

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository: <https://orca.cardiff.ac.uk/id/eprint/170523/>

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Khan, Imran, Majib, Yasar, Ullah, Rehmat and Rana, Omer 2024. Blockchain applications for Internet of Things - a survey. Internet of Things 27 , 101254. 10.1016/j.iot.2024.101254

Publishers page: <http://dx.doi.org/10.1016/j.iot.2024.101254>

Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See <http://orca.cf.ac.uk/policies.html> for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.



Blockchain Applications for Internet of Things – A Survey

Imran Khan^a, Yasar Majib^a, Rehmat Ullah^b, Omer Rana^a

^a*School of Computer Science and Informatics, Cardiff University, UK*

^b*Department of Computer Science, Cardiff Metropolitan University, UK*

Abstract

In recent years, the Internet of Things (IoT) has been shaping our lives through billions of internet based interconnected devices. However, due to the decentralized nature of these devices, security, privacy, trust, and traceability remain major concerns. Blockchain is a distributed ledger technology used across several application domains, with features such as immutability and distribution. This survey describes how blockchains can support IoT based systems. We also identify key challenges in using blockchains in IoT, such as scalability, energy consumption, data privacy and security, integration complexity, and regulatory compliance. A comparative analysis of current blockchain scalability solutions and lightweight encryption algorithms is also presented; providing research gaps that still need to be addressed.

Keywords: Blockchain, Internet of Things, Security, Trust, Traceability, Scalability

1. Introduction

The *Internet of Things* (IoT) [1] connecting physical devices to the internet is a fast growing industry. These connected gadgets range from wearable and home appliances to industrial equipment and sensors [2, 3, 4]. The resultant connectivity and generated data serve various purposes, e.g., increase productivity, cut expenses, and enhance user experience. IoT devices are vulnerable to security risks including hacking and data leaks [5, 6, 7]. The decentralized nature of these IoT devices makes it challenging to secure them through conventional security techniques.

Blockchain technology [8] which was originally developed for cryptocurrencies, e.g., Bitcoin [9], has found application in a variety of domains [10, 11, 12]. Blockchain offers a decentralized and distributed ledger that can be used to securely and openly store data and transactions. It is built on consensus mechanisms [13] that make certain that all network nodes agree on the legitimacy of transactions. Depending on the extent of access and control given to various network participants, the blockchain can be categorized as public, private, or hybrid [14]. It also enables the use of smart contracts [15], which can automate the execution of agreements between IoT devices.

The use of blockchain for various IoT based applications is gaining much popularity [16, 17]. Researchers [18, 19] are working on blockchain based solutions to safeguard IoT devices, protect data privacy, and build trust between IoT devices. Blockchain has a significant impact on different sectors e.g., healthcare, financial industry, supply chain management (SCM), and energy management. Consequently, it will ensure a secure [20] platform and greater trust [19] among IoT network participants. Interoperability, security, cost, and scalability issues [21, 22, 23] are current challenges to the successful integration of blockchain and IoT.

The security, privacy, trust, and traceability of IoT data is an important issue and demands innovative solutions. In this survey paper, we present a comprehensive review of the current research on the application of blockchain technology for mitigating security and privacy, trust, and traceability issues in IoT environments. One of the key challenges of the current blockchain technology is the scalability issue of blockchain platforms. This survey also provides a detailed review of current blockchain scalability solutions. IoT devices limited storage and processing capabilities demand lightweight encryption algorithms for data security and privacy. A comprehensive review of lightweight encryption algorithms for IoT environments is also presented in this paper.

Table 1: Comparison with other surveys

References	Year	Security	SPTT	Blockchain Platforms	Lightweight Encryption	Interoperability	Scalability Review	Application
Minhaj et al. [24]	2018	✓		✓				
Bhabendu et al. [25]	2019	✓		✓				✓
Tejasvi et al. [26]	2019	✓		✓		✓		✓
Muhammad et al. [27]	2019	✓		✓		✓		✓
Chong et al. [28]	2020	✓				✓		✓
Dedeoglu et al. [29]	2020	✓		✓		✓	✓	✓
Li et al. [30]	2021	✓		✓		✓		
Ramamoorthi et al. [31]	2021	✓						✓
Abraham et al. [32]	2021	✓						✓
Sujith et al. [33]	2022	✓				✓		
Mohammad et al. [34]	2022	✓						
Rajesh et al. [35]	2022	✓				✓		
Dimitris et al. [36]	2023	✓				✓		✓
Wael et al. [37]	2023	✓				✓		
Sa'ed et al. [38]	2023	✓				✓		✓
Haider et al. [39]	2023	✓		✓				✓
Saqib et al. [40]	2024	✓		✓				
Hadi et al. [41]	2024	✓		✓		✓		✓
Our Survey	2024	✓	✓	✓	✓	✓	✓	✓

This survey also discusses the underlying concepts of blockchain, IoT, and the security aspects of blockchain and IoT. Our survey also investigates the current challenges of blockchain based IoT integration and provides comprehensive insights into future trends and research directions. There are some other surveys that also focus on the application of blockchain in IoT environments. Table 1 shows the comparative analysis of our survey with other related surveys. Minhaj et al. [24] discuss security issues in IoT and the use of blockchain for handling security issues in IoT. However, this survey ignores the Interoperability issues and scalability aspects of blockchain technology for IoT environments. Bhabendu et al. [25] survey blockchain applications in various domains, e.g., healthcare, financial, IoT, and power grid. However, this is a more generic survey and ignores how blockchain can be beneficial in addressing the security and privacy issues of IoT environments. Dedeoglu et al. [29] review the application of blockchain in IoT and provide a generic view of blockchain scalability issues. However, this study lacks a detailed scalability review. Li et al. [30] survey presents state of art blockchain based IoT security with a focus on security features and issues. This survey is more focused on embedded IoT systems. A survey on blockchain and federated learning based intrusion detection in industrial IoT is presented in [40]. This survey mainly focuses on blockchain based distributed federated learning in industrial IoT environments. A survey on the use of post-quantum cryptosystems for ensuring post-quantum blockchain security for IoT is explored in [41]. The given survey also provides insights into recent blockchain based IoT applications. Our survey literature lists further blockchain based IoT works, including Sujith et al. [33], Rajesh et al. [35], Dimitris et al. [36], and Haider et al. [39].

It is evident from Table 1 that these surveys only discuss a subset of dimensions that merit discussion. This survey will offer a useful resource for researchers and practitioners interested in blockchain and IoT integration. The following are the key contributions of our survey:

- Overview of blockchain and IoT with their security and limitations.
- A detailed comparative analysis of blockchain scalability solutions and lightweight encryption algorithms.
- A comprehensive review of current blockchain based solutions for handling security and privacy, trust, and traceability issues in IoT environments.
- A detailed discussion on blockchain applications in various IoT related domains.
- Rigorous insights into the current limitation of blockchain and IoT integration and future direction for its successful mitigation.

Table 2 lists acronyms with their meaning used in this paper. The paper is organized as illustrated in Fig. 1. Section 2 provides an overview of the key components and fundamentals of IoT and blockchain technology, including its key features and current state of development. Section 3 discusses blockchain scalability solutions and lightweight

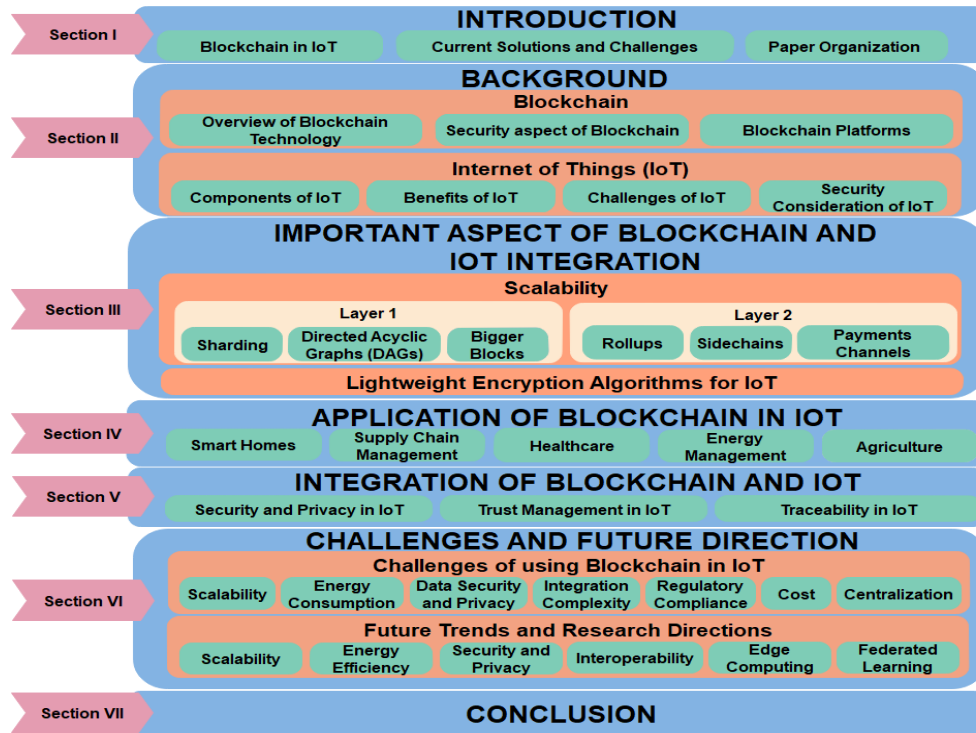


Figure 1: Paper structure

encryption algorithms. Section 4 outlines the detailed application of blockchain in IoT domain. Section 5 provides a review of blockchain based solutions for security, trust, and traceability in IoT environments. Section 6 describes the current challenges of blockchain and IoT integration with future trends and research directions. Finally, Section 7 summarizes the paper.

2. Background

2.1. Blockchain

2.1.1. Overview of Blockchain Technology

Blockchain is a decentralized method of recording information in a permanently verifiable and organized way so that anyone on the internet can see the entire history of information in a given data set, thus allowing access to information anywhere in the world. In essence, a blockchain is a digital ledger [42] of all transactions. Blockchain is continuously growing as newly completed blocks are appended with a new sequence of transactions. Each new block contains at minimum previous block cryptographic hash [43] as well as transaction related data, as shown in Fig. 2. The initial block of a blockchain is often designated as a genesis block. A newly created block is added to the blockchain and can never be changed or removed. This is because each block in a blockchain includes a cryptographic hash of the preceding block, as well as a timestamp. Changing any information in a block would cause the hash to change, which would invalidate all subsequent blocks. We recommend the readers to [44], on technical details on blockchain. The three most important characteristics of blockchain include:

- **Decentralization:** Contrary to traditional systems [45], blockchain is decentralized. There is no central authority, and the control is distributed across nodes of the network.
- **Security:** Blockchain is a highly secure concept based on cryptography and consensus mechanisms. This implies once data is stored on the blockchain, it cannot be changed or altered maliciously without tampering being detected.

Table 2: List of acronym

Acronym	Phrase
IIoT	Industrial Internet of Things
SPTT	Security and Privacy, Trust, and Traceability
PoW	Proof of Work
PoS	Proof of Stake
PoA	Proof of Authority
DPoS	Delegated Proof-of-Stake
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
IBFT	Istanbul Byzantine Fault Tolerance
PoTC	Proof of Trust Collaboration
DAG	Directed Acyclic Graph
ZK	Zero-Knowledge
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
ECC	Elliptic Curve Cryptography
HMAC	Hash-based Message Authentication Code
SCM	Supply chain management
EHR	Electric Health Record
ABAC	Attribute based Access Control
CP-ABE	Ciphertext-Policy Attribute based Encryption
HIPAA	Health Insurance Portability and Accountability Act
PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation
SSI	Self-Sovereign Identity
ISO/IEC	International Organization for Standardization/International Electro-technical Commission
IoV	Internet of vehicle
MAST	Merkleized Abstract Syntax Trees

- **Transparency:** Blockchain is also a transparent technology, as transaction data is publicly available and can easily be verified.

Blockchain can be categorized into three broad categories: public, private, and hybrid. Public blockchain also known as permissionless [46], allows anyone to join and access the blockchain network. A private blockchain known as a permissioned blockchain [47], allows only the participating entities and organizations to access and perform transactions in the blockchain network. A private blockchain is meant for organizations where privacy is a major requirement. In a hybrid blockchain, a separate chain is maintained for both public and private blockchains. Blockchain is composed of the following key components:

- **Transactions:** Transactions are operations performed on the current state of the blockchain.
- **Blocks:** Transactions are grouped into blocks and are then added to the blockchain. Each block is cryptographically connected to the previous block, thus creating an unbroken chain of blocks.
- **Nodes:** Users and organizations participate in a blockchain network through nodes [48]. Transactions are also initiated and processed through nodes. A copy of the blockchain is maintained by organization nodes.
- **Consensus Mechanism:** Legitimacy of blocks and transactions is achieved through a consensus mechanism. These are agreed-upon ways through which blocks are added to the blockchain by participating organizations.
- **Cryptography:** The security and immutability of blockchain networks are achieved through various cryptographic primitives, e.g., digital signature [49], encryption [50], and hashing.

2.1.2. Security aspect of Blockchain

One of the key aspects of blockchain is security. Blockchain security guarantees are the result of various elements such as cryptography and consensus mechanisms. It is impossible to maliciously change data in the blockchain network since blocks are connected through a cryptographic mechanism known as a hash function. Public-key cryptography [51] is another cryptographic mechanism used to secure blockchain transactions. In Public-key cryptography,

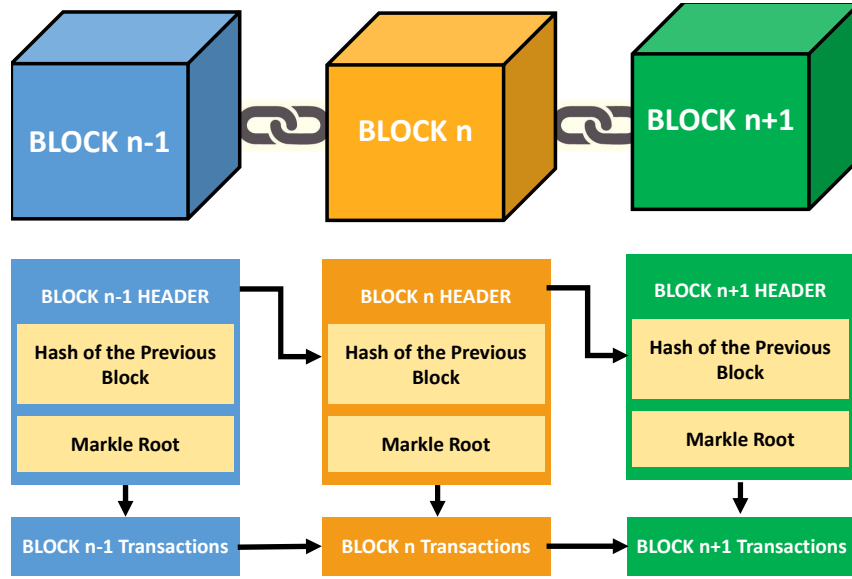


Figure 2: Blockchain structure

each network participant has a unique public and private key pair. The private key is typically used to sign a transaction whereas the signature is verified through the corresponding public key. This guarantees that only the owner of a private key can initiate a transaction.

The consensus mechanism is another important security aspect of blockchain technology to validate transactions. The consensus mechanism requires agreement between network participants before a transaction can be validated and added to the blockchain. Therefore, a single entity cannot maliciously change the status of the blockchain. The status of the blockchain is protected by the agreement between all network participants. Besides these core features, some additional security mechanisms can be implemented according to the given requirements. For instance, multi-factor authentication [52], digital signatures, and access controls [53] mechanisms can be used to protect blockchain networks from unauthorized users.

Recently, researchers have focused on designing new lightweight consensus protocols to meet the distinct needs of resource constraint IoT environments. Li et al. [54] proposed a reinforcement learning based delegated PoS (DPoS) consensus mechanism called QV-DPoS. This fast and lightweight consensus protocol for IoT environments improves the DPoS consensus mechanism in terms of efficiency, energy consumption, and trust management. Another lightweight consensus protocol for IoT environments is proposed in [55]. They have shown that their proposed mechanism reduces communication volume by 74.53%, storage capacity by 98.16%, and block verification time by 87% when compared with the Ethereum blockchain. Zhao et al. [56] suggested model based evolutionary lightweight consensus protocol called Proof of Evolutionary Model (PoEM) for BaaS (blockchain-as-a-service) IoT environments. PoEM achieves and boosts consensus efficiency by iteratively training a machine learning model for consensus. Other promising work related to lightweight consensus protocol for IoT based environments includes HLOChain [57] and LightBlocks [58].

Despite these security guarantees, blockchain technology is still subject to various security threats. Some of the potential threats to blockchain technology include:

- 51% attack [59]: This attack can be launched if a single entity or some small group of network miners control the bulk of hashing or processing power. The current state of the blockchain can then be altered by maliciously adding or removing transactions. 51% attacks are typically linked with public blockchains such as Bitcoin or Ethereum. Private blockchains with their centralized governance, permissioned access, and different incentives, making it one of their advantages over public blockchains.
- Sybil attack [60]: When an attacker generates numerous false identities in the network to take over the consensus mechanism.

- Smart contract vulnerabilities: Smart contracts execute transactions on a blockchain network. If there are some vulnerabilities [61] in a smart contract, then intruders can use them to maliciously change the state of a blockchain network.
- Private key management: Entities use private keys to initiate transactions and get access to the blockchain network. If an entity's private key is stolen by an intruder, it can be used to execute a malicious transaction on a blockchain network.

2.1.3. Blockchain Platforms

The first blockchain platform Bitcoin was introduced for financial purposes facing various challenges such as speed and energy consumption. Due to Bitcoin's financial nature and various challenges, many new platforms have been introduced to meet the diversified needs of the growing blockchain industry. The following are the most popular blockchain platforms introduced over the years.

- Bitcoin [62]: Bitcoin is the pioneer and one of the leading cryptocurrency public blockchain platforms. Bitcoin is based on the Proof-of-Work (PoW) consensus mechanism [63], where miners compete to solve a cryptographic puzzle to generate new blocks and confirm transactions. Due to the emergence of new efficient consensus mechanisms, PoW is now considered a computation and energy-intensive mechanism.
- Ethereum [64]: Ethereum is the second most well-known cryptocurrency based public blockchain platform. Ethereum is a decentralized public blockchain that supports distributed applications to securely share and access information worldwide. Ethereum was originally based on the PoW consensus algorithm. Recently, Ethereum has shifted to a more computation and energy-efficient Proof-of-Stake (PoS) consensus mechanism [65]. In PoS consensus, new blocks are generated by validators with high stakes in the network instead of solving cryptographic puzzles.
- Hyperledger Fabric [66]: Hyperledger Fabric is a private blockchain hosted by Linux Foundation. The modular architecture of Hyperledger Fabric supports a configurable consensus mechanism that implements smart contracts as *chain-code*. Due to its modular architecture, Hyperledger Fabric is ideal for use in a variety of application domains. Hyperledger Fabric is based on the Byzantine Fault Tolerance (BFT) consensus mechanism [67].
- Quorum [68]: Quorum is a JP Morgan fork of the Ethereum blockchain. Quorum provides support for various Proof-of-Authority (PoA) consensus mechanisms [69], which include QBFT [70], IBFT [71], and Raft [72]. Although Ethereum is a public blockchain, Quorum is a private blockchain with a high transaction throughput and low latency due to an efficient consensus mechanism. Besides private transactions, Quorum also provides support for privacy-enhanced transactions. Quorum uses a separate component known as privacy manager to support private transactions.
- Corda [73]: Corda is also a private blockchain design specifically for financial institutions. Corda can also be used in other domains, e.g., energy, insurance, and healthcare. Corda is based on a BFT-type consensus mechanism known as Notary. Notary introduces a network of validators to avoid double-spending [74] and order transactions.

2.2. Internet of Things (IoT)

IoT is a network of physical objects and sensors that collect, share, and transmit data through the internet. For instance, a smart device can be used to measure and adjust heating inside a room or building. These smart devices can be controlled remotely using a smartphone app. IoT enables an interconnected environment through the generation and sharing of information in real time without human intervention. This can benefit both individuals and businesses to make better-informed decisions. IoT devices such as sensors, microcontrollers, actuators, and communication devices collect data from their local operating environment. The data is then sent to external storage such as the cloud [75] for further processing, analysis, decision-making, and analytics.

2.2.1. Components of IoT

The operating environment of IoT can include buildings, automobiles, industrial units, and entire cities. The key components of IoT include:

- **Devices/Sensors:** Devices and sensors are one of the core elements of IoT that collect and then transmit data to the local storage devices or cloud for further processing and decision-making. These devices can be of different sizes and shapes depending on their attachment to the objects which include vehicles, wearable devices, home appliances, and industrial equipment. These devices and sensors can collect various types of data which include humidity, temperature, location, environmental, and performance related data [76].
- **Connectivity:** IoT devices have limited storage, power, and processing capabilities. Therefore, it needs connectivity to communicate with other local devices and transmit its generated data to the cloud for storage and processing purposes. IoT devices can use a variety of technologies, e.g., Bluetooth, Zigbee, Wi-Fi, and cellular networks for connectivity and data transmission purposes.
- **Cloud:** IoT data can be transferred to the cloud for storage, processing, security, and analytics purposes. IoT data is normally in raw form, therefore, further processing on the cloud may be required to make data understandable. Data processing can include transforming, cleaning, and aggregation. Similarly, data analytics [77] may be required to gain meaningful insights from the sensors-generated data. Therefore, IoT technology can benefit from various cloud based services which include Amazon Web Services [78], Microsoft Azure [79], and Google Cloud Platform services [80].
- **Applications:** IoT generated data are used and consumed by users through different IoT applications. These applications can range from asset tracking, home automation, and industrial automation to energy management based applications.

IoT devices and sensors with advanced technology provide various benefits in various domains including improved decision making, user experience, efficiency, and cost reduction. IoT enables data processing in real time to support a personalized, interactive, and better user experience. We can automate tasks and processes to increase efficiency and minimize human intervention in various domains. Besides these benefits, IoT also faces many challenges including security [24], interoperability, privacy, data management, and scalability [21, 22, 23]. The operating environment of IoT makes it vulnerable to various security risks and threats. Despite the various benefits and advancements, IoT technology still faces several challenges. The most significant challenges include security, interoperability, privacy, data management, and scalability. Lack of standardization [81] and diversity of communication protocols in IoT environment leads to Interoperability issues. Secure storage, transmission, and processing of huge volumes of data generated by IoT devices also become a real challenge.

2.2.2. Benefits and challenges of IoT

IoT devices and sensors have many advantages in diverse application domains and have improved decision making, user experience, efficiency, and cost reduction. The IoT facilitates the interaction with real time data to help offer a more personalized, interactive, and better user experience. We can automate tasks and processes in several domains to increase efficiency and minimize human intervention. Besides these benefits, there are numerous challenges that IoT faces, such as security [24], interoperability, privacy, data management, and scalability [21, 22, 23]. The operating environment of IoT is vulnerable to many security risks and threats. Nonstandardization [81] and diversity in communication protocols in the IoT environment are the main causes of the interoperability problems. Secure storage, transmission, and processing of huge amounts of data produced by devices in an IoT environment can also become a real challenge.

2.2.3. Security Consideration of IoT

The Internet of Things (IoT) has revolutionized our lives in many ways. However, due to IoT devices nature and operating environment, it also presents several security risks. The following are key security considerations for IoT:

- **Data privacy:** Data collected and transmitted by IoT devices (without proper anonymization and encryption) in sensitive environments such as healthcare and government can raise privacy concerns. Therefore, data should be protected from unauthorized access, and proper privacy regulations [82, 83] should be followed.
- **Device security:** Normally, IoT devices limited processing and storage capabilities make it challenging to configure them with traditional security software. Additionally, it may also be difficult to apply patches due to the remote locations of these devices. Therefore, it is essential to protect IoT devices from both physical and software based attacks.
- **Network security:** The communication channels used by IoT devices are mostly unsecured which makes the transmission of data vulnerable to different types of attacks, e.g., unauthorized access, data loss, and data modification. Consequently, it is essential to apply different security based measures to protect communication network from intruders and attackers.
- **Authentication and authorization:** As the number of IoT devices connected to a given IoT network increases, authentication and authorization become more challenging. Ensuring proper authentication and authorization in crowded networks is important to protect a network and its resources from intruders
- **Physical security:** IoT devices normally operate in an open environment, therefore, physical assaults become a significant threat. Therefore, physical access to devices and their firmware should be protected from attackers.

2.2.4. Integrating Blockchain with IoT Standards

Many researchers have explored the benefits of integrating blockchain with existing IoT standards. A detailed review of such schemes is presented in [84]. A blockchain based mechanism to boost the security of Constrained Application Protocol (CoAP) nodes is explored in [85]. The authors have used the COAP framework in combination with Ethereum to enhance the security of the Resource Directory (RD). DRDChain [86] suggests a lightweight blockchain framework in a CoAP network to cater to trust and reliability issues between devices and RDs. Trinity [87] attempts to integrate BC into IoT publish subscribe model. In Trinity, MQTT based network brokers execute a BFT based consensus in a permissioned blockchain to enhance application and processing IoT layers.

2.3. Lessons Learned: Summary and Insights

In this section, we have discussed blockchain technology and its enabling components and technologies. Although blockchain technology can be used to provide security based protection, caution is required in its widespread application as blockchain technology itself is vulnerable to various security based threats and attacks. We have also discussed IoT technology and its key components. While IoT provides various benefits, there are still various security and other challenges that need careful attention for the successful application of IoT in various domains.

3. Important Aspect of Blockchain and IoT Integration

In this section, we discuss in detail the most important aspects for the successful integration of blockchain and IoT, e.g., blockchain scalability and lightweight encryption. Blockchain scalability is an important aspect as blockchain networks need to efficiently handle large volumes of transactions and data generated by an increasing number of IoT devices. Lightweight encryption is important for the security and privacy of IoT devices because IoT devices have limited processing, storage, and memory capability.

3.1. Scalability

According to a survey [88], there are around 15 billion IoT devices worldwide and this growth is expected to increase further. The scalability of a blockchain network becomes significant in the context of rapidly increasing IoT devices and the amount of data they generate. Therefore, it becomes a central requirement for a blockchain network to process and handle large volumes of transactions and data of IoT devices in an efficient as well as secure fashion. The objective of blockchain scalability is to process a high number of transactions (e.g., throughput) without compromising the efficiency, security, and decentralization of a blockchain network. This becomes crucial for the smooth working of IoT environments to process data in a timely and secure fashion.

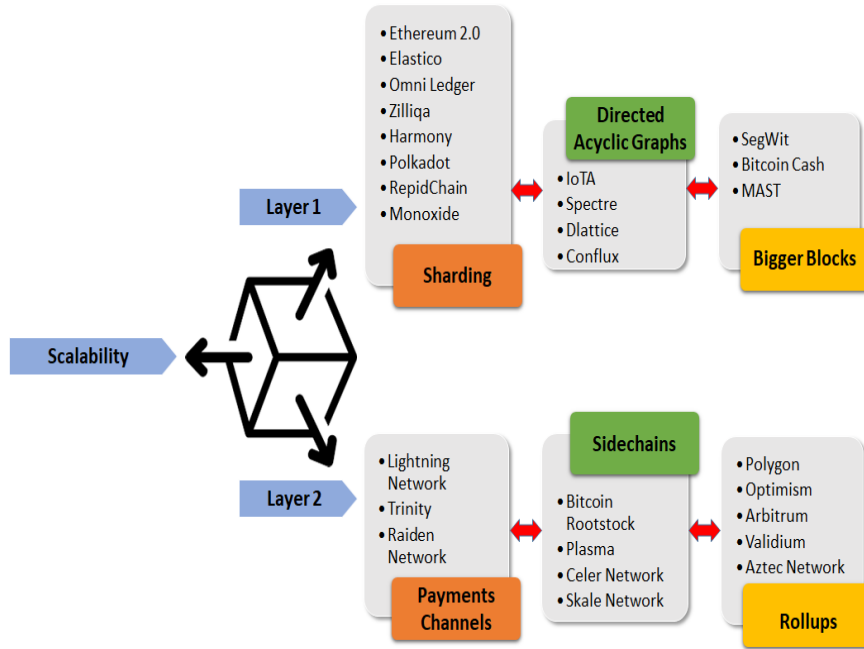


Figure 3: Blockchain scalability

Blockchain network scalability is dependent on several factors including block size, block time, network bandwidth, and transaction fees. Large blocks and faster block times can improve blockchain scalability but can result in network congestion and higher transaction fees. The integration of blockchain and IoT demands improvements in blockchain scalability. Blockchain scalability solutions can be categorized into layer 1 and layer 2 solutions as shown in Fig. 3. Blockchain layer 1 scalability solutions focus on the base layer of the blockchain network [89] whereas layer 2 solutions focus on off-chain solutions [90] built on top of layer 1. Layer 1 and layer 2 solutions and their combination are important for addressing scalability issues in blockchain based IoT environments. In this section, we provide a taxonomy of layer 1 and layer 2 blockchain scalability solutions and lightweight encryption algorithms for blockchain IoT environments.

3.1.1. Layer 1 Scalability

Blockchain layer 1 scalability solutions mainly focus on the base layer of a blockchain network and especially the consensus protocols [63, 69] used. Layer 1 solutions attempt to optimize the network architecture or underlying consensus algorithm to increase the throughput and scalability of a blockchain network. Layer 1 solutions either focus on increasing block size, reducing block creation time, or employing techniques such as sharding [106] to partition the blockchain into smaller and more manageable fragments. A comparative analysis of layer 1 blockchain scalability solutions is shown in Table 3.

Sharding. Sharding is a new emerging blockchain scalability solution that ensures processing more transactions per unit of time and high throughput. Sharding partitions the main blockchain network into several smaller but more manageable components known as shards as shown in Fig. 4. These shards have their own transaction history, state, and consensus mechanism and function as an independent blockchain network. Every transaction in a blockchain network is assigned to a designated shard. Nodes within a shard are then responsible for the processing and validation of these transactions. In situations where a transaction involves several shards, then an inter-shards communication occurs to verify that transaction. In this way, transactions can be executed more efficiently with validation achieved through a subset of blockchain nodes. Sharding based blockchain solutions include Ethereum 2.0 [91], Elastico [92], Omni Ledger [93], and Zilliqa [94].

Blockchain networks can benefit from sharding in several ways. Firstly, it enables high throughput by executing a high number of transactions in parallel. Secondly, it reduces the overall computational load of a blockchain network by validating transactions quickly. Thirdly, reducing computational load contributes to the environment-friendly

Table 3: Layer 1 blockchain scalability

Solution	Layer	Consensus	Throughput	Security	Decentralization
Sharding					
Ethereum 2.0 [91]	1	PoS	Medium	High	High
Elastico [92]	1	PBFT	Medium	High	High
Omni Ledger [93]	1	PoW, BFT	Excellent	High	High
Zilliqa [94]	1	PBFT	Excellent	High	High
Harmony [95]	1	PoS, FBFT	Excellent	High	High
Polkadot [96]	1	NPoS	Excellent	High	High
RapidChain [97]	1	PoW, BFT	Excellent	High	High
Monoxide [98]	1	PoW, Zones	Excellent	High	High
Directed Acyclic Graphs (DAGs)					
IoTA [99]	1	PoW,DAG	Good	High	High
Spectre [100]	1	PoW, DAG	Good	High	High
DLattice [101]	1	DPoS, DAG	Excellent	High	High
Conflux [102]	1	PoW, DAG	Excellent	High	High
Block size increase					
Segregated Witness (SegWit) [103]	1	PoW	Medium	High	High
Bitcoin Cash [104]	1	PoW	Excellent	Medium	High
MAST [105]	1	PoW	Excellent	High	High

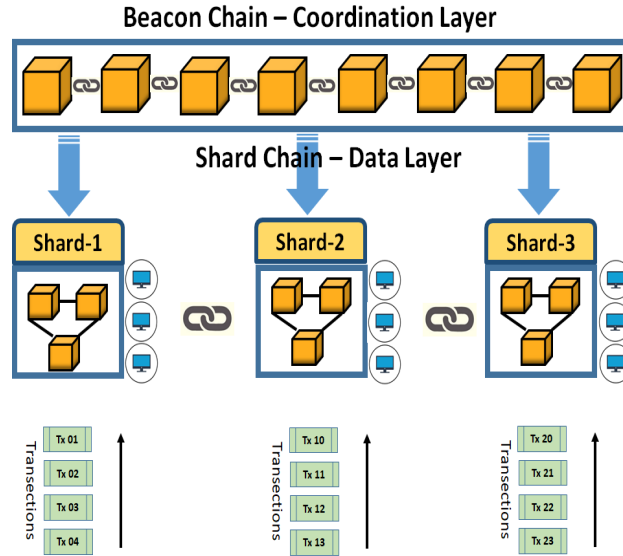


Figure 4: Blockchain scalability: Sharding

factor. Lastly, protection from an attacker is enhanced [107] as an attacker would need to compromise multiple shards simultaneously to launch a successful security attack. Shard chains execute independently and can be thought of as mini blockchains. Shard chains map their local transactions to the Beacon Chain (main chain) for security and consistency. Each shard will have its own validating nodes and transaction history. In this way, several shards can operate simultaneously in parallel to increase the overall throughput of a blockchain network.

Directed Acyclic Graphs (DAGs). Directed Acyclic Graph (DAG) is an alternate blockchain scalability solution besides conventional blockchain networks. DAG is based on a graph structure [108] to link transactions rather than creating a linear chain of interconnected transactions. The result is a more efficient and scalable blockchain network. In the DAG network, each transaction is connected to the previous transaction in a directed graph with no cycle. Transactions validated by the network nodes are added as a new node in the graph and it then points to the previous transaction through a directed edge. This links transactions together to create dependency and association between transactions.

The primary advantage of DAG is the processing of multiple transactions in parallel [109]. This feature allows to process and verify transactions independently and simultaneously without waiting for a single block. This results in a blockchain network with high speed and throughput. DAGs have the property to scale horizontally. Traditional

Table 4: Layer 2 blockchain scalability

Solution	Layer	Throughput	Security	Decentralization
Rollups				
Polygon (Matic) [115]	2	Excellent	High	High
Optimism [116]	2	Excellent	High	High
Arbitrum [117]	2	Excellent	High	High
Aztec Network [118]	2	Good	High	High
Loopring [119]	2	Excellent	High	High
Payments channels				
Lightning Network [120]	2	Excellent	High	High
Trinity [121]	2	Excellent	High	High
Raiden Network [122]	2	Excellent	High	High
Sidechains				
Bitcoin Rootstock [123]	2	Medium	High	High
Plasma [124]	2	Excellent	High	High
Celer Network [125]	2	Excellent	High	High
Skale Network [126]	2	Good	High	High

blockchains suffer from congestion due to an increase in transaction rates, resulting in throughput decrease and increase in transaction fees. DAGs are more scalable and high transaction throughput can be achieved by adding more nodes to the blockchain network. Some of the well-known DAG based blockchain networks include IOTA [99], Spectre [100], and DLattice [101].

Bigger Blocks. Current popular blockchains such as Bitcoin and Ethereum block size limits result in network bottlenecks and affect the networks overall throughput. Another solution to blockchain scalability is to use a bigger block size. The basic idea is that a bigger block will allow the processing of more transactions at a time and will result in increased network throughput. Temporary or permanent bigger blocks can be useful in a high network demand period and will increase throughput with possible reduced transaction fees. For instance, a fork of Bitcoin called Bitcoin Cash [104] has increased block size up to 32MB to achieve high throughput.

3.1.2. Layer 2 Scalability

Layer 2 scalability focuses on off-chain solutions built on top of layer 1 (a base layer of blockchain). Transactions are initially processed off-chain and then subsequently mapped into the main blockchain [110]. In this way, the load on the base layer is reduced, improving the scalability of the blockchain network. Layer 2 solutions include rollups, sidechains, and payment channels. A comparative analysis of layer 2 blockchain scalability solutions is shown in Table 4.

Rollups. Rollups are Layer 2 blockchain scalability solutions that allow for more transactions to be processed off-chain, reducing the load on the main blockchain and increasing scalability [111]. Rollups can be classified into two types, e.g., ZK Rollups (Zero-Knowledge Rollups) [112] and Optimistic Rollups [113].

ZK Rollups is based on Zero-Knowledge Proofs [114] to process transactions securely off-chain. ZK rollups first compress and batch transactions together into a unit proof and then subsequently map into the main blockchain. In this way, transactions are validated and processed using the generated proof without revealing details of transactions. A significant amount of transaction data is processed off-chain which improves overall network scalability. Additionally, ZK rollups ensure enhanced privacy and security as transaction data remains confidential. However, ZK rollups require technical expertise and computational resources for successful implementation.

Optimistic rollups are blockchain scalability solutions that are based on a different approach without using ZK proof. Optimistic Rollups process transactions off-chain and then subsequently map the transactions to the main chain for validations. It assumes that all transactions are valid until proven otherwise. A transaction is reverted if proven invalid and accordingly updating the rollups. Optimistic Rollups offer several benefits when compared to ZK rollups. Optimistic rollups are simpler to implement and consume fewer resources compared to ZK rollups. Also, it can handle high throughput in an overloaded environment. However, Optimistic rollups are vulnerable to various attacks and fraud [114] and are considered less secure when compared to their counterpart, e.g., ZK rollups. Both approaches have their benefits and limitations. The selection is subject to the specific requirements of a blockchain network.

Table 5: Lightweight encryption algorithms for IoT

Algorithm	Block Size	Key Size	Computational Efficiency	Mode of Operation	Type of Cipher
AES [129]	128 bits	128, 192, or 256 bits	Medium	Block cipher	Symmetric
SIMON [130]	32, 48, 64, 96, or 128 bits	256 bits	high	Block Cipher	Symmetric
PRESENT [131]	64 bits	80 to 128 bits	Medium	Block Cipher	Symmetric
SPECK [130]	32, 48, 64, 96, or 128 bits	64 to 256 bits	High	Block Cipher	Symmetric
RECTANGLE [132]	64 bits	80 to 128 bits	High	Block Cipher	Symmetric
KTANTAN [133]	32, 48, 0r 64 bits	80 bits	Medium	Block Cipher	Symmetric
ChaCha20 [134]	-	256 bits	Medium	Stream Cipher	Symmetric
LEA [135]	128	128, 192, or 256	High	Block Cipher	Symmetric
HIGHT [136]	64 bits	128 bits	High	Block Cipher	Symmetric
CLEFIA [137]	128 bits	128, 192, or 256 bits	Medium	Block Cipher	Symmetric
Pride [138]	64	128	High	Block Cipher	Symmetric

Sidechains or Child Chains. Sidechains or child chains is a blockchain scalability solution in which a separate blockchain known as a sidechain is created and operates independently but is linked to the main blockchain network. In this way, transactions are processed on the sidechain with the security and decentralization properties of the main blockchain intact. In sidechains, users can transfer their assets for trading and other purposes from the main chain to the sidechain. Assets on the side chains can be traded between users independently from the main chain. When required users can transfer their assets back to the main chain which is linked again to the user's accounts.

One of the primary benefits of these sidechains is that they can process a high number of transactions [127]. Transaction processing occurs on the sidechain, and the main blockchain can perform other tasks in parallel. The result is higher network throughput and lower transaction fees. Another benefit of sidechains is that they can be applied in a variety of areas, e.g., asset trading, gaming, and smart contract execution. Some of the well-known sidechains based blockchain network includes Bitcoin Rootstock [123], Plasma [124], Celer Network [125], and Skale Network [126].

Payment Channels. Payment Channels are blockchain based solutions to address traditional blockchain scalability challenges. In payment channels, a private channel is created between two parties that want to communicate through blockchain based networks. The participant of the payment channel is allowed to mutually perform blockchain transactions without broadcasting to the main blockchain at this stage. Payment channels are based on generating multi-signature addresses [128] on the blockchain controlled by both parties. The address is then top-up by both parties with some cryptocurrency to initialize the balance on the payment channel. The establishment of the channel can be followed by an unlimited number of transactions between parties. These transactions are recorded off-chain and are not committed to the main blockchain at this stage. Each off-chain transaction updates the balance of the channel and when the session is closed the final balance is then settled on the main blockchain. High throughput can be achieved through this mechanism as each transaction is not necessarily broadcast to the main blockchain network. Some of the well-known Payments Channels based blockchain network includes Lightning Network [120], Trinity [121] [120], and Raiden Network [122].

3.2. Lightweight Encryption Algorithms for IoT

Traditional general purpose encryption algorithms such as DES and AES [129] are not Ideal for IoT environments [139, 140] as these mechanisms are costly in terms of computation and memory requirements. Lightweight encryption algorithms are optimized for resource-constrained environments with a high level of security. Lightweight encryption algorithms are desirable to provide data security for IoT devices while minimizing the computational and memory overhead. IoT devices normally operate in hostile and distributed environments with diversified hardware and software configurations. Lightweight encryption can be easily implemented on a range of platforms and operating systems and will certainly contribute towards greater interoperability and standardization across various IoT devices. The low computational requirement of a lightweight encryption algorithm will also support standalone IoT devices with limited battery life. Several lightweight encryption algorithms have been proposed for IoT devices, including ChaCha20 [134], Speck [130], Simon [130], and PRESENT [131]. Many researchers [140, 141, 142, 143] have evaluated the

performance of lightweight encryption algorithms. A comparative review of lightweight encryption algorithms in terms of computational and memory efficiency is presented in Table 5.

3.3. Lightweight Cryptographic Schemes

Researchers are focusing on the design of new lightweight cryptographic protocols [144, 145] to meet the security needs of resource constraint IoT environments. A lightweight attribute based access control scheme for blockchain based IoT is proposed in [146]. The proposed scheme ensures the correctness of proxy re-encryption calculation using blockchain in an untrusted cloud environment. Yan et al. [147] presented a proof-of-work (PoW) mining with lightweight implementation and reconfigurable hardware primitives for blockchain IoT. The proposed scheme can considerably decrease power overheads and hardware resource requirements of PoW mining. The scheme uses efficient and secure hardware implementations instead of using classical blockchain hash and cryptographic functions. A lightweight authenticated encryption (AE) scheme for consensus in blockchain IoT is presented in [148]. The proposed scheme can be realized in hardware platforms (e.g., FPGA and ASIC) or software (e.g., microcontroller) with high throughput and scalability. Another lightweight authentication scheme for blockchain based IoT is proposed in [149]. The proposed scheme used a modular square root (MSR) algorithm for efficient and effective authentication in blockchain based IoT environments.

3.4. Lessons Learned: Summary and Insights

The growth in IoT devices and the volume of data they generate is on a high rise. To compete with this growth, recently many modifications to traditional blockchain mechanisms have been proposed to enhance the scalability of blockchain networks. We have summarized and provided a comprehensive analysis of blockchain scalability solutions. Traditional encryption algorithms are not suitable for IoT devices with limited storage and processing capabilities. A comparative analysis of lightweight encryption algorithms for an IoT environments is also present in this section.

4. Application of Blockchain in IoT

Blockchain features such as immutability, security, and decentralization make it ideal for overcoming security, trust, and traceability [150] issues in IoT. Therefore, blockchain technology has enormous potential for successful application in a variety of use cases in IoT domain. This section presents some useful applications of blockchain in IoT related domains as shown in Fig. 5.

4.1. Smart Homes

Blockchain technology has the potential to revolutionize the domain of smart homes ensuring safe and secure communication and sharing of data between smart home devices [151]. Following are some useful use cases for blockchain based smart homes.

- Decentralized energy trading: Nowadays many smart homes generate electricity using solar panels. Blockchain and IoT can be used to automate the trading of surplus energy without human intervention [152].
- Smart locks: Blockchain based decentralized authentication mechanisms [145] can be used to control access to smart homes. For instance, homeowners can remotely control access to their homes by using smart locks configured with blockchain based digital identities [153].
- Smart appliances: Blockchain reduces human intervention by making smart home appliances like washing machines and refrigerators self-order their maintenance and even make the payment for it [154].
- Home insurance: Blockchain can further be used in automating home assurance policies and risk assessment by using data from smart home devices [155].
- Automated billing and payments: Blockchain can further automate smart home energy consumption and maintenance bill payments through an automated execution of smart contracts [156].

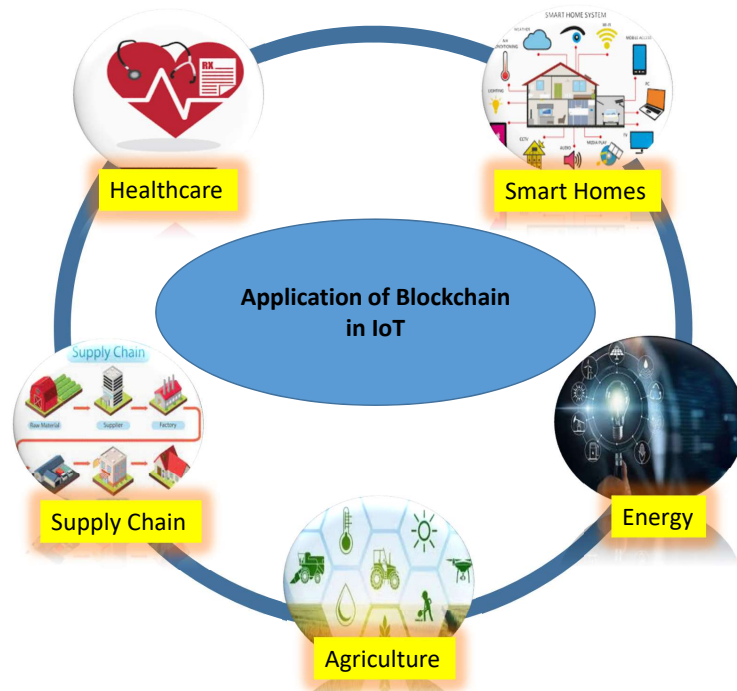


Figure 5: Blockchain application in IoT

4.2. Supply Chain Management

Supply chain management (SCM) [157] is the concept of delivery, tracking, and management of goods and services from the manufacturer to the final customer. A number of entities or stakeholders are involved during the whole life cycle of SCM, such as manufacturers, suppliers, distributors, retailers, and customers. Blockchain has gained much popularity in the last few years in the IoT based supply SCM due to its transparency, immutability features, and security. This could fundamentally change the process of SCM by providing blockchain with greater trust between parties, tracing, and verification of ownership of goods to make the process of SCM easier. Blockchain can provide parties involved with increased trust by offering an immutable and tamper-proof ledger keeping track of the flow of goods at each stage of SCM [158] with the aid of IoT sensors.

Blockchain technology can enhance transparency and visibility by tracking goods and services in real time using IoT sensors. Blockchain can decrease the time and costs [159] associated with SCM documentation and verification by smoothing the process associated with SCM. Similarly, smart contracts of blockchain can automate many activities of SCM, e.g., payment, custom clearance, and quality controls. Popular SCM solutions based on blockchains include IBM Food Trust [160] and Everledger platform [161]. The blockchain platform of IBM Food Trust uses smart contracts for the verification and tracing process of food products origin and authenticity. Everledger blockchain platform traces and verifies the origin and authenticity of diamonds to build trust among various stack holders.

4.3. Healthcare

Blockchain can successfully be used for sharing, security, interoperability, and privacy of healthcare data between patients, healthcare providers, pharmacies, and other stakeholders. Popular blockchain based healthcare systems include MedRec [162], and Gem Health Network [163]. Following are some useful applications of blockchain technology in IoT based healthcare:

- Patient healthcare data: These days patient uses various IoT based wearables and sensors for healthcare. The security and privacy of the patient's healthcare data is an important concern [164]. Blockchain can thus regulate patient data management [165] where patient's have to make provision for the sharing of their information with all healthcare providers, investigators, or other agents in a secure and controlled way.

- Secure sharing of medical records: In Electric Health Record (EHR) [166] system blockchain can be used to ensure patient data privacy and security. For instance, blockchain can play a vital role in sharing patient data between different healthcare providers as well as between healthcare providers and laboratories [167].
- Clinical research: The two prominent factors related to the clinical research arena are transparency and accountability. The transparency and accountability of clinical research data [168] can be ensured using blockchain based immutable and auditable records of all clinical research related data.
- Drug supply chain management: Blockchain can track and trace the pharmaceutical products supply chain [169], from manufacturer to end user through IoT sensors. This approach can guarantee safety, transparency, accountability, and counterfeit proof for medicines.
- Payment and insurance: Blockchain can minimize fraud and errors [170] in healthcare payment and insurance by automating and streamlining administrative processes.

4.4. Energy Management

Blockchain has enormous potential in the transformation of the energy sector by ensuring decentralized, transparent, and secure systems for managing energy [171, 172]. Smart grid [173] complemented by blockchain and IoT based real time data can improve energy production, storage, and distribution. One potential application of blockchain in the energy sector is peer-to-peer (P2P) energy trading platforms [174]. Such a platform can enable the trade of surplus renewable energy (solar) between homes and companies. The security and transparency of trading energy and its corresponding payment can be ensured by the use of blockchain technology. Improvement in energy management through blockchain can be realized by shaping decentralized energy storage systems [175]. Smart meters and energy storage systems [176] established through the integration of blockchain and IoT can advance distributed energy storage networks. Similarly, blockchain can also promote virtual power plants [177]. The Brooklyn Microgrid [178] and Energy Web Foundation [179] projects are the outcome of the successful application of blockchain applications in the energy sector.

4.5. Agriculture

Blockchain technology can also bring changes about traceability, transparency, and efficiency in the agricultural food supply chain [180, 181]. The IoT sensors can collect data in the agricultural food supply chain and transfer it to the blockchain for storage and reporting purposes. Consequently, this would act as useful evidence to all stakeholders about the source, processing, and transportation of products. Subsequently, that would enhance customers assurance, reliability, and confidence in the goods they buy. Other agricultural processes that this technology can potentially improve, in addition to food safety, are land registry [182], crop insurance [183], and supply chain financing [184].

4.6. Lessons Learned: Summary and Insights

Due to blockchain various features, it can be successfully used in a variety of IoT based applications, e.g., smart homes, SCM, healthcare, energy management, and agriculture. Blockchain is ideal for secure communication and data sharing in smart home scenarios such as smart locks, smart appliances, home insurance, and home surplus energy trading. Another valuable application of blockchain is to ensure data sharing, security, privacy, and interoperability in IoT based healthcare domain.

5. Integration of Blockchain and IoT

In recent years, the adoption of blockchain for IoT [185, 186] has gained much popularity. The use of blockchain to secure IoT devices, improve data privacy, and enable new applications is being studied by many researchers. A few of the sectors that potentially change as a result of implementing blockchain in IoT are healthcare, SCM, and energy management. Blockchain can boost trust among network users, and offer a secure, accountable, and transparent platform for data transmission. Overall, blockchain provides extended benefits to deal with security, transparency, trust, and traceability issues in IoT environments. A review of blockchain solutions for security and privacy, trust, and traceability is presented below.

Table 6: A comparison of existing literature on blockchain application for IoT security and privacy

Reference	Objective	Blockchain Platform	Cryptographic Algorithm	Advantage
Bera et al. [19]	Threat mitigation in IoT	-	ECC, ECDSA, SHA-256	Protection against diversified attacks
Yazdinejad et al. [190]	Privacy preserved threat intelligence in IoT environments	Ethereum	ECC	Performance, Scalability
Kumar et al. [191]	Security threat and fraud detection in IoT environments	Ethereum	Asymmetric cryptography, DS algorithm	Threat mitigation in the context of uncertain IoT environments
Alkhabbas et al. [192]	Security in mission critical IoT environments	Ethereum client-Hyperledger Besu	Asymmetric cryptography, HMAC	Adaptation, Collaborative learning
Makhdoom et al. [18]	Privacy-preserving IoT data sharing in a smart city environment	Hyperledger Fabric	Symmetric encryption-AES, Asymmetric cryptography	GDPR compliance, Reward mechanism for data owners
Daidone et al. [193]	Data privacy in IoT environments	Hyperledger Fabric	Asymmetric cryptography	Capability of user-centric and fine-grained data owner privacy
Loukil et al. [194]	Data privacy through blockchain based Devices control in IoT environments	Ethereum- Ganache blockchain	Asymmetric cryptography	Instead of device embedded security, dynamic privacy control through smart contracts
Ren et al. [195]	Data security in smart home	Bitcoin (simulated)	Identity-based cryptography (Asymmetric cryptography)	Data integrity, reliability, availability, and efficient utilization of resources
Ren et al. [196]	Secure data storage in edge computing	-	Asymmetric cryptography	Enhanced data security, reliability, and integrity
Shalini et al. [197]	Multimedia data security in IoT	-	quantum cryptography	Suitable for addressing range of security attacks
Sasikumar et al. [198]	Secure data sharing in industrial IoT	Ethereum	Asymmetric cryptography	Lightweight and efficiency
Liu et al. [199]	Access control of cloud based IoT data	Hyperledger Fabric	RSA, SHA algorithm	More practical paradigm, Fine-grained access control
Abdi et al. [200]	Edge based lightweight access control mechanism in IoT environments	Hyperledger Fabric	RSA, SHA algorithm	More scalable, Modular approach

5.1. Security and Privacy in IoT

IoT devices are vulnerable to security and privacy exploits and attacks [187, 188, 189] due to their operating environment. Moreover, IoT devices normally have limited security protection due to their limited processing and power capabilities. Recently, blockchain technology has become popular to address IoT security and privacy issues. Several researchers have conducted studies and have proposed various solutions to secure IoT devices and their corresponding data. A review of these solutions is presented in Table 6 with their objectives and advantages.

A blockchain based approach for IoT threat detection and mitigation is proposed in [19]. The proposed approach uses blockchain based access control, AI, and fog computing to secure IoT from various security attacks. It is difficult to judge the true performance measurement of the proposed approach as the blockchain platform used for experimentation was not mentioned in the paper. P2TIF [190] based on deep learning and a blockchain based approach, attempts to safeguard confidential data and provides threat intelligence in industrial IoT environments. The given approach securely stores IoT data on the blockchain and then uses a deep learning module for threat intelligence and identification. Kumar et al. [191] propose an intelligent fuzzy blockchain framework to counter security threats using an adaptive neuro-fuzzy inference system, and fuzzy control system. To cope with the uncertain nature of IoT, they have preferred fuzzy logic instead of a deep learning model. ASSERT [192] is a distributed blockchain based approach to cater to security threats in goal-driven and mission-critical IoT environments. ASSERT makes use of intelligent agents, federated learning, feedback loops, and blockchain to mitigate threats in mission-critical and cooperative IoT environments.

PrivySharing [18] based on blockchain and access control mechanisms attempts to ensure personal/critical data privacy and secure data sharing in a smart city environment. PrivySharing ensures privacy and control access to the data using a smart contract based embedded access control mechanism. Daidone et al. [193] proposed a blockchain based framework for data privacy in IoT environments. More specifically, the framework uses smart contracts and decentralized consensus among communicating parties to perform privacy compliance checks regarding IoT data privacy. In [194] authors have proposed an IoT privacy-preserved device management framework based on blockchain based smart contracts. IoT data privacy is preserved by controlling access to devices data through a pre-configured smart contract based access controlled mechanism.

An aggregate digital signature and blockchain based scheme to address security threats in smart home systems has

Table 7: A comparison of existing literature on blockchain application for trust in IoT environments

Reference	Objective	Blockchain Platform	Cryptographic Algorithm	Advantage
Malik et al. [203]	Trust management in IoT based SCM	Ethereum	Asymmetric cryptography	Layered trust management, Accountability mechanisms
Ayed et al. [203]	Decentralized trust in IoV	Ethereum	Asymmetric cryptography	Performance, Scalability
Javadi et al. [205]	Trust management wireless sensors network	Ethereum	Asymmetric cryptography	Interplanetary File System (IPFS) cost effective data storage
Xe et al. [206]	Trust in industrial IoT	Hyperledger Fabric	Asymmetric cryptography	Efficiency introduced through new proposed parallel consensus protocol (OPBFT) consensus protocol
Bi et al. [207]	Distributed medical trust management in large scale IoT environments	Ethereum	Asymmetric cryptography, HMAC	Trust specific protocol PoTC, Scalability
Asif et al. [208]	Trust management in IoT based smart cities	Ethereum	Asymmetric cryptography	Performance, Scalability
Wu et al. [204]	Trust management in wireless sensors network	Bitcoin	Asymmetric cryptography	Trust accuracy and resiliency against various attacks, Comparative analysis
Yan et al. [209]	To build trust and confidence on current status of IoT devices	Ethereum	Asymmetric cryptography	Reliable data collection and storage, Secure transmission
Liu et al. [210]	Secure data sharing in zero-trust IoT environments	Ethereum-Ganache	Asymmetric cryptography	Secure information sharing without requiring trusted third party

been proposed in [195]. The proposed scheme is based on identity based proxy aggregate signature (IBPAS) with the benefits of the efficiency of signature verification, compressed storage space, and reduced communication bandwidth. A novel mechanism based on blockchain and regeneration coding for data security and reliability in edge computing is proposed in [196]. The proposed mechanism uses local blockchain at the IoT layer and global blockchain at the cloud layer to enhance data security. Additionally, the reliability of data storage in blockchain is achieved through regeneration coding. A solution for secure data gathering, storage, and transmission in IoT environment is proposed in [197]. The given approach makes use of quantum cryptography and blockchain to secure multimedia data generated by IoT devices. A blockchain based hierarchical attribute based encryption algorithm for secure data sharing in the industrial IoT is proposed in [198]. The distributed nature of the proposed scheme makes it more efficient and secure when compared with related schemes.

Fabric-IoT [199] proposed a blockchain and Attribute based Access Control (ABAC) mechanism for access control to device data in large-scale IoT environments. Data collected from IoT devices is first stored on distributed cloud storage. Access to IoT cloud based data is then granted to authorized users through blockchain based access control and verification. A lightweight and hierarchical blockchain based access control mechanism is presented in [200]. The proposed approach uses blockchain based authorization at both the edge layer and cloud layer to control access to data generated by IoT devices.

5.2. Trust Management in IoT

IoT environment is highly heterogeneous and pervasive such as IoV [201] and wireless sensor networks [202]. IoT devices normally operate in a zero-trust environment where IoT devices are vulnerable to various compromises and thus are untrusted. Therefore, trust is an important aspect of secure communication and data transfer in IoT environments. Table 7 presents a review of important solutions for trust management in IoT environments. TrustChain [203] attempts to solve trust issues in IoT based SCM. Trustchain uses blockchain based smart contracts to calculate trust reputation through all phases of SCM. Ayed et al. [203] proposed a blockchain based trust management system based on reputation and message credibility metrics to enhance the security of IoV. In their previous proposed centralized trust management system, scalability was the main issue due to the centralized trust management system. Therefore, they introduced a new decentralized and scalable trust mechanism based on a clustering approach. In [204] authors attempted to build a trustworthy IoT sensor environment where interactions are driven by the blockchain based trustworthiness of IoT sensor nodes. Due to resource constraints, sensor nodes are supported by edge nodes in the construction of trust computation.

Xu et al. [206] used blockchain and federated learning for trust management in the industrial IoT (IIOT). Blockchain is not only suitable for establishing trust in a distributed fashion but also provides traceable trust evaluation capabilities. Bi et al. [207] proposed a distributed trust management system for the healthcare domain based

Table 8: A comparison of existing literature on blockchain application for traceability in IoT

Reference	Objective	Blockchain Platform	Cryptographic Algorithm	Advantage
Turki et al. [211]	Drug traceability during pharmaceutical supply chain	Ethereum	Asymmetric cryptography	Reliable access control through smart contracts, Included detailed insight to implementation details
Al-Rakhami et al. [212]	IoT supply chain traceability	IOTA	Asymmetric cryptography	Traceability complimented authenticity and integrity
Li et al. [213]	Anonymous Traceable in IIoT	Hyperledger Fabric	RSA, DSA, and ECC	Traceability complimented with adequate privacy, Resistance against coalition attacks
Ferrández-Pastor et al. [214]	Traceability of product in IoT based agriculture sector	Hyperledger Fabric	Asymmetric cryptography	User centric design
Song et al. [215]	Traceability in IoT based power material supply chain	Hyperledger Fabric	Asymmetric cryptography	Privacy of private data sharing with traceability
Junzheng et al. [216]	Traceability in IoT based supply chain	Hyperledger Fabric	Asymmetric cryptography	Traceability complemented with privacy
Roberto et al. [217]	Traceability in IoT based supply chain	Hyperledger Fabric	Asymmetric cryptography	Comprehensive framework for supply chain traceability
Siddiqui et al. [218]	Audit trail and provenance in sensitive IoT environments	Hyperledger Fabric	CP-ABE based signature, Asymmetric cryptography	Data provenance and traceability in sensitive IoT environments
Shahbazi et al. [219]	Traceability in IoT based Food supply chain management	Ethereum	Asymmetric cryptography	ML, Fuzzy data analysis
Alkaabi et al. [220]	Trusted data traceability in Additive Manufacturing (AM)	Ethereum	Asymmetric cryptography	Credible and secure traceability and protection against copyright infringement

on federated learning in IoT environments. Healthcare institutions were categorized into several groups for scalability and management purposes. For the establishment of trust, leaders of each group were elected based on a trust-specific consensus protocol is known as the PoTC consensus protocol. In [205] authors have proposed a new blockchain based mechanism for trust and transparency in a wireless IoT environment. The authors claim that the performance of their solution is increased by 13% by using the PoA consensus protocol instead of PoW. In [208] authors have presented the design of an efficient trust management mechanism based on blockchain for smart cities. They have proposed a mutual authentication mechanism between clients and servers to not only control user access to the system but also allow users to validate the server as well.

Trusted computing (TC) is a hardware based technology to build trust in distributed environments such as IoT. Many researchers have used TC for trust and security management in IoT environments. An architecture for reputation and trust building on IoT devices and to enable reliable data collection, storage, and secure transmission is proposed in [209]. The given approach uses trusted computing and blockchain to detect and isolate malicious nodes and guarantee stable, trusted, and safe IoT environments. Liu et al. [210] proposed a blockchain based trust mechanism for secure data sharing in a zero-trust IoT environment. The given approach can successfully detect fabricated information for untrusted devices using voting, smart contracts, and consensus mechanisms. The major benefit of this approach is that it can build trust without using a trusted third party.

5.3. Traceability in IoT

The distributed and immutable nature of the blockchain makes it ideal for addressing traceability issues. In the context of IoT, blockchain provides a secure and transparent way to record and share data securely. Therefore, blockchain is ideal for enforcing traceability of data storage and access. This subsection provides a comprehensive review of the application of blockchain for traceability in IoT domain and is shown in Table 8.

IoT based drug traceability system is proposed in [211], to ensure protection against drug counterfeiting in the pharmaceutical supply chain. The proposed approach uses blockchain based NFT (Non-Fungible Token) to provide a holistic view of a medicine lot detailing the environmental shipment conditions, current owner, and certifications. Information related to the medicine lot is updated on the blockchain during the supply chain to allow stakeholders to get comprehensive information regarding medicine throughout the supply chain process. ProChain [212] proposed a blockchain provenance-aware traceability scheme for IoT based supply chains. The IoT sensors and blockchain provide traceability of food items throughout the supply chain from production to retailer. Similarly, Ferrández-Pastor et al. [214] proposed a blockchain based model for traceability in the agriculture domain. Taking farming of hemp as a use-case, the authors have provided details about transparent and tamper-proof traceability in the agricultural sector.

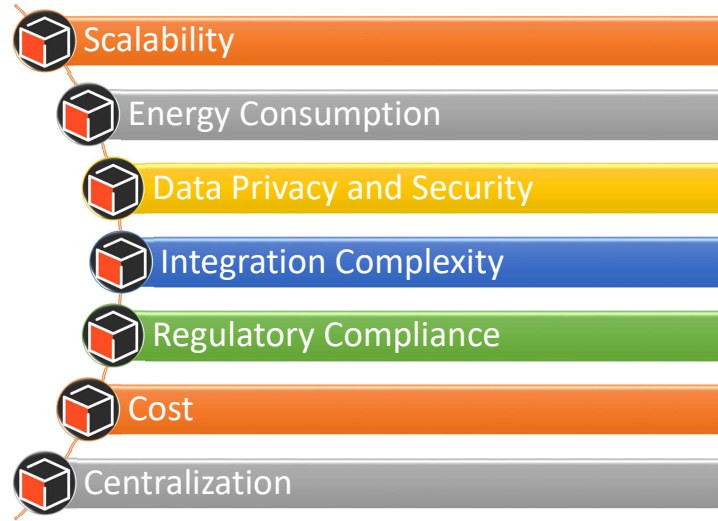


Figure 6: Challenges: Blockchain and IoT integration

In [213] the authors have proposed a blockchain based scheme to ensure the traceability of an abnormal data source in IIoT. The given approach uses smart contracts to authenticate anonymous users whereas blockchain recorded data is used to trace abnormal data sources.

Junzheng et al. [216] proposed a blockchain based traceability solution for supply chain management. The given approach uses zero-knowledge proof and attribute based encryption to protect the participant's privacy as well as ensure adequate traceability. Roberto et al. [217] presented a blockchain based framework for the traceability and reliability of assets in supply chain management related to offsite manufacturing. The framework uses blockchain as a service (BaaS) for smart contracts and infrastructure management. BlockTrack-L [218] based on blockchain technology proposed a lightweight message-tracking system in IoT. The proposed solution is ideal in a sensitive IoT environment to provide traceability of messages generated by IoT devices. A blockchain data sharing and tracing mechanism for the power material supply chain is proposed in [215]. The proposed approach uses proxy re-encryption alongside blockchain to support privacy besides traceability of data. A Machine Learning and fuzzy logic based traceability system for the perishable food supply chain is presented in [219]. The proposed approach uses ML for data analysis and prediction, and blockchain provides secure and immutable IoT device data tracking. In [220] the authors have presented a blockchain based solution for the protection of the copyright of digital product design in Additive Manufacturing (AM). The given approach ensures credible and secure traceability and protects against copyright infringement.

5.4. Lessons Learned: Summary and Insights

Blockchain can successfully solve various challenges in IoT environments, e.g., security and privacy, trust management, and transparency. This section provided a comprehensive comparative analysis of various blockchain solutions, for security and privacy, trust management, and transparency. In conclusion, the comparative analysis highlights that in a majority of these solutions, the implementation details (e.g., type of encryption, hash algorithms, and key size used) are missing in the given performance evaluations.

6. Challenges and Future Direction

6.1. Challenges of using Blockchain in IoT

Blockchain provides many opportunities and benefits [221, 222] related to IoT domain. Here, we present several use cases and IoT related domains where blockchain is currently showing great promise. Despite these opportunities, many challenges are emerging through the integration of blockchain and IoT, as illustrated in Fig. 6. Here, we present some of the current challenges that emerge through the integration of blockchain and IoT.

6.1.1. Scalability

Currently, blockchain technology is suffering from scalability issues [223, 224] because it has to process a huge amount of data and transactions. The huge amount of data generated in real time by IoT devices and sensors requires adequate processing and secure storage arrangements. Thus, when it comes to its application in IoT, the challenge of scalability becomes more significant. The IoT environment in itself comprises a lot of devices and sensors [76] that can generate a large volume of transactions. Again, this affects how the scalability to process and commit a large number of transactions to the ledger in a given time. The consensus mechanism [13] verifies and commits a transaction and a block to the blockchain. The main factors that contribute to the scalability issue of blockchain are the current blockchain consensus mechanisms and underlying protocols. Extensive computation, communication, and agreement are required for the consensus between participants in the blockchain network; this has consequently reduced the scalability of the blockchain network at large. Another element that affects blockchain scalability is blockchain size [103]. When new transactions are added, the size of the blockchain increases. Processing such a large amount of transactions becomes computationally challenging.

6.1.2. Energy Consumption

The other important challenge of using blockchain in IoT is related to energy consumption. Since blockchain makes use of complex computational algorithms [225] for validation, security, and commitment in transactions, blockchain technology has been rated as computational and energy intensive. This challenge gains greater significance within the context of IoT, where IoT devices have limited energy, power, and processing capabilities. Several reasons contribute to the energy aspects related to blockchain technology. This is mainly due to inefficient consensus algorithms like Proof-of-Work [63]. In PoW based consensus algorithms, miners have a race to solve an extremely hard mathematical puzzle to validate transactions with the expectation of getting a reward. This process requires a huge amount of energy and processing power. Another important factor contributing to blockchain energy aspect is cryptographic algorithms [51], which are used in securing and verifying transactions.

6.1.3. Data Privacy and Security

Blockchain is known for its security related features [226] due to its strong cryptographic algorithms. However, blockchain is still vulnerable to different security based attacks or breaches [187, 188, 189]. This is quite important in relation to the IoT. IoT devices normally operate in an open environment and generate sensitive data. For example, IoT devices operating in the healthcare and military domains [227] transmit highly sensitive data. Therefore, the integration of blockchain and IoT needs to be carefully managed against existing and new emerging security risks and vulnerabilities. When data moves from an IoT environment to a blockchain for storing and sharing purposes, security based protection is highly desirable. The distributed nature of blockchain poses several new security based challenges. First, due to the distributed nature of blockchain data [8], replication happens over several nodes in the network; this increases the possibility of security threats and their associated attacks. Second, blockchain nodes can be located over a large number of geographic locations with their associated privacy laws [228, 82] therefore, it is hard to enforce adequate data privacy. Moreover, IoT devices with limited security capabilities can easily become victim to security-based threats and attacks.

6.1.4. Integration Complexity

The integration of blockchain and IoT can get challenging and complicated, especially for organizations for whom both technologies are new. Its successful integration will demand careful planning, coordination, technical expertise, and resources. Several factors contribute to these integration challenges and complexities [229]. In the first place, the diverse nature and range of IoT sensors and devices make this integration both complex and challenging. Lacking standards in the IoT industry [81] is another reason. A wide scope of communication protocols [230] and different data formats are used in IoT. Thus, it makes the standardization of interfaces to integrate blockchain with IoT very demanding. At last, the processing and storage capabilities of IoT devices are pretty low and make it difficult to store data on the blockchain.

6.1.5. Regulatory Compliance

Another challenge in integrating blockchain and IoT is regulatory requirements and compliance. As in the domains of health and finance, data privacy and security requirements are essential. For instance, the Health Insurance

Portability and Accountability Act [231] and Payment Card Industry Data Security Standard (PCI DSS) [232] are the two healthcare and financial regulations, respectively, that need to be taken into consideration while integrating blockchain with IoT. Another key and related protection law in this regard is the EU's General Data Protection Regulation (GDPR) [228]. GDPR can be demanding, as it entails strict rules about collecting, storing, and processing personal data.

6.1.6. Cost

The requirements for hardware, software, and maintenance in blockchain technology can be costly. Thus, the use of blockchain technology in an IoT environment becomes a resource constraint challenge, especially where cost is a major issue. Moreover, blockchain based IoT solutions are expensive to implement compared with existing centralized IoT systems. One of the key costs in blockchain environments is processing power related to transaction validation and commit [8]. In a regular process of transaction validation, each node will have to process and validate a given transaction [63]. Such type of validation could greatly increase computational cost. These would present serious challenges because IoT devices normally possess limited processing, power, memory, and storage capabilities. Furthermore, the development of software, hardware up-gradation, and their continuous maintenance can increase manifold.

6.1.7. Centralization

Blockchain technology is a distributed and decentralized technology to exempt organizations from the requirement of one central or intermediary authority. Blockchain implementation in IoT can still demand a central authority, e.g., blockchain node operators or cloud service providers [233]. This conflicts with the decentralization that blockchains are really for and may raise security and privacy concerns. This centralization to identify a single or few nodes for transaction validation can result in a single point of failure. Centralization can also impact the overall transparency and accountability of the underlying system. At worst, centralization might lead to a system compromise and result in data manipulation or loss.

6.2. Future Trends and Research Directions

In this subsection, we present future research directions that need further research to address the current challenges that are emerging due to the integration of blockchain and IoT. Although, there is no one-size-fits-all solution, however for the successful integration of blockchain and IoT, a combination of practical and innovative solutions in these emerging directions will be required.

6.2.1. Scalability

A huge amount of data generated by IoT devices can become a problem to be handled by blockchain networks. Thus, scalability can become one of the major problems in blockchain based IoT environments. Due to the adoption of high speed 5G networks by IoT devices, the scalability issue becomes more challenging. Following are the expected future research trends that need further research to encounter the scalability challenges of blockchain based IoT.

- Layer 2 scaling solutions [115, 123]: The throughput of blockchain networks can increase to a massive extent using the new solutions. These include sidechains and rollups. These layer 2 scaling solutions off-chain transactions to improve the throughput and resultant scalability.
- Sharding [91]: In this scalability solution, at layer 1, the main network is partitioned into smaller sub-networks, making it manageable and scalable. Sharding allows less congestion on the main blockchain network with quick and efficient processing of more transactions.
- Optimized consensus algorithms: Another strategy to enhance the scalability of a blockchain network is the use of optimized consensus techniques, such as proof of stake (PoS) [65] and delegated proof-of-stake (DPoS) [101]. Such optimized consensus algorithms use fewer computational resources and are suited for solving the scalability challenge.
- Hybrid blockchain architecture [233]: Another way to improve scalability is to use hybrid blockchain solutions. Hybrid blockchain inherits the features of public and private blockchain. Hybrid blockchain can provide faster and more efficient transaction processing, ensuring data security and privacy.

6.2.2. *Energy Efficiency*

Due to energy demand and crises, the efficiency demand for energy efficient solutions and technologies keeps increasing. Energy efficiency is another important aspect to be taken into consideration while integrating blockchain and IoT. No doubt, energy efficient blockchain solutions will contribute towards a more sustainable and environment friendly blockchain based IoT ecosystem. The following are some new trends and developments that are likely to shape the energy efficiency aspect of blockchain based IoT.

- **Low-Power IoT devices:** Low power devices are intended to consume minimal quantities of energy, especially devices based on protocols like the LoRaWAN protocol [234]. Low power devices with properties of energy efficiency are, therefore, very suitable for use in blockchain based IoT applications. These devices consume less energy and can operate for a longer period before there is any significant need for battery replacement.
- **Blockchain based energy trading and management systems** can be deployed to bring efficiency in energy use and reduce energy wastage [235]. By creating such a peer-to-peer energy trading system, energy wastage could be reduced and energy efficiency enhanced by offering consumers the possibility to sell their excess energy to other consumers.
- **Efficient consensus mechanisms:** Currently, researchers are shifting from energy intensive consensus mechanisms like the PoW to more energy friendly protocols like proof of stake. Such energy efficient protocols have less consumption of energy, so they fit well in the IoT environment.
- **Green blockchain initiatives [236]:** Upcoming Green blockchain initiatives, such as the Chia Network, can be utilized in the construction of energy efficient and green blockchain networks. Its goal is to create more energy efficient and environment friendly blockchain protocols.

6.2.3. *Security and Privacy*

Integration of IoT using blockchain ensures security and privacy by providing appropriate protection against unauthorized access, disclosure, and manipulation of sensitive data generated by these devices. The trends of future research that have been emerging in the area of security and privacy for blockchain based IoT systems are presented herein.

- **Privacy-Preserving technologies:** Future privacy preserving techniques like Zero-Knowledge proofs [114] and homomorphic encryption [237], can complement the security and privacy of the data produced by devices and sensors in IoT environments. Both techniques show great promise for IoT sensitive data since data can be manipulated and processed without its contents being exposed in an untrusted environment like the cloud.
- **Decentralized identity solutions:** The centralized identity management techniques provide a single location for an attacker and, therefore, are prone to identity theft and other data breach attacks. In contrast, decentralized identity solutions—for instance, self-sovereign identity (SSI) [238]—can be a better way to let users have control over their identities. A blockchain based IoT setting enhances decentralized identity solutions for identity management and security of sensitive data from IoT devices.
- **Blockchain based security solutions:** The security-based techniques—secure smart contracts, Signcryption [239], a and digital signatures can be helpful in the enhancement of security of the Internet of Things devices and the blockchain. These techniques could help in generating secure, immutable transaction records for every transaction to mitigate fraud and cyber attacks.

6.2.4. *Interoperability*

Several diverse protocols and standards are present for IoT devices and blockchain. This makes the interoperability issue very important in blockchain based IoT environments. Future trends to assist interoperability in blockchain based IoT include:

- **Standardization:** Common standards and protocols are the requisite needs for the successful integration of blockchain and IoT. The recent initiative for developing common standards [240] by several standardization bodies like IEEE and IETF shall definitely move towards the interoperability aspect of blockchain and IoT.

- **Middleware:** A common middleware framework between IoT devices and blockchain needs to be developed. Further research in this domain is essential to support seamless communication and translation between IoT devices and blockchain networks.

Recently, IEEE has been actively engaged in developing standards for the successful integration of the blockchain and IoT domains. It has recognized the potential of blockchain and IoT integration in healthcare, smart cities, and supply chain management, among several other areas. Here are some of the popular IEEE standards for blockchain and IoT integration:

- **P2418.1 Standard for the Framework of Blockchain Use in the Internet of Things (IoT):** The focus of this standard is on developing definitions and protocols for blockchain and IoT integration in various application domains. This standard aims at secure data storage, data integrity, device communication, and management.
- **P2418.8 Standard for Blockchain Applications in Governments:** A common framework for the use of blockchain in government matters is the main focus of this standard. It attempts to address the security, privacy, and scalability challenges of blockchain in government operation and implementation. A few of the blockchain aspects this standard covers include smart contracts, tokens, and off-chain data storage.
- **P2418.9 Standard for Cryptocurrency Based Security Tokens:** This standard outlines a framework to design digital security tokens for cryptocurrency. The technical requirement to plan a security token under regional regulations and security laws.

6.2.5. *Edge Computing:*

Edge computing is an emerging computing initiative to process data closer to IoT devices. It is very challenging for IoT devices with limited computing power and storage capabilities to participate directly in the blockchain network. Edge devices could provide support to decentralized applications (dApps) [241] and IoT devices to participate and function as blockchain nodes. Therefore, edge devices can support secure and efficient data transfer in the context of blockchain based IoT.

Following are the few significant benefits of using edge computing in the context of blockchain and IoT integration.

- **Low Latency:** Sending massive amounts of data generated by IoT devices to a cloud based centralized environment introduces a significant latency. Latency can be significantly reduced by using edge computing [242] for faster decision making and real time experience in various domains, e.g., industrial automation and supply chain management.
- **Data Security and Privacy:** Data security and privacy [243] is an important aspect of blockchain based IoT systems. Edge computing allows sensitive data to be processed locally, and as a result, possible exposure of data to threats during transmission can be reduced. This results in enhanced data privacy and reduced risks connected with data transmission to the cloud.
- **Compliance and Regulatory Concerns:** In many circumstances, IoT device data must comply with explicit regional regulations or compliance standards [228, 231]. Edge computing can help in this regard to support the processing of data according to regional regulations or standards at the local level.

6.2.6. *Federated Learning*

Federated learning [244] based on machine learning models and capabilities provides another dimension in the context of blockchain and IoT. Through federated learning, IoT devices can work in cooperation and exchange information locally without exposing their sensitive data directly to central servers such as a cloud [245]. IoT devices can largely benefit from federated learning as transmission and processing of enormous data generated by IoT devices are usually challenging.

6.3. Lessons Learned: Summary and Insights

Although blockchain and IoT integration provide various benefits, several challenges need careful attention for the successful integration of blockchain and IoT. These challenges include blockchain scalability, energy consumption, data security and privacy, integration complexity, regulatory compliance, cost, and centralization. The chapter concludes with valuable future research directions to overcome the current challenges of a blockchain based IoT environments.

7. Conclusion

The Internet of Things (IoT) has revolutionized our way of life. Blockchain technology is an immutable and distributed ledger technology that is increasingly used in IoT environments due to its various benefits. In this paper, we have provided a review of blockchain based solutions for ensuring security and privacy, trust, and traceability based guarantees in IoT environments. Blockchain is increasingly used in various IoT based domains. We have discussed in detail various applications of blockchain in IoT based domains. One of the most significant challenges of current blockchain technology is the scalability issue. We have provided a comprehensive review of the current blockchain scalability solutions and lightweight encryption algorithms. IOTA, a distributed ledger technology based on directed acyclic graphs is gaining popularity in IoT environment due to its microtransaction and high throughput features. IOTA is the way forward as its microtransaction and high throughput features are well-suited for IoT environments where devices communicate frequently but often with small data. The paper concludes by highlighting the current challenges and future direction for the successful integration of blockchain and IoT.

References

- [1] S. Madakam, R. Ramaswamy, S. Tripathi, Internet of things (iot): A literature review, *Journal of Computer and Communications* 3 (05) (2015) 164–173.
- [2] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, B. Balusamy, Wearable devices and iot, *A Handbook of Internet of Things in Biomedical and Cyber Physical System* (2020) 245–273.
- [3] Z. Solatidehkordi, J. Ramesh, A. Al-Ali, A. Osman, M. Shaaban, An iot deep learning-based home appliances management and classification system, *Energy Reports* 9 (2023) 503–509.
- [4] A. Kanawaday, A. Sane, Machine learning for predictive maintenance of industrial machines using iot sensor data, in: *International Conference on Software Engineering and Service Science*, IEEE, 2017, pp. 87–90.
- [5] T. Alladi, V. Chamola, B. Sikdar, K.-K. R. Choo, Consumer iot: Security vulnerability case studies and solutions, *IEEE Consumer Electronics Magazine* 9 (2) (2020) 17–25.
- [6] V. Malik, S. Singh, Security risk management in iot environment, *Journal of Discrete Mathematical Sciences and Cryptography* 22 (4) (2019) 697–709.
- [7] C. Cao, L. Guan, N. Zhang, N. Gao, J. Lin, B. Luo, P. Liu, J. Xiang, W. Lou, Cryptme: Data leakage prevention for unmodified programs on arm devices, in: *International Symposium, RAID 2018*, Springer, 2018, pp. 380–400.
- [8] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, *International Journal of Web and Grid Services* 14 (4) (2018) 352–375.
- [9] R. Böhme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance, *Journal of Economic Perspectives* 29 (2) (2015) 213–238.
- [10] D. V. Dimitrov, Blockchain applications for healthcare data management, *Healthcare Informatics Research* 25 (1) (2019) 51–56.
- [11] J. Abou Jaoude, R. G. Saade, Blockchain applications—usage in different domains, *IEEE Access* 7 (2019) 45360–45381.
- [12] M. Pournader, Y. Shi, S. Seuring, S. L. Koh, Blockchain applications in supply chains, transport and logistics: a systematic review of the literature, *International Journal of Production Research* 58 (7) (2020) 2063–2081.
- [13] J. Xu, C. Wang, X. Jia, A survey of blockchain consensus protocols, *ACM Computing Surveys* To be published (2023). URL <https://doi.org/10.1145/3579845>
- [14] A. Alkhateeb, C. Catal, G. Kar, A. Mishra, Hybrid blockchain platforms for the internet of things (iot): A systematic literature review, *Sensors* 22 (4), art. no. 1304 (2022).
- [15] B. K. Mohanta, S. S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: *International Conference on Computing, Communication and Networking technologies (ICCCNT)*, IEEE, 2018, pp. 1–4.
- [16] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, G. Dhiman, Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives, *Journal of Food Quality* 2021 (2021) 1–20.
- [17] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, *Computer Communications* 136 (2019) 10–29.
- [18] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, W. Ni, Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, *Computers & Security* 88, art. no. 101653, doi: 10.1016/j.cose.2019.101653 (2020).
- [19] B. Bera, A. K. Das, M. S. Obaidat, P. Vijayakumar, K.-F. Hsiao, Y. Park, Ai-enabled blockchain-based access control for malicious attacks detection and mitigation in ioe, *IEEE Consumer Electronics Magazine* 10 (5) (2020) 82–92.

- [20] J.-H. Cho, K. Chan, S. Adali, A survey on trust modeling, *ACM Computing Surveys* 48 (2) (2015) 1–40.
- [21] S. A. Bhat, N.-F. Huang, I. B. Sofi, M. Sultan, Agriculture-food supply chain management based on blockchain and iot: A narrative on enterprise blockchain interoperability, *Agriculture* 12 (2020).
- [22] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, V. Weerakkody, Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis, *Journal of Enterprise Information Management* 34 (3) (2021) 884–899.
- [23] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: A survey, *IEEE Access* 8 (2020) 16440–16455.
- [24] M. A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, *Future Generation Computer Systems* 82 (2018) 395–411.
- [25] B. K. Mohanta, D. Jena, S. S. Panda, S. Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, *Internet of Things* 8, art. no. 100107 (2019).
- [26] T. Alladi, V. Chamola, R. M. Parizi, K.-K. R. Choo, Blockchain applications for industry 4.0 and industrial iot: A review, *IEEE Access* 7 (2019) 176935–176951.
- [27] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M. H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, *IEEE Communications Surveys & Tutorials* 21 (2) (2018) 1676–1717.
- [28] C. Ye, W. Cao, S. Chen, Security challenges of blockchain in internet of things: Systematic literature review, *Transactions on Emerging Telecommunications Technologies* 32 (8), art. no. e4177 (2021).
- [29] V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, S. Kanhere, Blockchain technologies for iot, *Advanced Applications of Blockchain Technology* (2020) 55–89.
- [30] L. Da Xu, Y. Lu, L. Li, Embedding blockchain technology into iot for security: A survey, *IEEE Internet of Things Journal* 8 (13) (2021) 10452–10473.
- [31] S. Ramamoorthi, B. M. Kumar, M. M. Sithik, T. T. Kumar, J. Ragaventhiran, M. Islabudeen, Enhanced security in iot environment using blockchain: A survey, *Materials Today: Proceedings* 1 (2021) 1–15.
- [32] A. A. Alfa, J. K. Alhassan, O. M. Olaniyi, M. Olalere, Blockchain technology in iot systems: Current trends, methodology, problems, applications, and future directions, *Journal of Reliable Intelligent Environments* 7 (2) (2021) 115–143.
- [33] S. S. Mathew, K. Hayawi, N. A. Dawit, I. Taleb, Z. Trabelsi, Integration of blockchain and collaborative intrusion detection for secure data transactions in industrial iot: a survey, *Cluster Computing* 25 (6) (2022) 4129–4149.
- [34] M. K. I. Rahmani, M. Shuaib, S. Alam, S. T. Siddiqui, S. Ahmad, S. Bhatia, A. Mashat, Blockchain-based trust management framework for cloud computing-based internet of medical things (iomt): a systematic review, *Computational Intelligence and Neuroscience* 2022 (2022).
- [35] R. Kumar, R. Sharma, Leveraging blockchain for ensuring trust in iot: A survey, *Journal of King Saud University-Computer and Information Sciences* 34 (10) (2022) 8599–8622.
- [36] D. Mourtzis, J. Angelopoulos, N. Panopoulos, Blockchain integration in the era of industrial metaverse, *Applied Sciences* 13 (3), art. no. 1353 (2023).
- [37] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, Z. Tari, Blockchain-based federated learning for securing internet of things: A comprehensive survey, *ACM Computing Surveys* 55 (9) (2023) 1–43.
- [38] S. Abed, R. Jaffal, B. J. Mohd, A review on blockchain and iot integration from energy, security and hardware perspectives, *Wireless Personal Communications* (2023) 1–44.
- [39] H. D. Zubaydi, P. Varga, S. Molnár, Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review, *Sensors* 23 (2), art. no. 788 (2023).
- [40] S. Ali, Q. Li, A. Yousafzai, Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial iot networks: a survey, *Ad Hoc Networks* 152 (2024) 103320.
- [41] H. Gharavi, J. Granjal, E. Monteiro, Post-quantum blockchain security for the internet of things: Survey and research directions, *IEEE Communications Surveys & Tutorials* (2024).
- [42] R. Adams, B. Kewell, G. Parry, Blockchain for good? digital ledger technology and sustainable development goals, *Handbook of Sustainability and Social Science Research* (2018) 127–140.
- [43] B. Preneel, Cryptographic hash functions, *European Transactions on Telecommunications* 5 (4) (1994) 431–448.
- [44] X. Yi, X. Yang, A. Kelarev, K. Y. Lam, Z. Tari, *Blockchain Foundations and Applications*, Springer Nature, 2022.
- [45] A. A. Al-Ghofaili, M. A. Al-Mashari, Erp system adoption traditional erp systems vs. cloud-based erp systems, in: *Fourth Edition of the International Conference on the Innovative Computing Technology*, IEEE, 2014, pp. 135–139.
- [46] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, S. Shimizu, Privacy preservation in permissionless blockchain: A survey, *Digital Communications and Networks* 7 (3) (2021) 295–307.
- [47] M. Liu, K. Wu, J. J. Xu, How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain, *Current Issues in auditing* 13 (2) (2019) A19–A29.
- [48] M. Florian, S. Henningsen, S. Beaucamp, B. Scheuermann, Erasing data from blockchain nodes, in: *European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2019, pp. 367–376.
- [49] R. C. Merkle, A certified digital signature, in: *Advances in Cryptology—CRYPTO’89 Proceedings*, Springer, 2001, pp. 218–238.
- [50] R. Davis, The data encryption standard in perspective, *IEEE Communications Society Magazine* 16 (6) (1978) 5–9.
- [51] M. E. Hellman, An overview of public key cryptography, *IEEE Communications Magazine* 40 (5) (2002) 42–49.
- [52] I. Velásquez, A. Caro, A. Rodríguez, Authentication schemes and methods: A systematic literature review, *Information and Software Technology* 94 (2018) 30–37.
- [53] P. Samarati, S. C. de Vimercati, Access control: Policies, models, and mechanisms, in: *Foundations of Security Analysis and Design: Tutorial Lectures 1*, Springer, 2001, pp. 137–196.
- [54] W. Li, Q. Zhang, S. Deng, B. Zhou, B. Wang, J. Cao, Q-learning improved lightweight consensus algorithm for blockchain-structured internet of things, *IEEE Internet of Things Journal* 11 (2) (2024) 2855–2869. doi:10.1109/JIOT.2023.3294265.
- [55] Y. TANG, Y. SUN, Z. LIN, Tinyledger: A lightweight blockchain ledger protocol for the mec network, *Computers and Electrical Engineering* 109 (2023) 108749. doi:https://doi.org/10.1016/j.compeleceng.2023.108749.

- URL <https://www.sciencedirect.com/science/article/pii/S0045790623001738>
- [56] Y. Zhao, Y. Qu, Y. Xiang, Y. Zhang, L. Gao, A lightweight model-based evolutionary consensus protocol in blockchain as a service for iot, *IEEE Transactions on Services Computing* 16 (4) (2023) 2343–2358. doi:10.1109/TSC.2023.3238690.
 - [57] Q. Xie, F. Dong, X. Feng, et al., Hlochain: A hierarchical blockchain framework with lightweight consensus and optimized storage for iot, *Security and Communication Networks* 2023 (2023).
 - [58] P. Bhattacharya, A. K. Tiwari, A. Verma, A. Alabdulatif, S. Tanwar, R. Sharma, Lightblocks: A trusted lightweight signcryption and consensus scheme for industrial iot ecosystems, *Computer Standards & Interfaces* 88 (2024) 103785.
 - [59] C. Ye, G. Li, H. Cai, Y. Gu, A. Fukuda, Analysis of security in blockchain: Case study in 51%-attack detecting, in: *International Conference on Dependable Systems and their Applications*, IEEE, 2018, pp. 15–24.
 - [60] J. R. Douceur, The sybil attack, in: *Peer-to-Peer Systems: First International Workshop, IPTPS*, Springer, 2002, pp. 251–260.
 - [61] S. Sayeed, H. Marco-Gisbert, T. Caira, Smart contract: Attacks and protections, *IEEE Access* 8 (2020) 24416–24427.
 - [62] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Technical Report (2008).
URL <https://bitcoin.org/bitcoin.pdf>
 - [63] C. Zhang, C. Wu, X. Wang, Overview of blockchain consensus mechanism, in: *International Conference on Big Data Engineering*, 2020, pp. 7–12.
 - [64] V. Buterin, Ethereum whitepaper (Sep. 2022).
URL <https://ethereum.org/en/whitepaper/>
 - [65] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, E. Dutkiewicz, Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities, *IEEE Access* 7 (2019) 85727–85745.
 - [66] C. Cachin, Architecture of the hyperledger blockchain fabric, in: *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, Vol. 310, Chicago, 2016, pp. 1–4.
 - [67] J. Sousa, A. Bessani, M. Vukolic, A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform, in: *IEEE/IFIP International Conference on Dependable Systems and Networks*, IEEE, 2018, pp. 51–58.
 - [68] A. Baliga, I. Subhod, P. Kamat, S. Chatterjee, Performance evaluation of the quorum blockchain platform ArXiv:1809.03421 (2018).
 - [69] G. Wood, Poa private chains (2015).
URL <https://github.com/ethereum/guide/blob/master/poa.md>
 - [70] R. Saltini, Qbft blockchain consensus protocol specification v1. (2023).
URL [URL URL:https://entethalliance.org/specs/qbft/](https://entethalliance.org/specs/qbft/)
 - [71] H. Moniz, The istanbul bft consensus algorithm ArXiv:2002.03613 (2020).
 - [72] D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: *{USENIX} Annual Technical Conference ({USENIX}{ATC})*, 2014, pp. 305–319.
 - [73] R. G. Brown, J. Carlyle, I. Grigg, M. Hearn, Corda: an introduction (2016).
URL <https://docs.r3.com/en/pdf/corda-introductory-whitepaper.pdf>
 - [74] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, A. Sarwar, Blockchain attacks analysis and a model to solve double spending attack, *International Journal of Machine Learning and Computing* 10 (2) (2020) 352–357.
 - [75] T. Dillon, C. Wu, E. Chang, Cloud computing: issues and challenges, in: *International Conference on Advanced Information Networking and Applications*, IEEE, 2010, pp. 27–33.
 - [76] D. Sehrawat, N. S. Gill, Smart sensors: Analysis of different types of iot sensors, in: *International Conference on Trends in Electronics and Informatics*, IEEE, 2019, pp. 523–528.
 - [77] E. Siow, T. Tiropanis, W. Hall, Analytics for the internet of things: A survey, *ACM Computing Surveys* 51 (4) (2018) 1–36.
 - [78] S. Narula, A. Jain, Prachi, Cloud computing security: Amazon web service, in: *International Conference on Advanced Computing & Communication Technologies*, IEEE, 2015, pp. 501–505.
 - [79] M. Copeland, J. Soh, A. Puca, M. Manning, D. Gollob, M. Copeland, J. Soh, A. Puca, M. Manning, D. Gollob, Microsoft azure and cloud computing, in *Microsoft Azure* (2015) 3–26.
 - [80] E. Bisong, An overview of google cloud platform services, *Building Machine Learning and Deep Learning Models on Google Cloud Platform: A Comprehensive Guide for Beginners* (2019) 7–10.
 - [81] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, S. R. Chaudhry, Iot architecture challenges and issues: Lack of standardization, in: *Future Technologies Conference*, IEEE, 2016, pp. 731–738.
 - [82] R. B. Ness, J. P. Committee, Influence of the hipaa privacy rule on health research, *Jama* 298 (18) (2007) 2164–2170.
 - [83] T. Linden, R. Khandelwal, H. Harkous, K. Fawaz, The privacy policy landscape after the gdpr, *Proceedings on Privacy Enhancing Technologies* 2020 (1) (2020) 47–64.
 - [84] K. Zaghouani, A. Yachir, B. Djamaa, A. Boutouba, Adoption and application of blockchain technology in iot: Survey and open issues, in: *2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAEECS)*, IEEE, 2023, pp. 1–6.
 - [85] J. Li, G. Wei, Research on coap resource directory based on blockchain, in: *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Vol. 1, IEEE, 2020, pp. 1730–1735.
 - [86] K. Zaghouani, B. Djamaa, A. Yachir, Drdchain: a blockchain-based distributed resource directory for the internet of things, *Cluster Computing* (2023) 1–22.
 - [87] G. S. Ramachandran, K.-L. Wright, L. Zheng, P. Navaney, M. Naveed, B. Krishnamachari, J. Dhaliwal, Trinity: A byzantine fault-tolerant distributed publish-subscribe system with immutable blockchain-based persistence, in: *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2019, pp. 227–235.
 - [88] L. S. Vailshery, Number of iot connected devices worldwide 2019–2021, with forecasts to 2030 (2022).
URL <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>
 - [89] P. R. Sathia Bhama, C. P. Jayabal, Metainfochain: Bi-layered blockchain consensus for metadata aggregation in iot and cloud environments, *Transactions on Emerging Telecommunications Technologies* 32 (12) (2021) e4362.
 - [90] R. Mühlberger, S. Bachhofner, E. Castelló Ferrer, C. Di Ciccio, I. Weber, M. Wöhrer, U. Zdun, Foundational oracle patterns: Connecting

- blockchain to the off-chain world, in: Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2020 Blockchain and RPA Forum, Seville, Spain, September 13–18, 2020, Proceedings 18, Springer, 2020, pp. 35–51.
- [91] M. Gu, Ethereum 2.0 – here’s what you need to know. (2023).
URL <https://boxmining.com/ethereum-2/>
 - [92] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, P. Saxena, A secure sharding protocol for open blockchains, in: SIGSAC conference on computer and communications security, ACM, 2016, pp. 17–30.
 - [93] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, B. Ford, Omniledger: A secure, scale-out, decentralized ledger via sharding, in: Symposium on Security and Privacy, IEEE, 2018, pp. 583–598.
 - [94] ZILLIQA Team, Zilliqa, technical whitepaper (2017).
URL <https://docs.zilliqa.com/whitepaper.pdf>
 - [95] Harmony Team, Harmony, technical whitepaper.
URL <https://harmony.one/whitepaper.pdf>
 - [96] G. Wood, An introduction to polkadot (2020).
URL <https://assets.polkadot.network/Polkadot-lightpaper.pdf>
 - [97] M. Zamani, M. Movahedi, M. Raykova, Rapidchain: Scaling blockchain via full sharding, in: SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 931–948.
 - [98] J. Wang, H. Wang, Monoxide: Scale out blockchains with asynchronous consensus zones, in: NSDI, Vol. 2019, 2019, pp. 95–112.
 - [99] W. F. Silvano, R. Marcelino, Iota tangle: A cryptocurrency to communicate internet-of-things data, Future Generation Computer Systems 112 (2020) 307–319.
 - [100] Y. Sompolinsky, Y. Lewenberg, A. Zohar, Spectre: A fast and scalable cryptocurrency protocol, IACR Cryptol. ePrint Archive, Rep. 2016/1159 (2016).
 - [101] T. Zhou, X. Li, H. Zhao, Dlattice: A permission-less blockchain based on dpos-ba-dag consensus for data tokenization, IEEE Access 7 (2019) 39273–39287.
 - [102] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, A. C.-C. Yao, A decentralized blockchain with high throughput and fast confirmation, in: {USENIX} Annual Technical Conference ({USENIX}{ATC} 20), 2020, pp. 515–528.
 - [103] M. Kedziora, D. Pieprzka, I. Jozwiak, Y. Liu, H. Song, Analysis of segregated witness implementation for increasing efficiency and security of the bitcoin cryptocurrency, Journal of Information and Telecommunication 7 (1) (2023) 44–55.
 - [104] M. A. Javarone, C. S. Wright, From bitcoin to bitcoin cash: a network analysis, in: Workshop on Cryptocurrencies and Blockchains for Distributed Systems, 2018, pp. 77–81.
 - [105] J. Rubin, M. Naik, N. Subramanian, Merkelized abstract syntax trees.
URL <https://www.mit.edu/~jlrubin/public/pdfs/858report.pdf>
 - [106] G. Wang, Z. J. Shi, M. Nixon, S. Han, Sok: Sharding on blockchain, in: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 2019, pp. 41–61.
 - [107] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, B. C. Ooi, Towards scaling blockchain systems via sharding, in: Proceedings of the 2019 international conference on management of data, 2019, pp. 123–140.
 - [108] H. W. Y. Adoni, T. Nahhal, M. Krichen, B. Aghezzaf, A. Elbyed, A survey of current challenges in partitioning and processing of graph-structured data in parallel and distributed systems, Distributed and Parallel Databases 38 (2020) 495–530.
 - [109] Q. Wang, J. Yu, S. Chen, Y. Xiang, Sok: Diving into dag-based blockchain systems, arXiv preprint arXiv:2012.06128 (2020).
 - [110] M. Joureko, K. Kurazumi, M. Larangeira, K. Tanaka, Sok: A taxonomy for layer-2 scalability related protocols for cryptocurrencies, Cryptology ePrint Archive (2019).
 - [111] L. T. Thibault, T. Sarry, A. S. Hafid, Blockchain scaling using rollups: A comprehensive survey, IEEE Access (2022).
 - [112] C. Sguanci, R. Spatafora, A. M. Vergani, Layer 2 blockchain scaling: A survey, arXiv preprint arXiv:2107.10881 (2021).
 - [113] R. Neiheiser, G. Inácio, L. Rech, C. Montez, M. Matos, L. Rodrigues, Practical limitations of ethereum’s layer-2, IEEE Access 11 (2023) 8651–8662.
 - [114] J. Kilian, A note on efficient zero-knowledge proofs and arguments, in: Symposium on Theory of Computing, ACM, 1992, pp. 723–732.
URL <https://www.sciencedirect.com/science/article/pii/S0920548923000016>
 - [115] Polygon Labs, Polygon (matic) (2023).
URL <https://wiki.polygon.technology/docs/home/new-to-polygon/>
 - [116] Optimism, Ethereum, scaled.
URL <https://www.optimism.io/>
 - [117] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, E. W. Felten, Arbitrum: Scalable, private smart contracts, in: {USENIX} Security Symposium ({USENIX} Security 18), 2018, pp. 1353–1370.
 - [118] Z. Williamson, The aztec protocol (2018).
URL <https://github.com/AztecProtocol/aztec-v1/blob/master/AZTEC.pdf>
 - [119] D. Wang, J. Zhou, A. Wang, M. Finestone, Loopring: A decentralized token exchange protocol (2018).
URL https://github.com/Loopring/whitepaper/blob/master/en_whitepaper.pdf
 - [120] J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments (2016).
URL <https://lightning.network/lightning-network-paper.pdf>
 - [121] T. Team, Universal off-chain scaling solution (2020).
URL <https://trinity.tech/>
 - [122] R. Network-Fast, Cheap, scalable token transfers for ethereum (2020).
URL <https://raiden.network/>
 - [123] S. D. Lerner, Rsk, White Paper (2015).
URL <https://rootstock.io/static/77b8332baf312e6f354e938e1ddbe252/rsk-white-paper-updated.pdf>
 - [124] J. Poon, V. Buterin, Plasma: Scalable autonomous smart contracts (2017).

- URL <https://www.plasma.io/plasma.pdf>
- [125] M. Dong, Q. Liang, X. Li, J. Liu, Celer network: Bring internet scale to every blockchainArXiv:1810.00037 (2018).
 - [126] Skale Lab, The skale network: An ethereum interoperable elastic blockchain network, Online: <https://skale.space/whitepaper> (2020).
 - [127] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, K.-K. R. Choo, Sidechain technologies in blockchain networks: An examination and state-of-the-art review, *Journal of Network and Computer Applications* 149 (2020) 102471.
 - [128] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, P. Lorenz, Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for internet of vehicles environment, *IEEE Transactions on Vehicular Technology* 71 (9) (2022) 9853–9867.
 - [129] J. Daemen, V. Rijmen, Aes proposal: Rijndael (1999).
URL https://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf
 - [130] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, The simon and speck families of lightweight block ciphers, *cryptology eprint archive* (2013).
URL <https://eprint.iacr.org/2013/404.pdf>
 - [131] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, C. Viskelson, Present: An ultra-lightweight block cipher, in: *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*, Springer, 2007, pp. 450–466.
 - [132] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, I. Verbauwhede, Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms, *Cryptology ePrint Archive* (2014).
URL <https://eprint.iacr.org/2014/084.pdf>
 - [133] C. De Canniere, O. Dunkelman, M. Knežević, Katan and ktantan—a family of small and efficient hardware-oriented block ciphers, in: *Cryptographic Hardware and Embedded Systems-CHES 2009: 11th International Workshop Lausanne, Switzerland, September 6-9, 2009 Proceedings*, Springer, 2009, pp. 272–288.
 - [134] Y. Nir, A. Langley, Chacha20 and poly1305 for ietf protocols (2018).
URL <https://datatracker.ietf.org/doc/html/rfc7539>
 - [135] D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, D.-G. Lee, Lea: A 128-bit block cipher for fast encryption on common processors, in: *Information Security Applications: 14th International Workshop, WISA 2013, Jeju Island, Korea, August 19-21, 2013, Revised Selected Papers 14*, Springer, 2014, pp. 3–27.
 - [136] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, et al., Hight: A new block cipher suitable for low-resource device, in: *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*, Springer, 2006, pp. 46–59.
 - [137] T. Sugawara, N. Homma, T. Aoki, A. Satoh, High-performance asic implementations of the 128-bit block cipher clefia, in: *International Symposium on Circuits and Systems, IEEE, 2008*, pp. 2925–2928.
 - [138] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, T. Yalçın, Block ciphers—focus on the linear layer (feat. pride), in: *Advances in Cryptology—CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I 34*, Springer, 2014, pp. 57–76.
 - [139] D. A. Saraiva, V. R. Q. Leithardt, D. de Paula, A. Sales Mendes, G. V. González, P. Crocker, Prisec: Comparison of symmetric key algorithms for iot devices, *Sensors* 19 (19) (2019) 4312.
 - [140] P. Panahi, C. Bayılmış, U. Çavuşoğlu, S. Kaçar, Performance evaluation of lightweight encryption algorithms for iot-based applications, *Arabian Journal for Science and Engineering* 46 (2021) 4015–4037.
 - [141] D. Dinu, Y. L. Corre, D. Khovratovich, L. Perrin, J. Großschädl, A. Biryukov, Triathlon of lightweight block ciphers for the internet of things, *Journal of Cryptographic Engineering* 9 (2019) 283–302.
 - [142] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, C. Manifavas, A review of lightweight block ciphers, *Journal of Cryptographic Engineering* 8 (2018) 141–184.
 - [143] S. Sallam, B. D. Beheshti, A survey on lightweight cryptographic algorithms, in: *TENCON 2018-2018 IEEE Region 10 Conference, IEEE, 2018*, pp. 1784–1789.
 - [144] J. Guruprakash, S. Koppu, Ec-elgamal and genetic algorithm-based enhancement for lightweight scalable blockchain in iot domain, *IEEE Access* 8 (2020) 141269–141281.
 - [145] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for iot systems, *Cluster Computing* 23 (3) (2020) 2067–2087.
 - [146] X. Qin, Y. Huang, Z. Yang, X. Li, Lbac: A lightweight blockchain-based access control scheme for the internet of things, *Information sciences* 554 (2021) 222–235.
 - [147] W. Yan, N. Zhang, L. L. Njilla, X. Zhang, Pcbchain: Lightweight reconfigurable blockchain primitives for secure iot applications, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28 (10) (2020) 2196–2209.
 - [148] S. Khan, W.-K. Lee, S. O. Hwang, Aechain: A lightweight blockchain for iot applications, *IEEE Consumer Electronics Magazine* 11 (2) (2021) 64–76.
 - [149] X. Yang, X. Yang, X. Yi, I. Khalil, X. Zhou, D. He, X. Huang, S. Nepal, Blockchain-based secure and lightweight authentication for internet of things, *IEEE Internet of Things Journal* 9 (5) (2021) 3321–3332.
 - [150] P. Olsen, M. Borit, The components of a food traceability system, *Trends in Food Science & Technology* 77 (2018) 143–149.
 - [151] R. J. Robles, T.-h. Kim, Applications, systems and methods in smart home technology: A review, *International Journal of Advanced Science And Technology* 15 (2010) 37–48.
 - [152] R. Khalid, N. Javaid, S. Javaid, M. Imran, N. Naseer, A blockchain-based decentralized energy management in a p2p trading system, in: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, 2020, pp. 1–6.
 - [153] J. Camp, Digital identity, *IEEE Technology and Society Magazine* 23 (3) (2004) 34–41.
 - [154] M. T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: A decentralized blockchain-based authentication system for iot, *Computers & Security* 78 (2018) 126–142.
 - [155] A. Sheth, H. Subramanian, Blockchain and contract theory: modeling smart contracts using insurance markets, *Managerial Finance* 46 (6)

- (2019) 803–814.
- [156] M. Afzal, Q. Huang, W. Amin, K. Umer, A. Raza, M. Naeem, Blockchain enabled distributed demand side management in community energy system with smart homes, *IEEE Access* 8 (2020) 37428–37439.
 - [157] K. C. Tan, Supply chain management: practices, concerns, and performance issues, *Journal of Supply Chain Management* 38 (4) (2002) 42–53.
 - [158] M. M. Queiroz, R. Telles, S. H. Bonilla, Blockchain and supply chain management integration: a systematic review of the literature, *Supply Chain Management: An international journal* 25 (2) (2020) 241–254.
 - [159] H. Min, Blockchain technology for enhancing supply chain resilience, *Business Horizons* 62 (1) (2019) 35–45.
 - [160] N. Kawaguchi, Application of blockchain to supply chain: Flexible blockchain technology, *Procedia Computer Science* 164 (2019) 143–148.
 - [161] N. Kshetri, Blockchain systems and ethical sourcing in the mineral and metal industry: a multiple case study, *The International Journal of Logistics Management* 33 (1) (2022) 1–27.
 - [162] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: *International Conference on Open and Big Data*, IEEE, 2016, pp. 25–30.
 - [163] G. Prisco, The blockchain for healthcare: Gem launches gem health network with philips blockchain lab, *Bitcoin Magazine* (2016). URL <https://bitcoinmagazine.com/business/the-blockchain-for-healthcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938>
 - [164] K. Abouelmehdi, A. Beni-Hessane, H. Khaloufi, Big healthcare data: preserving security and privacy, *Journal of Big Data* 5 (1) (2018) 1–18.
 - [165] A. Al Omar, M. S. Rahman, A. Basu, S. Kiyomoto, Medibchain: A blockchain based privacy preserving platform for healthcare data, in: *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops*, Guangzhou, China, December 12–15, 2017, *Proceedings* 10, Springer, 2017, pp. 534–543.
 - [166] N. Menachemi, T. H. Collum, Benefits and drawbacks of electronic health record systems, *Risk Management and Healthcare Policy* (2011) 47–55.
 - [167] H. B. Mahajan, A. S. Rashid, A. A. Junnarkar, N. Uke, S. D. Deshpande, P. R. Futane, A. Alkhayyat, B. Alhayani, Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems, *Applied Nanoscience* 13 (3) (2023) 2329–2342.
 - [168] P. Ndayizigamiye, S. Dube, Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in south africa, in: *International Multidisciplinary Information Technology and Engineering Conference*, IEEE, 2019, pp. 1–5.
 - [169] E. Settanni, T. S. Harrington, J. S. Srai, Pharmaceutical supply chain models: A synthesis from a systems view of operations research, *Operations Research Perspectives* 4 (2017) 74–95.
 - [170] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, L. Tawalbeh, Health care insurance fraud detection using blockchain, in: *International Conference on Software Defined Systems*, IEEE, 2020, pp. 145–152.
 - [171] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, *Renewable and Sustainable Energy Reviews* 100 (2019) 143–174.
 - [172] F. Teng, Q. Zhang, G. Wang, J. Liu, H. Li, A comprehensive review of energy blockchain: Application scenarios and development trends, *International Journal of Energy Research* 45 (12) (2021) 17515–17531.
 - [173] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—the new and improved power grid: A survey, *IEEE Communications Surveys & Tutorials* 14 (4) (2011) 944–980.
 - [174] P. Wongthongtham, D. Marrable, B. Abu-Salih, X. Liu, G. Morrison, Blockchain-enabled peer-to-peer energy trading, *Computers & Electrical Engineering* 94 (2021) 107299.
 - [175] F. Imbault, M. Swiatek, R. de Beaufort, R. Plana, The green blockchain: Managing decentralized energy production and consumption, in: *International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe*, IEEE, 2017, pp. 1–5.
 - [176] B. Römer, P. Reichhart, J. Kranz, A. Picot, The role of smart metering and decentralized electricity storage for smart grids: The importance of positive externalities, *Energy Policy* 50 (2012) 486–495.
 - [177] H. Saboori, M. Mohammadi, R. Taghe, Virtual power plant (vpp), definition, concept, components and types, in: *Asia-Pacific Power and Energy Engineering Conference*, IEEE, 2011, pp. 1–4.
 - [178] E. Mengelkamp, J. Gärtner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing microgrid energy markets: A case study: The brooklyn microgrid, *Applied Energy* 210 (2018) 870–880.
 - [179] A. Trbovich, S. Hambridge, D. van den Biggelaar, E. Hesse, F. Sioshansi, D3a energy exchange for a transactive grid, in: *Behind and Beyond the Meter*, Elsevier, 2020, pp. 267–284.
 - [180] F. Tian, An agri-food supply chain traceability system for china based on rfid & blockchain technology, in: *International Conference on Service Systems and Service Management*, IEEE, 2016, pp. 1–6.
 - [181] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, M. Alam, Blockchain-based agri-food supply chain: A complete solution, *IEEE Access* 8 (2020) 69230–69243.
 - [182] M. Barbieri, D. Gassen, Blockchain-can this new technology really revolutionize the land registry system, in: *Responsible Land Governance: Towards an Evidence Based Approach: Proceedings of the Annual World Bank Conference on Land and Poverty*, 2017, pp. 1–13.
 - [183] N. Kshetri, Blockchain-based smart contracts to provide crop insurance for smallholder farmers in developing countries, *IT Professional* 23 (6) (2021) 58–61.
 - [184] M. Du, Q. Chen, J. Xiao, H. Yang, X. Ma, Supply chain finance innovation using blockchain, *IEEE Transactions on Engineering Management* 67 (4) (2020) 1045–1058.
 - [185] A. Al Sadawi, M. S. Hassan, M. Ndiaye, A survey on the integration of blockchain with iot to enhance performance and eliminate challenges, *IEEE Access* 9 (2021) 54478–54497.
 - [186] S. Sun, R. Du, S. Chen, W. Li, Blockchain-based iot access control system: towards security, lightweight, and cross-domain, *IEEE Access* 9 (2021) 36868–36878.
 - [187] A. Rasheed, R. N. Mahapatra, C. Varol, K. Narashimha, Exploiting zero knowledge proof and blockchains towards the enforcement of anonymity, data integrity and privacy (adip) in the iot, *IEEE Transactions on Emerging Topics in Computing* 10 (3) (2021) 1476–1491.

- [188] A. Anjum, A. Siddiqua, S. Sabeer, S. Kondapalli, C. Kaur, K. Rafi, Analysis of security threats, attacks in the internet of things, *International Journal of Mechanical Engineering* 6 (2021) 2943–2946.
- [189] N. Jhanjhi, M. Humayun, S. N. Almuayqil, Cyber security and privacy issues in industrial internet of things, *Computer Systems Science and Engineering* 37 (3) (2021) 361–380.
- [190] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, H. Karimipour, Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks, *Computers in Industry* 144, art. no. 103801 (2023).
- [191] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, G. Srivastava, P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot, *IEEE Transactions on Industrial Informatics* 18 (9) (2022) 6358–6367.
- [192] F. Alkhabbas, M. Alsadi, S. Alawadi, F. M. Awaysheh, V. R. Kebande, M. T. Moghaddam, Assert: A blockchain-based architectural approach for engineering secure self-adaptive iot systems, *Sensors* 22 (18), art. no. 6842 (2022).
- [193] F. Daidone, B. Carminati, E. Ferrari, Blockchain-based privacy enforcement in the iot domain, *IEEE Transactions on Dependable and Secure Computing* 19 (6) (2021) 3887–3898.
- [194] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A.-N. Benharkat, E. Benkhelifa, Data privacy based on iot device behavior control using blockchain, *ACM Transactions on Internet Technology* 21 (1) (2021) 1–20.
- [195] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, J. Wang, Z. Almakhdme, A. Tolba, Multiple cloud storage mechanism based on blockchain in smart homes, *Future Generation Computer Systems* 115 (2021) 304–313.
- [196] Y. Ren, Y. Leng, Y. Cheng, J. Wang, Secure data storage based on blockchain and coding in edge computing, *Math. Biosci. Eng* 16 (4) (2019) 1874–1892.
- [197] S. Dhar, A. Khare, A. D. Dwivedi, R. Singh, Securing iot devices: A novel approach using blockchain and quantum cryptography, *Internet of Things* 25 (2024) 101019.
- [198] A. Sasikumar, L. Ravi, M. Devarajan, A. Selvalakshmi, A. T. Almaktoom, A. S. Almazyad, G. Xiong, A. W. Mohamed, Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial internet of things, *IEEE Access* (2024).
- [199] H. Liu, D. Han, D. Li, Fabric-iot: A blockchain-based access control system in iot, *IEEE Access* 8 (2020) 18207–18218.
- [200] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem, A. Basuhail, M. Yamin, Hierarchical blockchain-based multi-chaincode access control for securing iot systems, *Electronics* 11 (5), art. no. 711 (2022).
- [201] F. Yang, S. Wang, J. Li, Z. Liu, Q. Sun, An overview of internet of vehicles, *China Communications* 11 (10) (2014) 1–15.
- [202] V. Rajaravivarma, Y. Yang, T. Yang, An overview of wireless sensor network and applications, in: *Southeastern Symposium on System Theory*, IEEE, 2003, pp. 432–436.
- [203] S. Malik, V. Dedeoglu, S. S. Kanhere, R. Jurdak, Trustchain: Trust management in blockchain and iot supported supply chains, in: *International Conference on Blockchain (Blockchain)*, IEEE, 2019, pp. 184–193.
- [204] X. Wu, J. Liang, A blockchain-based trust management method for internet of things, *Pervasive and Mobile Computing* 72, art. no. 101330 (2021).
- [205] N. Javaid, A secure and efficient trust model for wireless sensor iots using blockchain, *IEEE Access* 10 (2022) 4568–4579.
- [206] X. Wu, Y. Liu, J. Tian, Y. Li, Privacy-preserving trust management method based on blockchain for cross-domain industrial iot, *Knowledge-Based Systems* 283 (2024) 111166.
- [207] L. Bi, T. Muazu, O. Samuel, Iot: A decentralized trust management system using blockchain-empowered federated learning, *Sustainability* 15 (1), art. no. 374 (2022).
- [208] M. Asif, Z. Aziz, M. Bin Ahmad, A. Khalid, H. A. Waris, A. Gilani, Blockchain-based authentication and trust management mechanism for smart cities, *Sensors* 22 (7), art. no. 2604 (2022).
- [209] Y. Yan, J. Chen, Y. Yao, S. Guo, A. Xiong, W. Zhang, Power iot system architecture integrating trusted computing and blockchain, *Wireless Communications and Mobile Computing* 2022, art. no. 2891917 (2022).
- [210] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K.-K. R. Choo, G. Min, A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things, *IEEE Transactions on Computers* (2022).
URL <https://doi.org/10.1109/TC.2022.3157996>
- [211] M. Turki, S. Cheikhrouhou, B. DAMMAK, M. Baklouti, R. Mars, A. Dhahbi, Nft-iot pharma chain: Iot drug traceability system based on blockchain and non fungible tokens (nfts), *Journal of King Saud University-Computer and Information Sciences* 35 (2) (2023) 527–543.
- [212] M. S. Al-Rakhami, M. Al-Mashari, Prochain: provenance-aware traceability framework for iot-based supply chain systems, *IEEE Access* 10 (2021) 3631–3642.
- [213] T. Li, H. Wang, D. He, J. Yu, Permissioned blockchain-based anonymous and traceable aggregate signature scheme for industrial internet of things, *IEEE Internet of Things Journal* 8 (10) (2020) 8387–8398.
- [214] F.-J. Ferrández-Pastor, J. Mora-Pascual, D. Díaz-Lajara, Agricultural traceability model based on iot and blockchain: Application in industrial hemp production, *Journal of Industrial Information Integration* 29, art. no. 100381 (2022).
- [215] J. Song, Y. Yang, J. Mei, G. Zhou, W. Qiu, Y. Wang, L. Xu, Y. Liu, J. Jiang, Z. Chu, et al., Proxy re-encryption-based traceability and sharing mechanism of the power material data in blockchain environment, *Energies* 15 (7), art. no. 2570 (2022).
- [216] J. Li, Z. Wang, S. Guan, Y. Cao, Prochain: A privacy-preserving blockchain-based supply chain traceability system model, *Computers & Industrial Engineering* 187 (2024) 109831.
- [217] R. Brandín, S. Abrishami, Iot-bim and blockchain integration for enhanced data traceability in offsite manufacturing, *Automation in Construction* 159 (2024) 105266.
- [218] M. S. Siddiqui, T. A. Syed, A. Nadeem, W. Nawaz, S. S. Albouq, Blocktrack-l: A lightweight blockchain-based provenance message tracking in iot, *International Journal of Advanced Computer Science and Applications* 11 (4) (2020) 463–470.
- [219] Z. Shahbazi, Y.-C. Byun, A procedure for tracing supply chains for perishable food based on blockchain, machine learning and fuzzy logic, *Electronics* 10 (1), art. no. 41 (2020).
- [220] N. Alkaabi, K. Salah, R. Jayaraman, J. Arshad, M. Omar, Blockchain-based traceability and management for additive manufacturing, *IEEE access* 8 (2020) 188363–188377.
- [221] T. M. Hewa, A. Kalla, A. Nag, M. E. Ylianttila, M. Liyanage, Blockchain for 5g and iot: Opportunities and challenges, in: *International*

- Conference on Communications and Networking, IEEE, 2020, pp. 1–8.
- [222] S. Biswas, K. Sharif, F. Li, B. Nour, Y. Wang, A scalable blockchain framework for secure transactions in iot, *IEEE Internet of Things Journal* 6 (3) (2018) 4650–4659.
 - [223] A. Chauhan, O. P. Malviya, M. Verma, T. S. Mor, Blockchain and scalability, in: *International Conference on Software Quality, Reliability and Security Companion*, IEEE, 2018, pp. 122–128.
 - [224] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, M. F. Yusof, Scalability challenges in healthcare blockchain system—a systematic review, *IEEE Access* 8 (2020) 23663–23673.
 - [225] S. M. H. Bamakan, A. Motavali, A. B. Bondarti, A survey of blockchain consensus algorithms performance evaluation criteria, *Expert Systems with Applications* 154, art. no. 113385 (2020).
 - [226] N. Mohamed, J. Al-Jaroodi, Applying blockchain in industry 4.0 applications, in: *Annual Computing and Communication Workshop and Conference*, IEEE, 2019, pp. 0852–0858.
 - [227] L. Grieco, A. Rizzo, S. Colucci, S. Sicari, G. Piro, D. Di Paola, G. Boggia, Iot-aided robotics applications: Technological implications, target domains and open issues, *Computer Communications* 54 (2014) 32–47. doi:<https://doi.org/10.1016/j.comcom.2014.07.013>. URL <https://www.sciencedirect.com/science/article/pii/S0140366414002783>
 - [228] P. Voigt, A. Von dem Bussche, *The eu general data protection regulation (gdpr)*, Springer International Publishing. URL <https://link.springer.com/book/10.1007/978-3-319-57959-7>
 - [229] S. Guergov, N. Radwan, Blockchain convergence: Analysis of issues affecting iot, ai and blockchain, *International Journal of Computations, Information and Manufacturing* 1 (1) (2021). URL <https://doi.org/10.54489/ijcim.v1i1.48>
 - [230] S. Al-Sarawi, M. Anbar, K. Alieyan, M. Alzubaidi, Internet of things (iot) communication protocols, in: *International Conference on Information Technology*, IEEE, 2017, pp. 685–690.
 - [231] S. J. Dwyer III, A. C. Weaver, K. K. Hughes, Health insurance portability and accountability act, *Security Issues in the Digital Medical Enterprise* 72 (2) (2004) 9–18.
 - [232] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, V. Singh, A survey of payment card industry data security standard, *IEEE Communications Surveys & Tutorials* 12 (3) (2010) 287–303.
 - [233] M. Saraswat, R. Tripathi, Cloud computing: Comparison and analysis of cloud service providers-aws, microsoft and google, in: *International Conference System Modeling and Advancement in Research Trends*, IEEE, 2020, pp. 281–285.
 - [234] A. Yegin, T. Kramp, P. Dufour, R. Gupta, R. Soss, O. Hersent, D. Hunt, N. Sornin, Lorawan protocol: specifications, security, and capabilities, in: *LPWAN Technologies for iot and m2m applications*, Elsevier, 2020, pp. 37–63.
 - [235] A. S. Yahaya, N. Javaid, M. U. Javed, M. Shafiq, W. Z. Khan, M. Y. Aalsalem, Blockchain-based energy trading and load balancing using contract theory and reputation in a smart community, *IEEE Access* 8 (2020) 222168–222186.
 - [236] S. Pratiksha, M. Kavitha, Survey on impact of green blockchain in green marketing—chennai city, in: *Green Blockchain Technology for Sustainable Smart Cities*, Elsevier, 2023, pp. 303–323.
 - [237] M. Naehrig, K. Lauter, V. Vaikuntanathan, Can homomorphic encryption be practical?, in: *Cloud computing Security Workshop*, ACM, 2011, pp. 113–124.
 - [238] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, A survey on essential components of a self-sovereign identity, *Computer Science Review* 30 (2018) 80–86.
 - [239] M. Barbosa, P. Farshim, Certificateless signcryption, in: *Symposium on Information, Computer and Communications Security*, ACM, 2008, pp. 369–372.
 - [240] Ieee standard for framework of blockchain-based internet of things (iot) data management, *IEEE Std 2144.1-2020* (2021) 1–20doi:10.1109/IEEESTD.2021.9329260.
 - [241] L. Cao, Decentralized ai: Edge intelligence and smart blockchain, metaverse, web3, and desc, *IEEE Intelligent Systems* 37 (3) (2022) 6–19.
 - [242] M. Mudassar, Y. Zhai, L. Lejian, Adaptive fault-tolerant strategy for latency-aware iot application executing in edge computing environment, *IEEE Internet of Things Journal* 9 (15) (2022) 13250–13262.
 - [243] A. K. Nair, J. Sahoo, E. D. Raj, Privacy preserving federated learning framework for iomt based big data analysis using edge computing, *Computer Standards Interfaces* 86 (2023) 103720. doi:<https://doi.org/10.1016/j.csi.2023.103720>. URL <https://www.sciencedirect.com/science/article/pii/S0920548923000016>
 - [244] T. Li, A. K. Sahu, A. Talwalkar, V. Smith, Federated learning: Challenges, methods, and future directions, *Signal Processing Magazine* 37 (3) (2020) 50–60.
 - [245] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, H. V. Poor, Federated learning meets blockchain in edge computing: Opportunities and challenges, *IEEE Internet of Things Journal* 8 (16) (2021) 12806–12825.