockchain-based passive DDoS attacks passively wait for the queries from other nodes where it modifies the Blockchain client/server software, and from there, it returns an incorrect response to achieve an attack effect. The target of this attack is to deploy multiple attack nodes, which include target hosts in one response message [34, 56, 78]. This attack deploys the pull mechanism in the Blockchain network protocol.

   DDoS attacks can be facilitated by Sybil attacks and eclipse attacks [34, 45, 56, 69]. The Sybil attack's goal is for each physical node to generate many different identities on the Blockchain network. On the other hand, DDoS attacks on a single node send many false messages to the blockchain networks or provide incorrect responses [34]. Another way to launch DDoS attacks is by using only one computer to exploit an intelligent contract repeatedly, thus congesting the network with megabytes of bytecode [42, 74, 77, 78].

4. Spoofing Attack: Another meaningful attack is a spoofing attack. In a Sybil attack, the attacker attempts to create false or virtual identities, and a spoofing attack attempts to spoof the identity of a legitimate user and use those privileges to exploit [45, 58, 74, 78]. Using this identity in spoofing attack can pretend to be a legitimate user in an IoT device by using a false identity, such as using the legitimate user's IP address or MAC address[42, 45, 77, 78]. Using this way, the attacker can gain unauthorized access to the IoT network and open doors to exploit other attacks that can seriously risk the network[45]. Table 6 shows the types of attacks and what layer those attacks have as targets.
5. A replay Attack: A replay attack is an attack where a valid transmission is maliciously repeated [34, 42, 45]. A blockchain reply attack occurs when the blockchain is hard fork and a transaction on one chain is replayed on another since both transactions are valid [34, 42, 78]. Because there are two chains, their addresses are the same as the algorithm used to generate the private key, where the transaction information is the same. This results in a transaction on one of the chains that are likely to be perfectly legal on the other[34, 45, 56, 77, 78]. Like this message, a replay attack occurs because verification of the message does not certify the correctness of the message's sending time; any messages can be selectively captured and replayed later without alteration by the attacker [45, 74, 77]. Message replay attacks are often combined with message removal attacks [45].
6. Off-Off Attack: In this attack, a malicious node behaves well and poorly. This behavior attacks before the trust system becomes aware of it[42, 45, 58, 77]. On-off attacks are known as selective attacks because malicious nodes can attack the multiservice IoT architecture by acting according to the type of service they provide to other nodes in the network [34, 42, 45, 56, 78]. On and off, attackers behave differently with different neighbors to obtain contradictory trust opinions for the same node. This attack is hard to detect because it uses traditional trust management schemes. To classify a node's behaviors requires prior trust knowledge and time. Also, not all malicious devices do misbehave [45, 77, 78].

7.2. Countermeasures

To protect against cyber-attacks on blockchain-based IoT systems, several countermeasures can be implemented: Here we will discuss countermeasures for physical attacks, network attacks, and software attacks.

1. Countermeasures against Physical Attacks: When it comes to physical attacks, a mutual authentication protocol has been proposed based on PUF (Physically Unclonable function) for small devices, which exploits the inbuilt variability of an integrated circuit [42, 44, 56, 74, 77]. Authentication is carried out using a challenge-response mechanism whose output primarily depends on the device's physical microstructure. In this case, forging the PUF [42] to clone the same structure is impossible because it eliminates attacks like tampering and malicious code injection [42, 56, 74]. In physical attacks, a heterogeneous architecture is also proposed, which is used on a customizable and trustable device mote, which can benefit energy and performance[42]. This architecture is used with reconfigurable computing with an IEEE 802.15.3 radio transceiver and hardcore micro-controller unit [34, 42, 44, 74, 78] which is host Contiki-OS [42, 56]. Another proposed solution is named REATO [42, 44, 56] which deals with different kinds of DoS attacks in IoT devices. It is proposed that a cross-domain and flexible middleware is named NetwOrked Smart object (NOS) and tailored REATO to it [42]. The solution is said to be based on an HTTP connection request to NOS, and validation, the encrypted information is sent back [34, 42, 56].
2. Countermeasures against Network Attacks: On the other hand, in-network attacks (replay and Sybil attack), there are proposed solutions to defending from the attacks[34, 42, 56]. One of the solutions offered is detecting and isolating the nodes launching Sybil attacks. It presented a trust-aware RPL routing protocol which is named SecTrust-RPL the way how it works is that it uses a mechanism based on trust to fulfill the goal [42, 56, 78]. The framework is attached to ContikiRPL. The purpose is to serve as a trust engine for making routing decisions and malicious

node detection [42, 44, 56, 74, 77]. There is proposed another model of protection, which is the “signcryption technique,” which is based on Identity Based Cryptography (IBC) that can satisfy confidentiality, integrity, and authenticity[42]. This technique combines encryption and signature and deletes the need to access a trusted third party to fulfill the authentication process [34, 42, 74]. This method is mainly proposed to be applied in a replay attack. Also, in-network attacks prevent the idea of a defensive framework against network DoS and DDoS attacks, mostly related to message flooding[42, 56, 77, 78]. This is done using a DDoS server from a third party, and the algorithm for the server consists of two parts. A part analyzes the incoming traffic to decide the suspicion of danger level [42, 44, 77, 78]. This explores the suspicious activity in DoS or DDoS. Also, has been proposed SD-IoT framework which uses an algorithm to detect and mitigate DDoS attacks using cosine similarity of vectors[34, 42, 44, 56]. This works because a threshold value is obtained using the cosine similarity of the vectors of the packet-in-message rate at the SD-IoT boundary [42]. When a DDoS attack is found, a threshold value is used, and the attacker is found out and blocked at the source.

3. Countermeasures against Software Attacks: When it comes to software attacks, a framework is developed to integrate three security aspects to protect trojan hardware from being affected on IoT devices [34, 42, 44]. The first is vendor diversity, which enables trusted communication between untrusted nodes. Secondly, message encryption prevents unauthorized parties from accessing contacts. Lastly, mutual auditing is allowed to allow authorized nodes to verify the encryption status and content of a message [42, 56, 77, 78]. Also, another way to prevent hardware trojans is proposed, and that way is by using high-level synthesis (HLS). Security improves the hardware produced by HLS, which is an indirect way to prevent the injection of hardware Trojans into the network [34, 42, 44].

Many other ideas are proposed to protect against the attacks used for all of them. One of them is the greedy heaviest observed subtree rule (known as GOST). It is a variant applied to Ethernet projects [34, 44, 56, 77]. First, it analyzes the impact of Bitcoin security in the case of higher throughput. The block size and the block creation rate increase. Although blockchain throughput can be promoted, the risk of occurring forks in the block tree also increases, reducing blockchain security [34, 74, 78]. Using this method, we can solve the security problem by replacing the principle of the longest chain with the heaviest subtree [42, 56, 74, 77, 78]. Changing the node construction and organization mod of bitcoin Blockchain, as well the computing power the dishonest of node reach 50

7.3. Blockchain Privacy and Issue

Each user in the Blockchain is identified and does a transaction using their public key is also known as a hash. This guarantees everyone that their anonymity is present in the Blockchain even though their transactions are shared, and everybody can see and analyze them. Still, they never know the identity of the user [26, 54, 56, 65]. So, we can say that anonymity is a fundamental property in Blockchain technology, and this is one of the reasons why Bitcoin, as well as other cryptocurrencies, have been so successful since users can utilize several anonymous addresses for transactions, as well as many different methods have been taken to fulfill the goals [33, 34, 45, 56]. But the researcher has raised many questions about the privacy of Blockchain technology [26, 34, 58, 60, 65]. Those concerns have mostly been raised because all the transactions are publicly logged[34]. Since the development of different technologies over the years, privacy has been concerted for everybody, such that privacy has been recognized as a fundamental human right by the United Nations in their Declaration of Human Rights, Charter of Fundamental Rights in the European Union, and many other parties and organizations Worldwide [33, 54, 56, 65].

Since privacy is one of the main concerns in Blockchain technology, privacy itself requires that each application be determined by the nature it has been used and which is appropriate; another requirement can appear such as cryptocurrency being offered in public such that anybody will be able to contribute such adding transaction in the ledger, which is public, in Blockchain we are not able to do private transactions as we mentioned above[45, 51, 56, 65]. Also, Blockchain was able to enhance the transparency of the user's communications, such as by providing an audit trail of the underlying data processes. In this case, the other data protection requirements may be present[45, 51, 54, 56, 58]. In this section, we will present some techniques to alleviate privacy issues using Blockchain technology to process personal data. Pseudonymization is available in all the Blockchain platforms used to protect individuals' identities, allowing them to retain some utility in their data[54, 56, 65]. Pseudonymization can be defined as the processing of personal data, where the personal data can no longer be attributable to a specific individual without the use of additional information, where the information is kept separately and is subject to technical and organizational measures to make sure that the personal data are not attributed to an identified where is this case it is achieved by replacing users' identifiers by pseudonyms[33, 45, 51].

Cryptocurrencies like Bitcoin and Ethereum use pseudonymization techniques because each user's wallet is uniquely associated with a random-looking address. All the transactions can be seen as public, like the amount sent or received, public key, or hash generated, and there is no way to map the address back to an identified individual[33, 56, 65]. Mixing techniques – This technique is used in Bitcoin and Ethereum, which allows more than two to shuffle many transactions without revealing the exact relationship between the transactions. This means they can interfere with each other and cannot be linked. Since this technique is old, the Blockchain is used to conceal the history taken because each transaction stored in the Blockchain is connected to multiple senders and receivers [26, 65]. Those mixing services can also be provided through a centralized mixing service provider or on a peer-to-peer basis [45, 56, 58]. This method also can be a perfect way to improve privacy because it may aggregate communication between peers in various strategies and output actions. The technique has been used to expand privacy but was not complete and thus may not be as present in Blockchain technology[51, 56, 60]. The mixing method is also used to confuse attackers, making it hard for them to infer the exact number of real coins spent by transactions[33, 45, 60, 65]. Another technique being presented and operated is the Zero coin, also known as zero of knowledge, which is evidence that it allows showing to counterparty, where the users recognized obvious information of uncovering the information [56, 58, 60]. In this case, it does help with the verification of reliable transactions by preventing user identity detection, even though there is evidence that those were not immune to attacks[45, 56, 58, 60, 65]. In the mixing method, they were vulnerable to de-anonymization across statistical detection attacks, which were developed to prevent the requirement for a mixing server that presents security.

Advanced cryptography technologies protect Blockchain user privacy in recent Blockchain. There has been a proposal to solve the issue through smart contracts in the public Blockchain, which automatically its dose generates efficient cryptographic protocols using primitives, namely zero-knowledge proves[45, 54, 58, 65], which some of us talked about earlier. Zero-knowledge proof enables a statement to be verified without information except for the statement itself [33, 51, 54, 65]. Zero-knowledge is used for many reasons and applied to zerocoin, and zerocash. Another important thing is data protection which can be affected by Blockchain. It is preserved by confidentially of transaction technologies[26, 45, 54, 56]. Some researchers [33, 45, 51, 54] have shown to keep the content of transaction example amount being sent or show participant, where it concludes that the content can be verified such that no more coins can be available ones can be spent in a cryptographic means[51, 54, 65]. Another solution that has been proposed that we did not mention until now is attributed-based encryption (ABE). In this case, secret keys are generated based on the attributes of peers. Applying this method, sensor data in transactions can be encrypted and decrypted using the miners and users using decryption credentials from attribute authorities [54, 56, 65].Table 7.

There are also other privacy issues in the IoT section, such as the Lack of IoT in centric consensus mechanisms[58] where consensus protocols are deployed in different Blockchain platforms. They share a common issue: the consensus finality, while permanently committing new blocks might result in delayed transactions and confirm it [50, 56, 58, 79]. Because of that, it does not fit the instantaneous

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 September 2024 doi:10.20944/preprints202409.1193.v

IoT system. Another issue is transaction validation because some rules include the correct transaction format, signature, and other parameters depending on the Blockchain platforms [45, 54, 79]. An example of this is Bitcoin transaction validation rules, which include that the same transaction has been spent before.

Table 7. Security .

Blockchain	Hyperledge	Ethereum	Bitcoin
Nature	Permissioned	Permissionless	Permissionless
Validation	PBFT	Ethash PoW	PoW
Purpose	Chaincode	Smart Contracts	Crytocurrency
Language	Java,Go	Internet Code	Scripts based in stack

On the other hand, in Ethereum, different rules are included, such as checking the balance of the sender account. In addition, other validation rules can be created to meet the heterogeneity of the sense data [50, 58]. Table 7 shows how those features work and how they can be used. Data scalability and management issues are another problem because Blockchain is a distributed ledger of databases that grows over time because of the massive volume of data collected from a wide range of interconnected IoT devices [50, 56, 58, 79]. Those devices without proper security control might cause compatibility issues that would result in severe security issues [51, 56, 58, 60]. User experience is another issue; as we know, most applications are built on top of the Blockchain, which requires the end user to manage and gives them the right to control their transactions through e-payments instead of using the middleman as can be Banks. The issue also spreads in the computational power it acquires from the user to mine or commit new blocks[33, 50, 56, 79]. This may cause the Blockchain network to be cumbersome to log transactions due to the complexity of decentralization. Those issues are being presented when blockchain is integrated into IoT.

7.4. IoT Trust Issues and Their Solution by Blockchain

Security Necessities for IoT or Issues

1. Data privacy - Due to the wide-ranging integration of services and networks, the data stored on a device is susceptible to attacks by compromising nodes within connected IoT systems [33, 51]. Additionally, attackers can access the data without the owner's authorization.
2. Data integrity - Within a centralized client-server architecture, an attacker might exploit unauthorized network access to alter the original data or information before forwarding it. For example, when Alice sends data to Bob, Watson, an intermediary, could intercept and modify these data before passing them on [45, 54, 78].
3. Third-party - Information gathered in a centralized setup is held and managed by an external centralized organization, which might abuse this information or share it with others [45, 58].
4. Reliable data source - Within an IoT context, identifying the source of data generated by various devices is challenging because the information is stored across the entire network and can be modified by any user [34, 56, 78].
5. Access management - One of the primary challenges in IoT networks is access management. Determining which node is authorized to access and execute various functions across the entire IoT network can be complex [45].
6. Single points of failure - The ongoing expansion of centralized networks for the IoT infrastructure can reveal single points of failure. If a central authority stores and verifies all data of the network [58, 60, 78], the entire network becomes vulnerable if the main point fails or experiences downtime.
7. Scalability - The Internet of Things interlinks numerous sensors and diverse devices for data exchange and various applications over the Internet[65, 79]. It poses a challenge to the system's architecture and its ability to grow swiftly to scale. Figure 19 illustrates the dimensions of

scalability which are divided into horizontal and vertical scalability, depicting the dimensions of blockchain scalability.

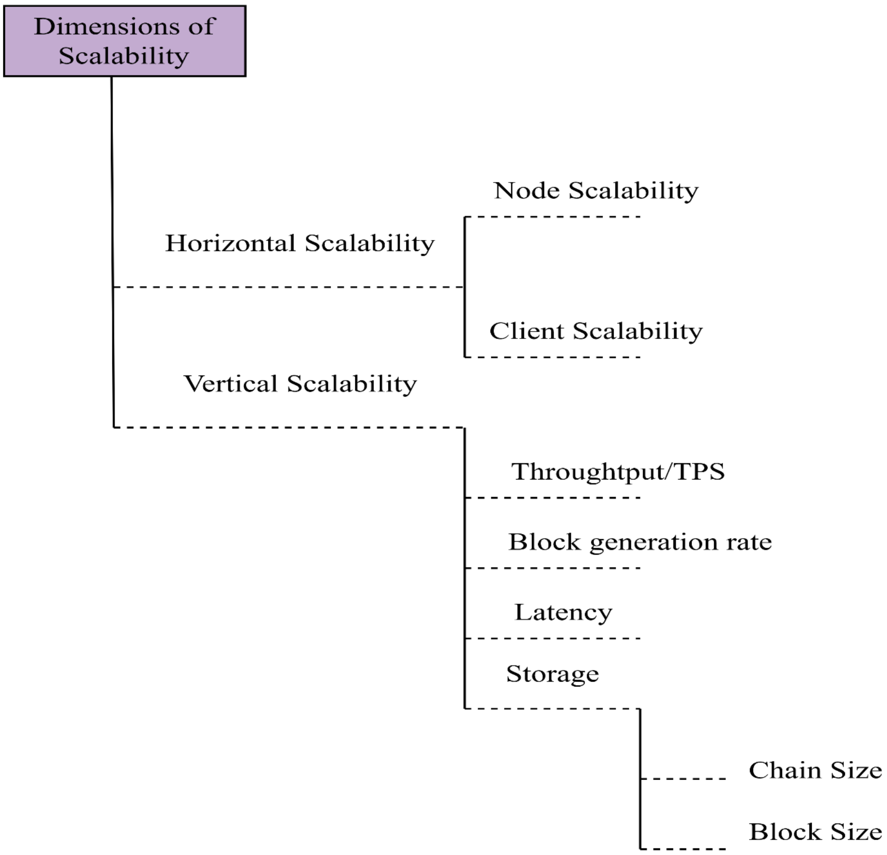

Figure 19. Dimensions of Blockchain scalability

7.5. Blockchain Solutions for IoT

- Data integrity - Blockchain operates as a peer-to-peer network where each node maintains a duplicate set of records. When a transaction is initiated, the originating node uses its private key to sign the transaction and then sends it to other nodes for validation. All miner nodes take part in the validation process to find a nonce [34, 42, 65]. The first node to discover the nonce gains the right to validate the transaction and receives a reward. It will then broadcast the validated transaction to all other nodes in the network. Once the transaction is added to the Blockchain, it is immutable and cannot be altered, rolled back, or deleted [33, 51].
- Data privacy - A consortium Blockchain ensures data privacy within a Blockchain network. As depicted in Figure 3, all nodes intended for a specific purpose are grouped to create a private network or Sidechain. Each Sidechain handles its respective IoT data [34, 78]. Nodes belonging to one Sidechain do not participate in the validation process of other Sidechains. To access data on the consortium Blockchain network, a requestor node must first register and join the relevant Sidechain network, then submit an access request. Consortium Blockchain includes access control mechanisms to prevent unauthorized access [34, 42, 65, 78].
- Addressing space - Blockchain utilizes a 160-bit address, while IPv6 employs a 128-bit address scheme. Consequently, Blockchain offers 4.3 billion more addresses than IPv6, thereby enhancing the addressing capacity compared to the IPv6 addressing scheme [51].
- Trusted accountability - Each operation record is required to be logged into the Blockchain network. This process assigns an identity to every operation, making each one traceable. If any abnormal behavior is identified, it is reported back to the origin for further investigation [56, 58].

- Fault tolerance - Decentralized devices are less likely to fail accidentally because they rely on many separate components. Blockchain is a point-to-point decentralizing network. Every device has the same record copy in it, which is why a single node's failure has not affected the network [45, 56]. So, the Blockchain prevents a single point of failure.
- Trusted data origin - To track data in a Blockchain network, a unique ID is assigned to each IoT device [56].
- Removing third-party risks - Blockchain technology empowers devices to execute operations without relying on an intermediary or third party, thereby enabling thus making them risk-free from a third party [51, 58, 78].
- Access Control: The smart contract is one of the most effective features of Ethereum, first proposed by Nick Szabo in 1994 [44]. These smart contract programs for Blockchain are designed to establish access rights and various policies. For instance, a rule might be set so that when the meter hits 135 KW, devices automatically switch to energy-saving mode [33, 51, 65]. The Internet of Things (IoT) is a rapidly advancing technology due to the growth of high-speed networks and smart devices. However, IoT devices are particularly vulnerable to attacks and lack the ability to defend themselves. This paper explores the various characteristics of Blockchain networks, such as Proof of Work (POW), decentralization, persistence, and network scalability [45, 58]. It also examines the challenges faced by IoT devices, including data integrity, access control, and privacy, while presenting Blockchain-based solutions proposed in the literature.

7.6. Consensus Protocols/Algorithms in Blockchain

The consensus algorithm is here to securely update replicated shared states, which are necessary to make possible working principles of the Blockchain [39]. There is also a system known as the state machine replication, a consensus protocol that ensures that all replicas of the shared state are synchronized and in agreement with any stated point [39, 62, 64, 70]. Consensus protocols incentivize the participating nodes to create and add new blocks to the Blockchain [34, 45, 56, 65]. The consensus protocol must exhibit the Byzantine Fault Tolerant (BFT) property. Those protocols are categorized as proof of a given delegation which is the basis of these kinds of algorithms in the election of a leader [52, 62, 70]. Check Figure 20 for types of consensus algorithms.

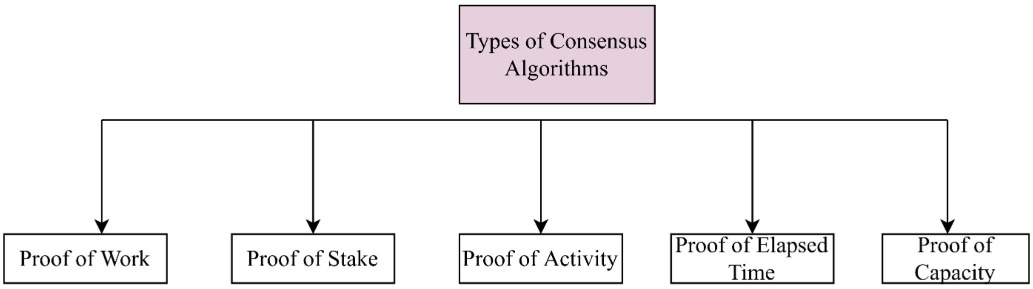

Figure 20. Most popular consensus algorithm

- The Proof-of-Work (PoW) is computed as a mathematical problem. The nonexistence of PoW today would make it impossible to talk about Blockchain[52, 62]. PoW has been considered to be hard to computationally heavy and expensive in energy consumption[34, 52]. PoW is often considered challenging because it would not be easy to do if you want to obtain a value that can be Bitcoin or another cryptocurrency because of performed work. One of the main goals of Proof of Work is to avoid spamming attacks. PoW should be an asymmetric task, which is hard to solve but would be easy to verify. A miner needs much more time to find the nonce that solves the hash problem, where other miners in the network can easily verify and validate the solution [45, 52, 64]. One of the main problems of PoW [52, 62, 69, 70] is that multiple miners working on a standard objective lead to tremendous wastage of computing power and electricity. With a high requirement in computing power, mining has advantages if done in pools by defeating decentralization for its sound. PoW-based consensus is vulnerable when a user takes control of 51 percent of processing power in the network, as illustrated in Figure 21, [39, 45, 62].

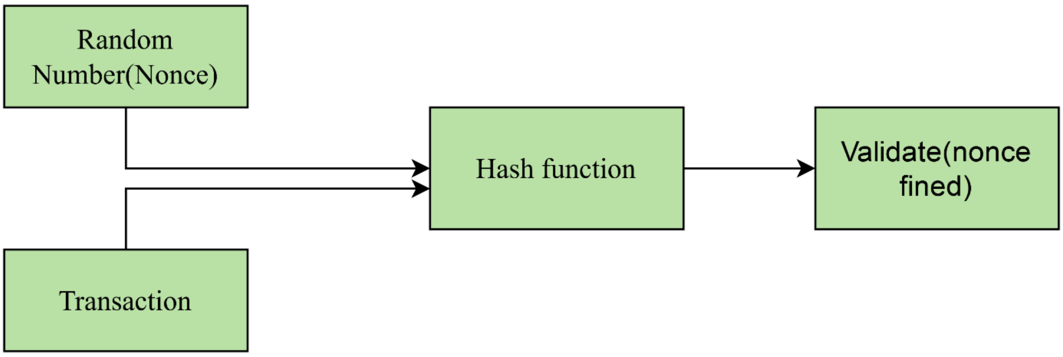

Figure 21. Proof of Work

- Proof-of-Stake (PoS) – the main concept of proof of stake is the concept itself "stake," where the nodes participating in this consensus process lock into account a specific number of coins. The idea is to ensure that every node will act respecting the protocol rules and will not deviate from them [34, 45, 56]. As a result, users with larger stakes have a stronger incentive to protect the system's reliability, as they risk losing more if the stake is compromised. Thus, there is less chance for a node to become malicious. It has been said that PoS protocols have a low performance. For that reason, a few other variations from Algorand are proposed on top of the Byzantine agreement [56, 62, 69]. See Figure 22 for how those transactions work.

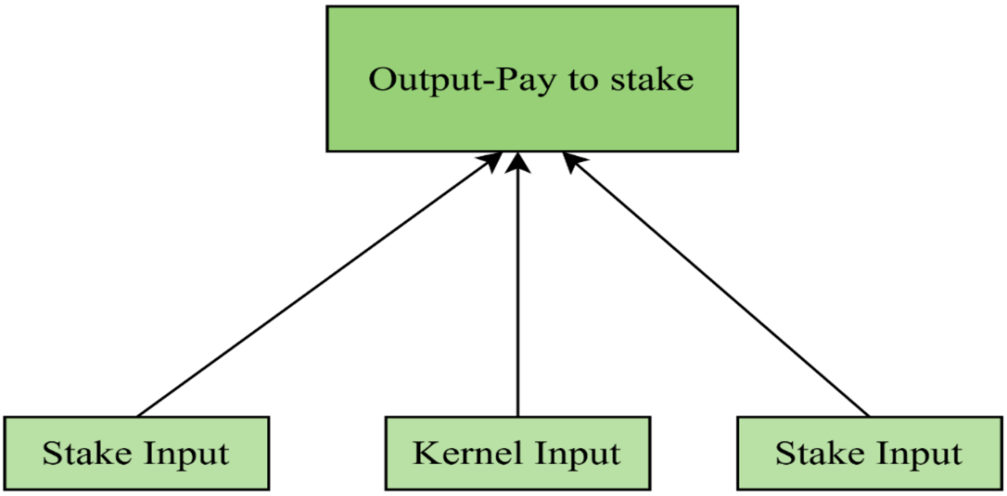

Figure 22. Proof of Stake Transaction Structure

- Algorand solves the decentralization, scalability, and security by attaching a cryptographic proof where each new block checks the eligibility of the block proposed to be chosen, which is directly proportional to its stake. Based on security and performance, Algorand can tolerate malicious behavior and provide high scalability [34, 56, 64, 70]. Also, as part of PoS, there is Delegated PoS, which does require voting to reach a consensus [52, 62, 69]. The responsibility of network management is given to delegates who are not incentivized. The duties they have include fee schedules, block intervals, as well transaction sizes. There can also be changes, and those changes can be adopted based on the network's voting. Proof of Authority (POA) is the successor of PoS, where the reputation of the validator acts as a stake [52, 64]. When it comes to reputation, it is hard to regain it when lost; that's why there will be a better choice for "stake. PoA networks have high throughput but are centrally controlled by the validators [34, 52, 56, 61]. Figure 23 shows the hybrid network using Proof of work and Proof of stake and how that works.

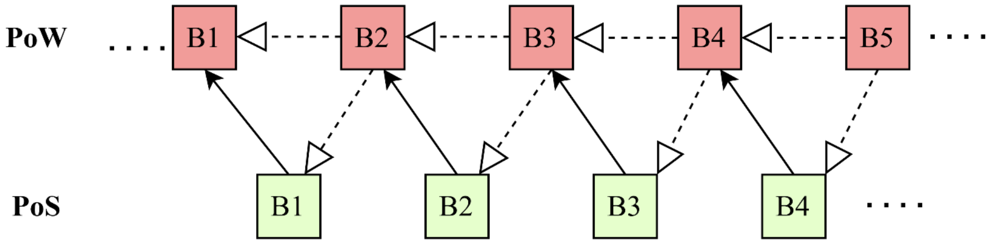

Figure 23. Combining Proof of Work and Proof of Stake

- Proof-of-Activity is introduced as an alternative to Bitcoin mining, combining elements of both proof-of-work and proof-of-stake to achieve consensus. Its primary aim is to reward stakeholders who are actively involved in the network [39, 61, 69, 70]. Additionally, Proof-of-Activity is used to ensure distributed consensus by finding proof-of-work against an empty block, with no transactions included. From there, a group of validators is selected to vote on the validity of the mined block header [39, 62].
- Proof-of-Elapsed-Time (PoET) is designed to eliminate the need for the computational power required by PoW-based consensus protocols. Implemented in the Sawtooth platform, this protocol addresses the Byzantine agreement problem by using a lottery-like approach to ensure fairness, investment, and verification during leader election [39, 45, 56, 70]. In PoET, peers wait for a random amount of time to elapse, and the peer that finishes waiting first is selected as the leader to create a new block [56, 62, 64]. This process takes place in a secure memory area, such as Intel's SGX, which is commonly used in the Sawtooth platform [56, 61].
- Proof-of-Capacity (PoC) is an alternative to PoW that leverages miners' hard drive space instead of computational power to solve cryptographic challenges. In PoC, miners engage in a process called "plotting," where they store various solutions to problems in advance, removing the need to solve them on the spot. This method is more energy-efficient compared to PoW [45, 52, 56, 70]. However, there is a possibility that multiple users could collude to combine their storage power within a centralized network.
- The Kafka protocol utilizes a shared subscribe messaging pattern capable of transferring large volumes of log data with minimal latency. It involves producers, topics, consumers, and brokers. Producers publish recorded information as a stream of messages, which are segments of partitioned files [56, 61, 64, 69]. These messages are stored by brokers in the latest segment file, and subscribed consumers can read them by requesting access from the brokers [56, 62]. Kafka uses a Crash Fault Tolerant (CFT) consensus protocol, which can handle up to 50 percent of network failures, and is primarily implemented in fabric systems [45, 70].
- The Practical Byzantine Fault Tolerance (PBFT) protocol is a widely recognized protocol that has gained increased attention with the rise of Blockchain technology. PBFT operates under the assumption that less than 33 percent of network nodes behave maliciously. Consensus is achieved through three phases: pre-prepare, prepare, and commit [56, 61, 69]. In this process, each node acts as a validating replica that votes to elect a primary node, or leader, which initiates the three-phase consensus after receiving a request from clients [34, 39, 56, 70], starting by multicasting a pre-prepared message. Despite its effectiveness, PBFT lacks scalability, supporting only a limited number of nodes and requiring the transfer of numerous messages to reach consensus [56]. The Ripple Protocol Consensus Algorithm (RPCA) was designed to ensure security and stability within a cryptocurrency-based network for remittance transfers, without the need to implement

smart contracts [62, 64]. Each node in RPCA maintains a unique node list, which is a set of trusted validators involved in the consensus process [34, 45, 56]. Nodes listen to these trusted validators, and if consensus is not achieved on a set of transactions, the node's proposals are adjusted according to suggestions from their trusted validators [56, 61, 69, 70]. Transactions that receive more than 80 percent positive votes are processed, while others are either discarded or placed in a candidate pool for future ledger-inclusion [56, 64].

- The Stellar Consensus Protocol (SCP) is designed as a Federated Byzantine Agreement (FBA). Unlike other protocols, SCP does not require consensus from a threshold of all nodes in the network; instead, each node forms a subset of trusted nodes within the network [45, 52]. Nodes make decisions based on the consensus of their trusted circle, and any misbehaving nodes are excluded from both the trusted circle and the decision-making process. In Hyperledger Fabric, where PBFT is used, network nodes validate each transaction, and a leader is elected to propose the transaction sequence. In the Delegated Byzantine Fault Tolerant (DBFT) protocol, specific nodes are chosen to reach consensus on the next block to be added to the Blockchain [52, 61, 69, 70]. These nodes, known as bookkeepers, continuously vote and are selected through a registration process in the network [34, 52]. The table below provides a detailed summary of various consensus algorithms.

7.7. Taxonomy of Security Research in IoT

Here we will provide more information about the general taxonomy of security research related to the IoT domain. The way how we can discuss it is by separating it into different sections, as in this case, we are going to talk about seven provinces. Those sections are based on the domain security for IoT in those sections: Developing Authorized Schemes, Ensuring Trust, Preventing Attacks, Designing Authentication Protocols, Privacy, Secure Data Management, and Ensuring Basic Security [42, 61, 68].

All those categories are integrated and how they help with the domain. Authentication protocols are designed to authenticate users and devices, and even the simplest cryptographic operations are attached to achieve data authentication. Some of the areas in which authentication is used are biometric-based solutions, and interestingly, user authentication is also used in blockchain-based fingerprint verification methods [33, 42, 68]. Expect user authentication. Data authentication is also complete by designing the proper signature schemes on which it is based and suits different applications. In addition, smart contracts are deployed on the Blockchain to develop appropriate authorization schemes [42, 61]. Another area to be discussed in this section is attacks that are a serious threat to IoT systems, especially the damage caused by industrial IoT systems can be wiped away due to those different attacks like replay attacks, DDoS attacks, and other attack risks that need to be analyzed more, which is why many studies and solutions tend to find a different explanation for those attacks[42, 61].

Concerning the IoT, data and user privacy are essential and crucial requirements for all devices. Different kinds of Blockchain have proposed various solutions, such as data aggregation techniques using Blockchain, which helps preserve privacy. Apart from that, secure data management is an essential concern that many researchers are focusing on to find a different solution [33, 42, 68]. One of the well-known solutions is securing data management by multi-key aggregate keyword searchable encryption has been proposed and as a technique adopted a lot. When it comes to security, one of the real solutions is CIA security, non-repudiation, and access control [42, 61, 68], some of the solutions that have been proposed are using SVM, a credit-based consensus mechanism, and various encryption techniques within the Blockchain have been used [42]. Moreover, to ensure trust in consensus algorithms and re-encryption techniques with blockchain have been proposed. The figure below shows the taxonomy of security research advancements in the IoT. As we have been talking about in the section if we go over the constitution and analyze it, we can get a clear idea about which areas different researchers have focused on more and what solution is being proposed. An in-depth analysis of this dose helps us identify various solutions to security issues [33, 42].

8. Research Directions and Open Research Issues of IoT with Blockchain

Blockchain is a powerful yet emerging technology. While integrating IoT with Blockchain offers numerous advantages, it also introduces several challenges that must be addressed to fully realize the potential of both technologies. Considering the security of current Blockchain systems, we outline future trends to inspire further research in this field. To make these solutions practical, certain research challenges must be tackled in the future to make Blockchain a viable solution for securing IoT data and integrating Blockchain with IoT [56, 58, 60]. Figure 24 highlights the open research directions for future studies. This section will explore these challenges, the trade-offs between public and private Blockchain implementations, and future research directions for Blockchain integration in IoT. In the IoT domain, the ideal distributed platform should support the following key functionalities:

- Trustless peer-to-peer M2M communication
- Decentralized access control
- Private-by-design file sharing
- Scalable security provision over multiple IoT use cases

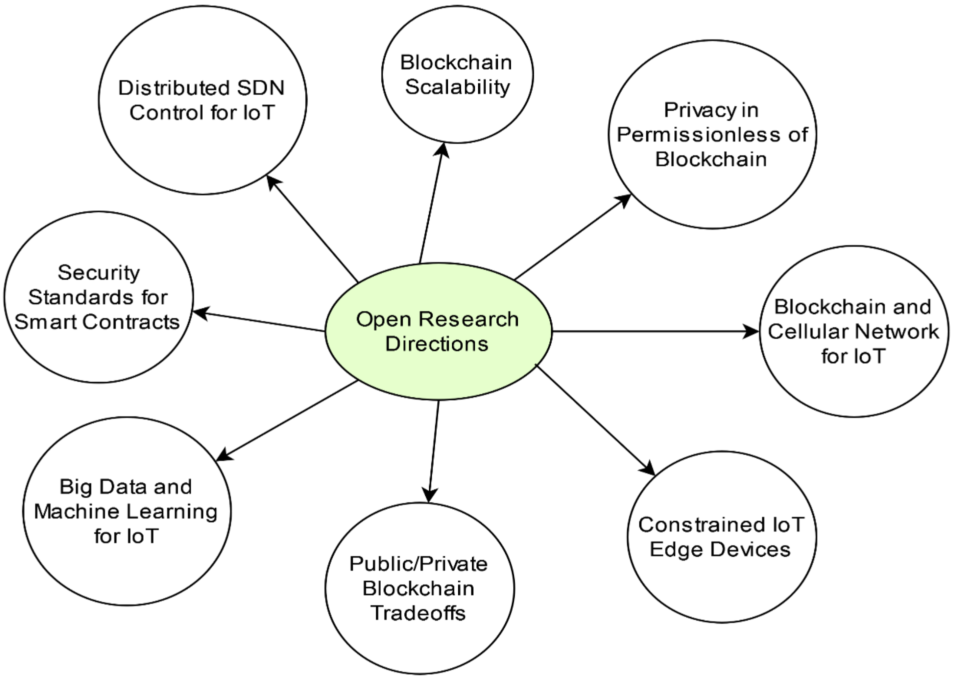
Open Research Directions
Distributed SDN Control for IoT
Blockchain Scalability
Privacy in Permissionless of Blockchain
Security Standards for Smart Contracts
Blockchain and Cellular Network for IoT
Big Data and Machine Learning for IoT
Public/Private Blockchain Tradeoffs
Constrained IoT Edge Devices

Figure 24. Open Research Directions

- Security: IoT systems are often seen as easy targets for various security attacks due to the inadequate security measures in place for billions of heterogeneous Internet of Things devices [65]. Advanced encryption algorithms are often not feasible for IoT devices. Blockchain technology also faces security vulnerabilities, such as bugs in smart contracts and attacks on decentralized autonomous organizations (DAOs) [4, 80-83]. Since Blockchain data is stored on a public ledger, privacy and confidentiality issues remain. However, different anonymization or encryption techniques can be applied to protect this information. An effective IoT network should be resilient to all potential attacks. Current advanced security strategies largely rely on complex hash puzzles, making it challenging to secure a network with resource-limited devices that cannot handle heavy computational tasks [34, 54, 65]. Therefore, further research is needed to address the security challenges in both IoT and Blockchain.
- Scalability: A major challenge in integrating Blockchain with IoT is the Blockchain's ability to scale and function effectively within a large-scale network like the IoT. Due to scalability issues

with existing Blockchains, IoT cannot fully utilize them because of slow transaction rates and high volumes of concurrent workloads [45, 51, 56, 58]. Blockchain technology currently faces significant scalability problems. Although there are proposals for addressing these issues, such as developing more scalable consensus algorithms and creating private Blockchains for IoT, further research is required to identify efficient solutions [56]. Two potential approaches to improve Blockchain scalability in IoT are: 1) designing more scalable consensus algorithms and 2) building private or consortium Blockchains specifically for IoT. Enhancing scalability with current implementations may impact throughput and latency. Table 8 provides more details.

- IoT Edge-Device Constraints: IoT smart devices are interconnected to automate processes, but many of these devices face strict computational and networking limitations, which create challenges when implementing Blockchain-based decentralized systems [80, 84]. Blockchain technology can manage both structured and unstructured data transfers through distributed records, facilitating interoperability across various IoT edge devices despite these constraints [4, 82, 85]. One proposed solution to extend Blockchain to the IoT edge is to utilize computationally capable IoT gateways for end-to-end communication, leveraging their high performance and networking capabilities. A key challenge in this approach is to enable IoT devices and gateways to transmit transactions to the Blockchain using light clients, without establishing centralized block validation pools [73, 86].
- Smart-Contract-Related Solutions: Ethereum supports multiple programming languages, with Solidity being the most commonly used for writing and compiling smart contracts. Smart contracts, introduced by Nick Szabo in 1994, are a key feature of Ethereum's efficiency [4]. Research into Blockchain IoT integration includes developing security standards for smart contracts to ensure that their security is not compromised by vulnerabilities, despite the Blockchain's inherent security features. For instance, the DAO attack highlighted how adversaries can exploit weaknesses in smart contracts [4, 82, 83, 87]. Therefore, smart contracts must securely model the application logic of IoT systems. They rely on data feeds from real-world systems, known as oracles, which provide reliable real-world data. Given the potential unreliability of IoT, validating these smart contracts can be challenging [82, 87]. Blockchain technologies face design constraints in transaction capacity, validation protocols, and smart contract implementation [87]. Thus, future research is crucial to enhance the use of smart contracts in IoT applications.
- Data Storage: While Blockchain and IoT data storage frameworks handle various types of information, the primary challenge is the systematic sharing and securing of this critical data. In Blockchain design, there are two main components: the transaction hubs and the linked blocks. The Blockchain framework provides users with accountability, privacy, and traceability [73, 81, 85]. User data is stored in blocks corresponding to specific block numbers, which are used to identify the user only at designated thresholds. The data volume is verified by referencing a specific block number and its segmentation.

Table 8. Expected Data Size with Increase of Transaction Throughput.

Block Size	Block Fees	TPS	Annual Size
1	0.12BTC	1	15GB
0.9MB	0.36BTC	3	47GB
3MB	1.2BTC	10	150GB
30MB	12BTC	100	1.5TB
300MB	120BTC	1000	15TB
3GB	1,200BTC	10,000	150TB
30GB	12,000BTC	100,000	1,500TB

The data packets received are initially stored in blocks by users during the first checkpoint, along with the fragmentation of the stored data, as illustrated in Table 8, which shows that the size of the data increases with the volume of transactions. The new cluster number is then encrypted using a shared key derived from the Diffie-Hellman algorithm. This encryption ensures that the cluster number's owner cannot be determined by others. Because partitions are crash resistant and only the legitimate user knows the cluster number, unauthorized users are prevented from accessing the data [73, 85, 86]. Although data storage frameworks for blockchain IoT (BIoT) handle diverse information assets, the main challenges involve systematically sharing and securing these crucial data [88]. Therefore, extensive research is needed to enhance the security of data storage for blockchain and IoT devices [87].

- SDN Integration for Blockchain-Based IoT Edge: Fog Computing, also known as Edge Computing, is an extensive virtual system that facilitates processing and storage between users and the traditional cloud data centers [4, 81, 89]. In the evolving landscape of the Internet, particularly with IoT, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are designed to provide a virtualized edge platform where virtual hosts can be dynamically deployed [4, 85]. SDN's separation of control plane and data forwarding functions allows for easy management and control of virtual IoT resources. This approach has the potential to improve IoT edge configuration and management. However, as SDN and NFV technologies advance, they introduce new cybersecurity challenges, which are further complicated when integrated with IoT.
- Big Data and Machine Learning for Decentralized IoT Frameworks: In the IoT, machine learning can be used to make intelligent decisions to optimize automation tasks like managing IoT assets, scheduling, and energy transactions [4, 85, 88,91]. The secure and verifiable Blockchain structure may be used to ease extensive data management. However, data analytics using Blockchain structure implies too much overhead. Despite this, in most cases, processing all transactions will not be necessary; hence, intermediate, or efficient auxiliary systems may be implemented, thereby increasing the overall efficiency. Nevertheless, Blockchain-based architectures already exist for ample data storage [80]. IoT and Blockchain integration will significantly increase the use of Blockchain and establish cryptocurrencies on the same level as current fiduciary money. One of the significant concerns about Blockchain, particularly cryptocurrencies, is their volatility, which individuals have also exploited to profit [83]. The mixture of Blockchain and IoT can suggest a robust methodology that can meaningfully cover the path for new business methods and spread applications[79,89,90]. Additionally, the design of Blockchain for IoT applications would also adapt to the specific properties of IoT networks, such as immense scale, inherent partitioning, incomplete network connectivity, non-trivial topology, non-zero propagation delay, heterogeneous data, and finite device memory[92].

9. Conclusion

This survey provides a comprehensive discussion on the integration of blockchain technology with IoT addressing architecture alignment, application security, and limitations. The findings highlight the potential of blockchain to improve IT security through decentralized, immutable, and encrypted frameworks. Although the promising implications, challenges such as scalability, energy consumption, and data privacy need to be addressed. Moreover, the Internet of Things continues to proliferate and security and privacy remain paramount concerns. This survey has explored the compelling solution of Blockchain technology integration into IoT to mitigate these concerns. Although the implications are promising, challenges such as scalability, energy consumption, and data privacy need to be addressed. We have investigated the characteristics and components of blockchain technology, examined its possible applications in IoT, and discussed architectures for IoT-Blockchain integration. Furthermore, we have highlighted the importance of Blockchain in protecting IoT from cyber-attacks, providing practical suggestions and outlining the consensus protocols and algorithms inherent to the technology. Future research should focus on optimizing blockchain for IoT environments, developing robust consensus algorithms, and establishing interoperability standards. By addressing these challenges, the integration of blockchain and IoT can significantly contribute to secure, efficient, and scalable systems for various applications.

Author Contributions: Conceptualization, M.A.O. and K.T.; methodology, M.A.O., M.R. and M.A.; formal analysis, M.A. and M.A; investigation, M.R., M.A., K.T. and A.K.; resources, M.A. and A.K.; writing—original draft preparation, M.R., K.T., M.A and A. K.; writing—review and editing, M.A.O. and M.A.; visualization, A.K; project administration, M.A.O. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures", Computers Journal, MDPI. May 2020, 9, 44.
2. Muath Obaidat, Kutub Thakur, and Jian Choong, "A Secure Authentication and Access Control Scheme for CoAP-based IoT", 5th Conference on Cloud and Internet of Things. March 2022. Marrakech, Morocco.
3. Al-Fuqaha, A., et al., Internet of things: A survey on enabling technologies, protocols, and applications. 2015. 17(4): p. 2347-2376.
4. Lone, A.H. and R.J.C.S.R. Naaz, Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic review of the literature. 2021. 39: p. 100360.
5. Davis, K.J.T.c.r., The urbanization of the human population. 2011. 5: p. 20-30.
6. Muath Obaidat, Joseph Brown, and Abdullah Al Hayajneh, "A novel Paradigm for Access Control Trust in IoT Applications: A Distributed Cross-Communication Approach", 13th IFIP Wireless and Mobile Networking Conference (IFIP WMNC), Montreal, Canada. October 2021.
7. M. Rawashdeha, M. G.H. Al Zamilb, S. M. Samarah, Muath Obaidat and M. Masude, "IOT based service migration for connected communities", Computers & Electrical Engineering. Elsevier, Volume 96, December 2021
8. Muath Obaidat, Matluba Khodjaeva, S. Obeidat, Douglas Salane, Jennifer Holst, "Security Architecture Framework for Internet of Things", 10th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference. Columbia University, New York, NY 2019
9. Bernard Marr,.Dorsemaine, B., Internet of things: a definition and taxonomy, 2015.
10. Bezabih, Y.M., et al., Correlation of the global spread of coronavirus disease-19 with atmospheric air temperature. 2020: p. 2020.05. 27.20115048.
11. M. Abouali, K. Sharma and T. Saadawi, "Access Delegation Framework for Private Decentralized Patient Health Records Sharing System Based on Blockchain," 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022, pp. 0007-0013.
12. Fabiano, N. The Internet of Things ecosystem: The Blockchain and privacy issues. The challenge for a global privacy standard. in 2017 International Conference on Internet of Things for the Global Community (IoTGC). 2017. IEEE.
13. Wang, T., et al., Privacy preservation in big data from the communication perspective—A survey. 2018. 21(1): p. 753-778.
14. Rivera, R., et al. How digital identity on Blockchain can contribute in a smart city environment. in 2017 International smart cities conference (ISC2). 2017. IEEE.
15. Matluba Khodjaeva, Muath A. Obaidat, and Douglas Salane "Mitigating Threats and Vulnerabilities of RFID in IoT through Outsourcing Computations Using Public Key Cryptography" In Security, Privacy and Trust in the IoT Environment. Springer, Cham, Switzerland. July 2019
16. Yang, S., et al., Optimization of heterogeneous clustering routing protocol for internet of things in wireless sensor networks. 2022. 2022: p. 1-9.
17. De Montjoye, Y.-A., et al., openpds: Protecting the privacy of metadata through safeanswers. 2014. 9(7): p. e98790.
18. Novo, Oscar. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. 5. 1184-1195.

19. M. Abouali, K. Sharma and T. Saadawi, "Blockchain-Based Solution for Patient Controlled Health Records Sharing for Private Decentralized Storage," Edited Book: Advanced AI and Internet of Health Things Technologies for Combating Pandemic, Springer 2023. eBook ISBN 978-3-031-28631-5. Print ISBN978-3-031-28630-8.
20. Nakamoto, S.J.D.b.r., Bitcoin: A peer-to-peer electronic cash system. 2008: p. 21260.
21. Khordadpour, P., & Ahmadi, S. (2024). Security and Privacy Enhancing in Blockchain-based IoT Environments via Anonym Auditing. ArXiv. /abs/2403.01356
22. Pilkington, M., Blockchain technology: principles and applications, in Research handbook on digital transformations. 2016, Edward Elgar Publishing. p. 225-253.
23. Morgan, J.J.E.l.A.h.w.j.c.c.U.E.Q., Quorum, advancing Blockchain technology. 2018.
24. Anees, Tayyaba, Qaiser Habib, Ahmad Sami Al-Shamayleh, Wajeeha Khalil, Muath A. Obaidat, and Adnan Akhunzada. 2023. "The Integration of WoT and Edge Computing: Issues and Challenges" Sustainability 15, no. 7: 5983.
25. M. Abouali, K. Sharma and T. Saadawi, "Patient Full Control over Secured Medical Records Transfer Framework Based on Blockchain," 2022 International Conference on Electrical Engineering and Informatics (ICELTICs), 2022, pp. 43-48,
26. Fernández-Caramés, T.M. and P.J.I.A. Fraga-Lamas, A Review on the Use of Blockchain for the Internet of Things. 2018. 6: p. 32979-33001.
27. Krco, S., D. Cleary, and D. Parker. P2P mobile sensor networks. in Proceedings of the 38th Annual Hawaii International Conference on System Sciences. 2005. IEEE.
28. Seok, B., J. Park, and J.H.J.A.S. Park, A lightweight hash-based Blockchain architecture for industrial IoT. 2019. 9(18): p. 3740.
29. Zheng, Z., et al., Blockchain challenges and opportunities: A survey. 2018. 14(4): p. 352-375.
30. Aljabhan, Basim, and Muath A. Obaidat. 2023. "Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO)" Sustainability 15, no. 8: 6905.
31. Feng, Q., et al., A survey on privacy protection in Blockchain system. 2019. 126: p. 45-58.
32. Lo, S.K., et al., Analysis of Blockchain solutions for IoT: A systematic literature review. 2019. 7: p. 58822-58835.
33. Dai, Hong-Ning & Zheng, Zibin & Zhang, Yan. (2019). Blockchain for Internet of Things: A Survey.
34. Wu, M., et al., A comprehensive survey of Blockchain: From theory to IoT applications and beyond. 2019. 6(5): p. 8114-8154.
35. Da Xu, L., W. He, and S.J.I.T.o.i.i. Li, Internet of things in industries: A survey. 2014. 10(4): p. 2233-2243.
36. Muath A. Obaidat and Joseph Brown, “Perspectives of Blockchain in Cybersecurity”, In Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector. IGI Global Publisher, Pennsylvania, USA. Feb. 2023.
37. Khan, M.A. and K.J.F.g.c.s. Salah, IoT security: Review, Blockchain solutions, and open challenges. 2018. 82: p. 395-411.
38. Ferrag, M.A., et al., Blockchain technologies for the internet of things: Research issues and challenges. 2018. 6(2): p. 2188-2204.
39. Makhdoom, I., et al., Blockchain’s adoption in IoT: The challenges, and a way forward. 2019. 125: p. 251-279.
40. Ali, M.S., et al., Applications of Blockchains in the Internet of Things: A comprehensive survey. 2018. 21(2): p. 1676-1717.
41. Yang, R., et al., Integrated Blockchain and edge computing systems: A survey, some research issues and challenges. 2019. 21(2): p. 1508-1532.
42. Viriyasitavat, W., et al., Blockchain technology for applications in internet of things—mapping from system design perspective. 2019. 6(5): p. 8155-8168.
43. Sengupta, J., et al., A comprehensive survey on attacks, security issues and Blockchain solutions for IoT and IIoT. 2020. 149: p. 102481.
44. Taylor, P.J., et al., A systematic literature review of Blockchain cyber security. 2020. 6(2): p. 147-156.
45. M. Abouali, K. Sharma, O. Ajayi, and T. Saadawi, "Blockchain Framework for Secured On-Demand Patient Health Records Sharing," 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 0035-0040

46. M. D. J. Peters, C. M. Godfrey, H. Khalil, P. McInerney, D. Parker, and C. B. Soares, “Guidance for conducting systematic scoping reviews,” Int. J. Evidence-Based Healthcare, vol. 13, no. 3, pp. 141–146, 2015.
47. Atlam, H.F., et al., A Review of Blockchain in Internet of Things and AI. 2020. 4(4): p. 28.
48. Kumar, R.L., et al., A survey on Blockchain for industrial internet of things. 2022. 61(8): p. 6001-6022.
49. Uddin, M.A., et al., A survey on the adoption of Blockchain in iot: Challenges and solutions. 2021. 2(2): p. 100006.
50. Tran, N.K., et al., Integrating Blockchain and Internet of Things systems: A systematic review on objectives and designs. 2021. 173: p. 102844.
51. Nasir, M.H., et al., Scalable Blockchains—A systematic review. 2022. 126: p. 136-162.
52. Al Sadawi, A., M.S. Hassan, and M.J.I.A. Ndiaye, A survey on the integration of Blockchain with IoT to enhance performance and eliminate challenges. 2021. 9: p. 54478-54497.
53. Panarello, A., et al., Blockchain and iot integration: A systematic survey. 2018. 18(8): p. 2575.
54. Al-Megren, S., et al. Blockchain use cases in digital sectors: A review of the literature. in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2018. IEEE.
55. Wang, X., et al., Survey on Blockchain for Internet of Things. 2019. 136: p. 10-29.
56. Sultan, A., M.A. Malik, and A.J.A.J.C.S.I.T. Mushtaq, Internet of Things security issues and their solutions with Blockchain technology characteristics: A systematic literature review. 2018. 6(3): p. 27.
57. Brotsis, S., et al., On the suitability of Blockchain platforms for IoT applications: Architectures, security, privacy, and performance. 2021. 191: p. 108005.
58. Jesus, E.F., et al., A survey of how to use Blockchain to secure internet of things and the stalker attack. 2018. 2018.
59. Alfandi, O., et al., A survey on boosting IoT security and privacy through Blockchain: Exploration, requirements, and open issues. 2021. 24: p. 37-55.
60. Butun, I. and P.J.I.A. Österberg, A review of distributed access control for Blockchain systems towards securing the internet of things. 2020. 9: p. 5428-5441.
61. Alamri, M., N. Jhanjhi, and M.J.I.J.C.S.N.S. Humayun, Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. 2019. 19(1): p. 244-258.
62. Da Xu, L., Y. Lu, and L.J.I.I.o.T.J. Li, Embedding Blockchain technology into IoT for security: A survey. 2021. 8(13): p. 10452-10473.
63. Salimitari, M., M. Chatterjee, and Y.P.J.I.o.T. Fallah, A survey on consensus methods in Blockchain for resource-constrained IoT networks. 2020. 11: p. 100212.
64. Uddin, M.; Selvarajan, S.; Obaidat, M.; Arfeen, S.U.; Khadidos, A.O.; Khadidos, A.O.; Abdelhaq, M. “From Hype to Reality: Unveiling the Promises, Challenges and Opportunities of Blockchain in Supply Chain Systems.” Sustainability Journal. 2023, 15, 12193.
65. Patil, P., M. Sangeetha, and V.J.W.P.C. Bhaskar, Blockchain for IoT access control, security and privacy: a review. 2021. 117: p. 1815-1834.
66. Huo, R., et al., A comprehensive survey on Blockchain in industrial internet of things: Motivations, research progresses, and future challenges. 2022. 24(1): p. 88-122.
67. Ali, J., et al. Blockchain-based smart-IoT trust zone measurement architecture. in Proceedings of the International Conference on Omni-Layer Intelligent Systems. 2019.
68. Pieroni, A., N. Scarpato, and L.J.A.S. Felli, Blockchain and IoT convergence—a systematic survey on technologies, protocols and security. 2020. 10(19): p. 6749.
69. Kumar, R., & Sharma, R. (2022). Leveraging Blockchain for Ensuring Trust in IoT: A Survey. Journal of King Saud University—Computer and Information Sciences, 34, 8599-8622.
70. Lao, L., et al., A survey of IoT applications in Blockchain systems: Architecture, consensus, and traffic modeling. 2020. 53(1): p. 1-32.
71. Reyna, A., et al., On Blockchain and its integration with IoT. Challenges and opportunities. 2018. 88: p. 173-190.
72. M. Abouali, K. Sharma, O. Ajayi, and T. Saadawi, "Performance Evaluation of Secured Blockchain-Based Patient Health Records Sharing Framework," 2022 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp

doi:10.20944/preprints202409.1193.v

73. Noby, D.A. and A. Khattab. A survey of Blockchain applications in IoT systems. in 2019 14th International Conference on Computer Engineering and Systems (ICCES). 2019. IEEE.
74. Shehzad, K., et al. Use of Blockchain in internet of things: A systematic literature review. in 2019 Cybersecurity and Cyberforensics Conference (CCC). 2019. IEEE.
75. Khor, J.H., M. Sidorov, and P.Y.J.I.I.o.T.J. Woon, Public Blockchains for resource-constrained iot devices—a state-of-the-art survey. 2021. 8(15): p. 11960-11982.
76. Moin, S., et al., Securing IoTs in distributed Blockchain: Analysis, requirements and open issues. 2019. 100: p. 325-343.
77. Mohanta, B.K., et al., Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and Blockchain technology. 2020. 11: p. 100227.
78. Anand, M.V. and S. Vijayalakshmi. A Survey on Blockchain Adaptability in IoT Environments. in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2021. IEEE.
79. Kumari, A., R. Gupta, and S.J.C.C. Tanwar, Amalgamation of Blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. 2021. 172: p. 102-118.
80. Ferrag, M.A., et al., Security and privacy for green IoT-based agriculture: Review, Blockchain solutions, and challenges. 2020. 8: p. 32031-32053.
81. Azbeg, K., et al., A taxonomic review of the use of IoT and Blockchain in healthcare applications. 2022. 43(5): p. 511-519.
82. Liang, W. and N.J.C.C. Ji, Privacy challenges of IoT-based Blockchain: a systematic review. 2022. 25(3): p. 2203-2221.
83. Chowdhury, M.J.M., et al., A survey on Blockchain-based platforms for IoT use-cases. 2020. 35: p. e19.
84. Chen, F., et al., Blockchain for Internet of things applications: A review and open issues. 2020. 172: p. 102839.
85. Hasan, W.K., A.M. Abood, and M. Habbal. A Review of Blockchain-based on IoT applications (challenges and future research directions). in 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA). 2020. IEEE.
86. Lin, J., et al. Using Blockchain and IoT technologies to enhance intellectual property protection. in Proceedings of the 4th International Conference on Crowd Science and Engineering. 2019.
87. Karthikeyyan, P. and S. Velliangiri. Review of Blockchain based IoT application and its security issues. in 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). 2019. IEEE.
88. Mezquita, Y., et al., Blockchain technology in IoT systems: review of the challenges. 2019: p. 2516-0281.
89. Ye, C., W. Cao, and S.J.T.o.E.T.T. Chen, Security challenges of Blockchain in Internet of things: Systematic literature review. 2021. 32(8): p. e4177.
90. Alfrhan, A., et al., Comparative study on hash functions for lightweight Blockchain in Internet of Things (IoT). 2021. 2(4): p. 100036.
91. Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through Blockchain: Exploration, requirements, and open issues. Cluster Computing, 24, 37-55.
92. Tao, F., Wang, Y., Zuo, Y., Yang, H., & Zhang, M. (2016). Internet of Things in product life-cycle energy management. Journal of Industrial Information Integration, 1, 26-39.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.