Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan *Vol. 29 No. 3-2024*
ISSN:1813-1786 (Print) 2313-7770 (Online)

Examining the Implications of Blockchain Integration in IoT Environments

M. Hassan [1]

[1] *College of Information Technology, Jilin Agricultural University, Changchun, China*

[1] musharafhassanmayo@gmail.com

Abstract- A dramatic shift in the present network architecture exemplifies how two of the most promising new technologies, blockchain and the Internet of Things (IoT), are already reshaping our digital future. The Internet of Things (IoT) has given our everyday items intelligence, allowing them to interact with us and each other in new ways. This has led to the accumulation of vast amounts of data, which can be analyzed and used to make intelligent decisions. It has changed the very nature of how we see the physical world and brought our ideal of the seamless merger of the digital and physical realms to fruition. But the problem with existing Internet of Things solutions is that they need a third party with control over everything—like a cloud server. The most important consequences of the most difficult Internet of Things (IoT) situations, as shown by recent studies, when it comes to connecting and interacting online, are covered in this study. An unexpected initial step in the design process is to propose a decentralized system, similar to a distributed or P2P (peer-to-peer) network, which poses a much greater threat to data privacy and security because of the enormous amounts of sensitive information that would be generated. This case illustrates how the blockchain may provide a reliable and decentralized/P2P architecture for exchanging information and accomplishing goals such as immutability of data, auditability, resilience, security, privacy, and access. By combining blockchain with IoT, we can address each technology's limitations and reap the full advantages of both. The Internet of Things (IoT) and Bitcoin are also covered in detail in this study. We walk you through every aspect of the two systems, from the fundamentals of blockchain technology to the inner workings of the blockchain-based Internet of Things (BIoT), and even show you some BIoT apps and how they compare to the others.

Keywords- Blockchain and IoT Applications, Blockchain, Internet of Things

I. INTRODUCTION

Built from the ground up for Bitcoin, the blockchain is a decentralized database that anybody can use[1]. An interconnected network of everyday "smart" things that can exchange data and coordinate their actions without human intervention is known as the "Internet of Things" (IoT). The efficient and rapid swapping of records is made possible by the IoT. Security, general performance, and operational efficiency have all been enhanced thanks to IoT-enabled devices[2]. You may also think of the Internet of Things as one giant global network[3]. Businesses that must adopt IoT packages expect revenues to skyrocket in the IoT sector[4]. Intelligent devices and equipment that can exchange data with one another and with the underlying infrastructure make up the Internet of Things (IoT)[5]. Physical and digital objects that can communicate with one another make up the "things" in the Internet of Things[6]. As shown in Figure 1, the Internet of Things (IoT) could be static[7].

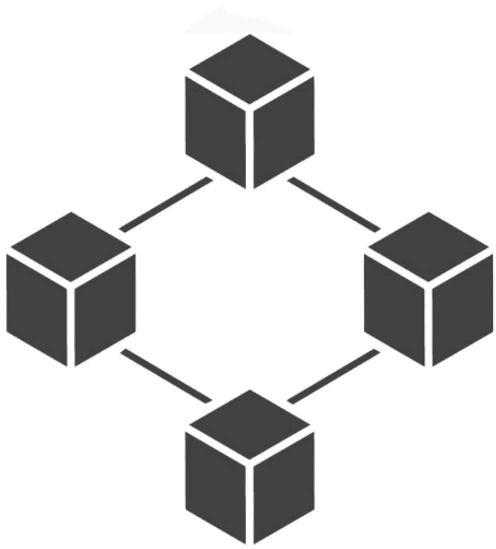

Figure 1: Structural Design of a Blockchain System

"We are on the cusp of a new digital age, and the coming together of blockchain with the IoT promises to be a game-changer for all of our linked devices[8-9]. Strong solutions that can guarantee efficiency, scalability, and security are required to keep up with the fast-paced development of the digital ecosystem, which is characterized by an ever-growing array of smart devices and systems[10]. With its decentralized, transparent, and immutable nature, blockchain technology stands out as a promising solution that could tackle some of the biggest problems with IoT networks[11-12]. Innovative applications that can reinvent interactions within the digital and physical realms are made possible by this unique confluence of technology, which also promises increased security and operational efficiency. We must carefully analyze the interdependent possibilities of blockchain and the Internet of Things (IoT) as we go further into this integration[13-14]. We must investigate how blockchain might improve the IoT environment and discover the subtleties of this partnership that may determine the destiny of digital connectedness."

1.1 Challenges in IoT

Given its pervasiveness in modern life, the Internet of Things (IoT) is undeniably more than just a notion these days[15-16]. The "cellphone" is the most ubiquitous example of an Internet of Things framework in everyday life. Smart homes are only one use of the Internet of Things. Commercial agriculture, public safety, and healthcare are just a few of the many areas that make up this vast enterprise[17]. The Internet of Things is another name for the IoE. The Internet of Things (IoT) is a network of interconnected computing devices that can exchange data and coordinate their actions autonomously, and there are many different kinds of IoT real-global software. The fast and environmentally friendly transport of data is thus made possible. Equipment that can connect to the Internet of Things boosts productivity, performance, and security[18].

Many commercial, consumer, and defense-related IoT activities rely on data collecting, processing, and storage[19]. This encompasses a wide range of topics, such as smart buildings, environmental monitoring, organization evaluations, and networked architecture. There is a deluge of data being exchanged right now[20]. However, IoT devices are variable in terms of energy consumption due to the large-scale and contractual architecture of IoT networks[21-22]. As an aside, protecting user privacy and security in the IoT is still an important concern. For reasons of privacy and security, or because the data it contains is sensitive, the information collected by IoT devices is often of the utmost importance[23]. Due to the pervasive vulnerabilities of devices in IoT networks, cyberattacks have impacted several populations.

1.1.1 Real-World Applications of Blockchain in IoT

Many companies have successfully integrated blockchain technology with IoT in recent years. This shows how useful it can be. For example, companies such as Siemens in the industrial sector have been using blockchain to improve the visibility and traceability of their supply chains[24]. Using IoT devices to monitor the status of both products in real time and immutable records of the blockchain to ensure the legality of the products. It will help reduce fraud. In the same way city of Dubai has been using blockchain solutions to improve or control traffic by connecting cars[25]. This reduces bottlenecks and greatly increases productivity. These cases show how blockchain and IoT can change things for the better. With real benefits like safety, speed, and more responsibility. Reading these case studies will help us understand how or blockchain can be used to solve problems in non-real world IoT environments[26].

Table 1: Applications of Blockchain Technology in IoT Across Various Sectors and Their Benefits

Company/ Organization	Application Area	Blockchain Use	Benefits
Siemens	Industrial Supply Chain	Enhances visibility and traceability of supply chains	Reduces fraud, ensures product legality
City of Dubai	Traffic Management	Connects cars for improved traffic control	Reduces bottlenecks, increases productivity
Various Industries	IoT Solutions	Integrates IoT devices with blockchain for various uses	Enhances safety, speed, and accountability

1.2 Centralized Models for Security and Communication

Most current safety systems, as well as structures for security and linguistic interaction, are centralized. The introduction of a few assaults (such as scenarios using IoT packages) and enterprises' inflexibility and one-to-many architecture both contribute to the imperfection of central operations. It is also challenging to scale conversation styles based on central agents when dealing with many IoT devices[27]. A further constraint and potentially catastrophic aspect is that all cable activity is likewise managed via cloud servers [28]. A formalized formal, as shown in Figure 2, is one example.

Table 2: IoT Communication Infrastructure

Limitations on Resources	User Data Protection
The majority of IoT devices are limited in their processing power, memory, and bandwidth[29]. Their limited resources are mostly used up by executing the main functionality of programs, so they need privacy and security solutions that are lightweight[30]. Traditional security and privacy solutions are inadequate for most IoT applications [28], as they consume a lot of energy and have a lot of communication and processing overhead.	As part of their functionality, IoT applications may gather, process, and transmit sensitive data[31]. Despite the disastrous consequences, many current IoT solutions flagrantly ignore user privacy[32]. Before delivering privacy-sensitive data to IoT service providers, conventional methods for protecting user privacy would usually summaries or amplify it with noise[33]. Internet of Things (IoT) service companies risk having their personalized offerings compromised if they get incomplete or incorrect data.

II. INTRODUCTION TO COMPARATIVE ANALYSIS

There is a revolutionary chance for the digital ecosystem at the crossroads of blockchain and the IoT[34]. Significant security, scalability, and efficiency concerns have emerged in response to the Internet of Things (IoT) as it develops further and incorporates intelligence into commonplace items and systems. These difficulties highlight the importance of having a solid foundation to back the expanding needs of IoT applications[35-36]. One promising approach to these problems is blockchain technology, which is known for its distributed ledger, immutability, and improved security features. Because there is a wide variety of blockchain technologies, each with its own set of advantages and disadvantages, it is essential to do a comparison in order to determine which blockchain is most suited for which Internet of Things (IoT) applications. The purpose of this introductory section is to explain why a comparative study is necessary to fully utilize blockchain in IoT domains[37].

When it comes to Internet of Things (IoT) applications, security is of the utmost importance because security flaws can lead to serious problems like money loss, compromised personal privacy, and threats to physical safety. Attacks are more likely to succeed in traditional centralized designs because of the vulnerabilities they offer[38]. By decentralizing decision-making and guaranteeing data integrity throughout the network, blockchain technology provides a more secure basis by doing away with centralized vulnerabilities[39]. However, factors like consensus methods, encryption standards, and network design impact the security guarantees, which vary across blockchain platforms[40]. In order to determine whether blockchain can provide the best security features tailored to the unique needs of an IoT application, it is essential to conduct a thorough comparison of various platforms.

The Internet of Things (IoT) ecosystem could include billions of networked devices producing massive volumes of data, scalability is an additional important factor to consider[41]. Scalability of Internet of Things applications is dependent on the blockchain platform's capacity to process and store this data efficiently, without substantial delays or additional expenses[42-43]. Problems with transaction throughput and rising prices have plagued traditional blockchains like Ethereum and Bitcoin in this area[44]. To counter these scalability issues, newer or more specialized platforms, such as IOTA and Hyperledger Fabric, suggest alternative topologies and consensus methods[45]. To make sure the selected technology can handle the expansion and data needs of IoT devices, it is crucial to know how each blockchain platform is likely to scale[46].

Transaction time, operational expenses, and energy use are all components of efficiency. Applications built for the Internet of Things necessitate fast transaction times and cheap operational expenses, especially those that deal with micro transactions and real-time data processing[47]. Additionally, blockchain solutions that are energy efficient are gaining popularity as people become more conscious of the environmental effects of technology. The underlying technology of blockchain platforms, including the network design and consensus algorithm type (e.g., Proof of Work, Directed Acyclic Graphs, etc.), have a significant impact on the platform's efficiency[48-49]. Stakeholders can make well-informed decisions based on efficiency needs when these disparities are clarified through a comparison analysis.

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGIES IN IOT

The integration of blockchain technology with the IoT is an exciting new direction for improving the scalability, efficiency, and security of the IoT. New difficulties arise when the Internet of Things (IoT) ecosystem grows to include an ever-expanding web of linked devices that gather and share data[50]. Among these, keeping user privacy intact, efficiently scaling the network to meet future demands, and strong security measures to safeguard sensitive data are all essential[51]. An attractive answer to these problems is blockchain technology, which is characterised by its decentralised structure, immutable record, and capacity to enable safe, transparent transactions. Presented below is a synopsis of three groundbreaking blockchain technologies: Ethereum, Hyperledger Fabric, and IOTA[52]. These platforms each have unique features and capabilities that are well-suited to certain areas of Internet of Things applications[41].

3.1 Blockchain Consensus Mechanisms

To learn how the blockchain network works It is very important to understand how agreement works. They're like rules for a game that make sure everyone agrees on how the game is going. Another popular way is Proof of Work (PoW), which is like a group of friends trying to decide on a place[53]. Every friend has to show that they've done their prep. (figuring out a hard math problem) before the group can make a choice This step helps make sure the deal is real. It can be slow and take a lot of power, though. Byzantine False Tolerance (BFT), which works like a vote among peers, is another way[54]. We told you wrong things because some of our friends were there. The group was still able to make good decisions because most people agreed. This method makes networks more trustworthy when some people in them are not trustworthy. To help us understand these ideas better, we can look at how the speed and stability of blockchain technology are affected by the different consensus methods. This is especially important for Internet of Things (IoT) apps[55].

Table 3: Key Consensus Mechanisms in Blockchain, Highlighting their Pros and Cons for IoT.

Consensus Mechanism	Description	Advantages	Dis-advantages	Relevance to IoT Applications
Proof of Work (PoW)	A consensus method where participants solve complex mathematical problems to validate transactions and create new blocks.	High security; prevents spam attacks	Slow transaction speed; high energy consumption	Suitable for applications needing high security but limited by speed.
Byzantine Fault Tolerance (BFT)	A mechanism that allows a network to reach consensus even if some nodes fail or act maliciously, through a majority vote.	Increases trustworthiness; can operate in unreliable environments	More complex to implement; can be slower	Enhances reliability in critical IoT systems where some nodes may fail.

3.2 Ethereum

3.2.1 Smart Contract Capabilities

By introducing smart contracts, which are agreements whose conditions are put into lines of code and self-execute, Ethereum, a public blockchain platform, shook up the blockchain industry[56]. With this function, middlemen can be eliminated from the automation of complicated operations and transactions. When used to the Internet of Things (IoT), Ethereum's smart contracts allow devices to independently carry out predetermined activities in response to specific events, such as making inter-device payments or automatically changing a smart thermostat. This automation does double duty: it makes IoT operations more efficient and it makes sure that all interactions and transactions are done safely and transparently, which builds trust in the IoT ecosystem[57-58].

3.2.2 Scalability and Transaction Costs

The consensus mechanism (Proof of Work) and the resulting constraints on transaction processing capacity are Ethereum's biggest scalability issues, notwithstanding the platform's unique features[59]. When dealing with Internet of Things (IoT) scenarios, the scalability problem becomes much more acute because of the large volume of transactions that these devices produce, which can cause network congestion and expensive transaction fees[36]. When it comes to large-scale Internet of Things applications, where efficiency and minimal operational expenses are of the utmost importance, these limitations make Ethereum seem less than ideal[60].

3.2.3 Suitability for IoT

When it comes to Internet of Things (IoT) settings, Ethereum shines when the advantages of smart contracts and decentralized apps (DApps) surpass the disadvantages of scalability and transaction fees[61]. Ethereum 2.0, which will include the Proof of Stake (PoS) consensus mechanism, is one of the upcoming improvements that aims to fix these scalability and efficiency problems, making it more suitable for more Internet of Things (IoT) uses[62].

3.3 Hyperledger Fabric

3.3.1 Modular and Permissioned Architecture

Hyperledger Fabric provides an alternative method with its enterprise-focused permissioned blockchain platform. Organizations can establish private or consortium blockchains with known and vetted players using Hyperledger Fabric, in contrast to Ethereum's public blockchain. The ability to control transactions and network members is enhanced by its permissioned nature and modular design, which helps to keep sensitive data secret and secure. Applications like healthcare and industrial IoT, which require stringent privacy controls and data protection, benefit greatly from such characteristics[63].

3.3.2 Efficiency and Privacy

The customizable consensus processes of Hyperledger Fabric do not necessitate energy-intensive mining, and the channels feature enables private transactions among a subset of participants, addressing efficiency and privacy issues. Important for business settings where data secrecy and integrity are paramount, this guarantees that IoT apps may grow efficiently without compromising security or privacy[31].

3.3.3 Suitability for IoT

Hyperledger Fabric is a great choice for enterprise-level IoT applications that need scalable, secure, and efficient blockchain implementations because of its architectural advantages[64]. Many companies are choosing it to improve their Internet of Things (IoT) applications because of its ability to process complicated, multi-party transactions while simultaneously protecting customer data[65].

3.4 IOTA

3.4.1 The Tangle Architecture

A Directed Acyclic Graph (DAG) that enables feeless transactions and scalability that grows with the amount of transactions, IOTA provides a new ledger technology called the Tangle[66]. Devices in IoT applications often carry out minor transactions, making this design ideal for them. One major drawback of conventional blockchain technology is the presence of transaction fees; however, IOTA's Tangle eliminates this problem, allowing for micropayments and the transmission of data in real time between devices[67].

3.4.2 Real-time Data Exchange

Because of its Tangle structure, IOTA can handle a lot of transactions, which is great for Internet of Things apps that need to send and receive data quickly. New Internet of Things (IoT) business models based on micropayment transactions and real-time data sharing can be developed thanks to this capacity, which enables IoT devices to send data and value to each other easily[68].

3.4.3 Suitability for IoT

IOTA is a ground breaking technology for Internet of Things (IoT) applications because to its design and capabilities. It is especially useful for applications that need efficient, scalable, and feeless transactions among a large network of devices[69]. Problems with network security and stability are, however, the subject of current study and development due to its innovative approach. Therefore, IOTA has enormous potential in the IoT, but its present status and future development path must be carefully considered."

Table 4: The Table Contrasts Ethereum, Hyperledger Fabric, and IOTA on Key Features for IoT Application Suitability.

Feature	**Ethereum**	**Hyperledger Fabric**	**IOTA**
Smart Contract Capabilities	Supports complex smart contracts, enabling automated operations and transactions within IoT networks.	Supports chain code for implementing business logic, but with a focus on permissioned network environments.	Does not support traditional smart contracts but introduces unique features like Masked Authenticated Messaging for secure data transmission.
Scalability	Faces challenges due to its PoW consensus mechanism, affecting transaction throughput and leading to potential bottlenecks in large-scale IoT applications.	Designed for scalability within enterprise environments, thanks to its permissioned nature and efficient consensus protocols.	Highly scalable due to the DAG-based Tangle architecture, facilitating fast transactions with increased network activity.
Transaction Costs	Incurs gas fees for transactions and smart contract execution, which can be prohibitive for microtransactions common in IoT applications.	No transaction fees within the network, making it cost-effective for internal business operations.	Enables feeless transactions, offering a significant advantage for IoT applications requiring frequent, small data exchanges.
Suitability for IoT	Well-suited for applications that can benefit from decentralized apps and complex smart contracts, considering scalability enhancements (Ethereum 2.0).	Ideal for enterprise-level IoT applications requiring high degrees of privacy, security, and scalable transaction processing.	Excellently suited for large-scale IoT ecosystems needing real-time data exchange and microtransactions, with considerations for its novel security model.

IV. BENEFITS OF BLOCKCHAIN INTEGRATION IN CONNECTED DEVICES

The quantity and importance of Bitcoin IoT solutions have increased over the last several years, and Figure 3 shows some of the possible benefits of deploying these solutions.

Figure 2: Benefits of Blockchain Integration in IoT Systems

Table 5: Impactful Benefits of Blockchain-Based Connectivity

1	**Tamper-Proof Tracking**	Due to the distributed consensus process and the hash linking the blocks, the transactions on a blockchain cannot be cracked. This ensures the secure gathering of data and the preservation of a record of all communications and transactions for users of the Internet of Things[70].
2	**Distributed Design**	In the event of a data breach or manipulation by an Internet of Things (IoT) device, the distributed ledger technology known as blockchain will prevent any one component of the system from failing or becoming vulnerable. Scalability and the avoidance of network bottlenecks are two further benefits of the distributed architecture.[71].
3	**Accountability**	On the blockchain, all transactions are transparent and can be traced back to their original timestamp. As a result, the transactions are now more responsible than they were previously. Anyone with access to a blockchain may easily check the integrity of recorded transactions to ensure they haven't been altered or deleted [72].
4	**Trustless Consensus**	Internet of Things (IoT) applications involve potentially unreliable connections and transactions across IoT systems. Conventional designs depend on trustworthy intermediates to establish confidence between parties that aren't trustworthy. Conversely, blockchain-based lot applications are based on distributed consensus, which removes the need for trusted middlemen by reaching agreement among untrusted network nodes.[71].
5	**Privacy**	Blockchain technology offers a promising solution to the problem of privacy by enabling anonymous loT transactions. All nodes in a blockchain network have access to the public key, which allows them to generate pseudo masks. Node identities cannot be inferred from on-chain transactions alone since each transaction is associated with a unique address due to the use of a separate public key for each new transaction. Aside from encryption and delayed transactions, other blockchain-based privacy-preserving mechanisms include access control and transaction mixing.[73].
6	**Contracts That Are Resourceful**	The decentralized ledger known as blockchain allows for the deployment and execution of autonomous contracts. Without the need for intermediaries, smart contracts are performed when specific conditions are satisfied. The rules of an Internet of Things application, its automation of routine tasks, and the smooth exchange of data and other services between loT devices and third parties can all be facilitated by smart contracts.[74].

Blockchain technology allows embedded devices to log data such as status, produced data, location, and temperature. Using permanent blockchain transactions, reliable data can be organized and transferred easily and quickly.

V. Blockchains Era

There has been prior work on the blockchain. Studies examining the interference time stamp ordering process have referred to this idea since the early 1990s[75]. To further secure payment systems, the same idea has been expanded to include transactions and ledgers. Satoshi Nakamoto published a paper on blockchain technology in 2008, claiming credit for its invention[76]. In the time after, a large number of scientists, cryptographers, and software developers worked together to convert the blockchain into a network for digital money known as Bitcoin.

5.1 Social Ramifications of Blockchain and IoT Integration

Many social issues will be affected by blockchain and the Internet of Things. Figure 4 shows a few examples.

5.1.1 Personal Responsibility

Responsibility rests entirely with the individual. Residing in an open-air region no longer allows you to evade duties. Without your private key, you will not be able to access your funds[77].

5.1.2 Spreading the Value of Distribution

No one can break the system. You can't destroy the whole thing by taking it apart piece by piece. Using the network's current value distribution is the only choice. All crucial info is included in the end nodes[78].

5.1.3 Transportation Infrastructure

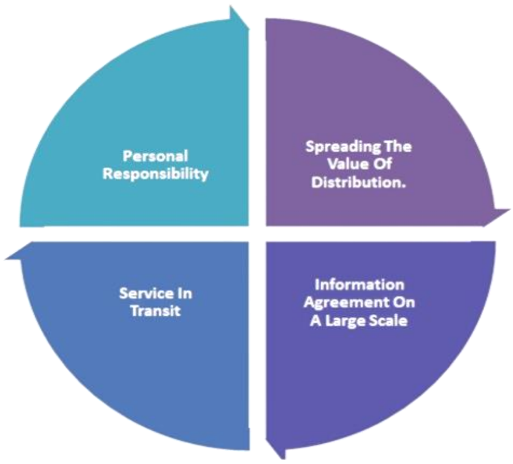

Figure 3: Convergence System of Blockchain and IoT

Some people may choose to focus on transportation services if they want to go off the grid. Never does a single node retain any funds; instead, they are constantly moved. Some data has been moved and altered[79].

5.1.4 Comprehensive Information Agreement

In contrast to the client-server model, data stored in one program could not be identical to or duplicated by data stored in another program[80]. Therefore, a bank consortium necessitates a plethora of intermediaries, each of whom must coordinate an overwhelming array of audits. This problem may be resolved by using the blockchain. For completely automated payment and money transfer systems, blockchain technology eliminates the need for intermediaries due to its decentralized nature[81]. Furthermore, blockchain enables decentralization, whereas IoT permits the connection of all devices. Thus, the two technologies may work together to facilitate information agreement on a wide scale[82].

VI. FUNDAMENTAL HURDLES IN BLOCKCHAIN AND IOT INTEGRATION

Figure 5 shows the challenges that users face when attempting to use the blockchain with IoT.

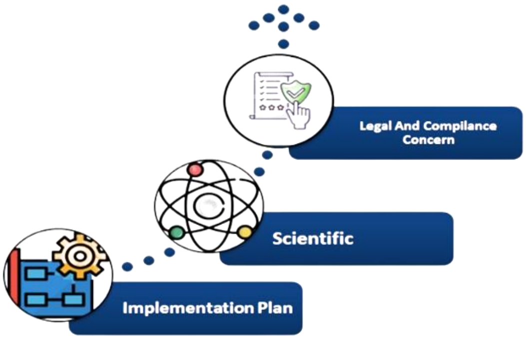

Figure 4: Primary Obstacles in the Utilization of Blockchain and IoT

6.1 Execution Strategy

Connecting previously incompatible systems and devices is becoming easier with the help of blockchain and the Internet of Things[83]. On the other hand, compatibility problems might arise when devices connect. To make sure these technologies work efficiently, we need a single platform for all of them and some built-in tech[82].

6.2 Scientific

Two of the biggest technical hurdles for blockchain and IoT are storage needs, security, and scalability[84]. A lot of research has already been done on security. With that in mind, we zero in on the scalability issue, namely the blockchain's limited transaction handling capabilities[85]. On a microsecond scale, the financial sector handles thousands of transactions. As a result, there are limitations on blockchain security, high availability, and disk size. The researchers are still working on these issues, but they are making headway[86].

Table 6: Block Benefits

There is no doubt that blockchain technology offers the following benefits due to its design and functionality.		
1	**Delegation**	The primary and most essential virtue of blockchain is that it runs on a distributed network, with the ledger copied across all nodes. As a result, all of blockchains additional benefits are primarily due to its decentralized character[36].
2	**Integrity**	Transparency is inherent in blockchain transactions due to the fact that they are recorded and time-stamped in a decentralized ledger. The use of Markel Tree further simplified the process of verifying transactions in blockchain technology. Being able to authoritatively and correctly trace the ledger back to its source is another critical component of transparency [87].
3	**Access Control**	Distributed ledger technology has eliminated SPF as a concern. In addition, PoW and the longest chain rule are consensus mechanisms that safeguard the blockchain network from DDoS attacks by capturing at least 51% of the nodes [88].
4	**Security and Privacy**	An edit to a single transaction in the chain renders all hashes of blocks issued after that particular block invalid, as mathematical hashing links all time-stamped records of transactions[89]. Conversely, proof-of-work and complete immutability of the chain are achieved by duplicating it across all nodes in the network. The ledger is very immutable due to its append-only nature, which prevents the removal or modification of existing information
5	**Charge**	In comparison to more conventional technologies, blockchain may be less expensive and easier to maintain when deployed for large-scale applications, making it a more practical and economical choice over time. Using blockchain for a private, small-scale application could be expensive because it depends on a distributed network to run. Offshoring is possible with many of the Blockchain as a Service (BaaS) offerings from third-party platforms, such as Ethereum, Hyperledger, and many more [90].
There is no doubt that blockchain technology offers the following benefits due to its design and functionality.		
1	**Delegation**	The primary and most essential virtue of blockchain is that it runs on a distributed network, with the ledger copied across all nodes. As a result, all of blockchains additional benefits are primarily due to its decentralized character[36].
2	**Integrity**	Transparency is inherent in blockchain transactions due to the fact that they are recorded and time-stamped in a decentralized ledger. The use of Markel Tree further simplified the process of verifying transactions in blockchain technology. Being able to authoritatively and correctly trace the ledger back to its source is another critical component of transparency [87].
3	**Access Control**	Distributed ledger technology has eliminated SPF as a concern. In addition, PoW and the longest chain rule are consensus mechanisms that safeguard the blockchain network from DDoS attacks by capturing at least 51% of the nodes [88].
4	**Security and Privacy**	An edit to a single transaction in the chain renders all hashes of blocks issued after that particular block invalid, as mathematical hashing links all time-stamped records of transactions[89]. Conversely, proof-of-work and complete immutability of the chain are achieved by duplicating it across all nodes in the network. The ledger is very immutable due to its append-only nature, which prevents the removal or modification of existing information
5	**Charge**	In comparison to more conventional technologies, blockchain may be less expensive and easier to maintain when deployed for large-scale applications, making it a more practical and economical choice over time. Using blockchain for a private, small-scale application could be expensive because it depends on a distributed network to run. Offshoring is possible with many of the Blockchain as a Service (BaaS) offerings from third-party platforms, such as Ethereum, Hyperledger, and many more [90].

ISSN:1813-1786 (Print) 2313-7770 (Online)

6.3 Legal and Compliance Concerns

It is advantageous to incorporate modern technologies. However, the Internet can't make enough connections to the actual world to support the idea of the Internet of Things[91]. Not only will physical items be a part of an IoT, but so will human actions and lives. Quality control and responsibility are two important ethical considerations[92]. Last but not least, it's becoming harder to find solutions to the question of what occurs when someone defies a law. Making a central database is another challenge. The topic of what will be the identification requirements often arises, for example, when lawyers consider ways to safeguard personal data. The best way to evaluate certain factors from an ethical and legal standpoint is a matter of concern. It is a question of law and ethics, say Somov and Giaffreda[93], to know how to set up, keep tabs on, and oversee "anything" inside a framework.

VII. Blockchain

7.1. Blockchain Essentials

Cryptocurrencies like Bitcoin rely on the blockchain, a decentralized database. Improving the speed and efficiency of order transmission, receipt, and tracking via the use of secure data is the main objective. In Figure 6, we can see the blockchain in action.

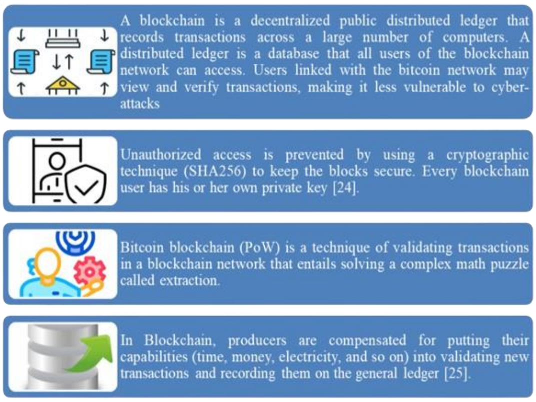

Figure 5. Blockchain Essentials

VIII. Literature Survey

A study conducted by [94] investigated the relationship between blockchain technology and the Internet of Things. Cloud computing, intelligent comparisons, encryption methods, password security, and other significant blockchain aspects were investigated to determine their potential usefulness in the context of the Internet of Things (IoT)[95]. So, we were able to collect first-hand information. Based on our findings, blockchain technology offers a promising and generally recognized foundation for the expansion of the IIoT and the Internet of Things (IoT), but it also poses several problems that need fixing[96].

The most effective decentralized and distributed method, according to [97], who investigated the security of the Internet of Things, is the blockchain, which is a distributed ledger composed of linked blocks. For billions of Internet of Things devices, the blockchain can record and oversee transactions and store data. The system makes use of motion time stamping, data encryption, distributed consensus, and financial incentives. Aside from solving the issue of unprotected data storage in centralized businesses, it may also increase productivity while decreasing costs[98].

To modernize traditional centralized designs, proposed a consensus-based approach. Initially, they referred to the system as a blockchain, a portmanteau of the words "block" and "chain." In 2016, the merging of these two ideas led to the birth of cryptocurrency.

Using a guide, [99] investigated blockchain and IoT technology. The fundamental framework of the IoT built on blockchain was first described. The advantages and disadvantages of blockchain technology were also considered. Finding the commonalities in the IoT system's design and key components was the next stage in our investigation. We also looked at the various benefits and drawbacks of the IoT system.

For example, [100]have shown that blockchain stability is maintained even when IoT device networks undergo upgrades, highlighting the immutability of the blockchain. A legitimate block added to the blockchain during a software update cannot be erased by the attacker[101]. You may also avoid new software problems by not installing risks. Once an Internet of Things (IoT) device consensus mechanism has been established, the changes may be validated using the blockchain application. Furthermore, as the network becomes larger, the Internet of Things (IoT) blockchain that is used to improve the security of IoT devices becomes more effective[39, 102]. Several devices may have longer lifespans if they would only download trusted and authorized updates, which would save resource waste.

An Internet of Things (IoT) optimized lightweight blockchain was shown to be important [103]. The high-level mathematics, complexities, and latency of blockchain networks are often cited as reasons why they are unsuitable for the Internet of Things (IoT). A lightweight blockchain tailored to the IoT intended to be developed to remove the needless complexity and security concerns linked to conventional blockchains[104-105]. A centrally controlled node and blockchain technology are two components of the planned Internet of Things architecture that would work together to improve energy efficiency. Instead of using sensor nodes, central nodes with enough processing power and storage capacity build overlay networks. To provide end-to-end confidentiality and anonymity, these networks use the public blockchain[106]. In addition, they suggested a layout that, with the use of distributed trusts, might reduce the processing time required for block verification. The proposed layout was tested in a smart home to see how well it worked. The proposed system was unsafe due to its reliance on a single node for data integration; nevertheless, it used a blockchain to circumvent the storage and processing limits of the IoT device[107]. The assessment was carried out while considering the battery problems of the sensor equipment.

Lightweight blockchains were suggested by [108] as a foundation for Internet of Things (IoT) services that would make use of cloud and fog computing. Constraints on processing power, data transfer rates, and battery life are some of the issues that can arise from implementing a blockchain on an IoT network[97, 109]. Although both cloud and fog computing may host blockchain technology, the two have polar opposite processing power and latency profiles[110-111]. Low latency is achieved via fog computing despite its restricted resources. At the same time, resource restrictions linked to latency may be scaled by using cloud computing. Even low-powered Internet of Things devices may reap the benefits of blockchain when coupled with the aforementioned platform, cloud computing.

IX. RESULTS

The total number of Internet of Things (IoT) devices outpaced the human population in 2008. Constant innovation in IoT applications and services is a direct result of the system's many advantages. If predictions made by [112] are to be believed, the number of Internet of Things (IoT) devices will surpass 31 billion by 2020 and reach approximately 75 billion by 2025.

According to, the amount spent on blockchain solutions worldwide will rise from $4.5 billion in 2017 to $6.6 billion in 2021. Predictions for the future show that digital identity security and Web 3.0 will drive significant demand for blockchain technology. Spending on blockchain is expected to exceed $19 billion by 2024, thanks to the growing number of businesses using the technology for identity security and data authentication and access. On top of that, the Internet of Things industry is growing at an exponential pace. According to Statista, the income from the Internet of Things reached $743 billion in 2015. At the year's conclusion, this figure had increased significantly to USD 1710 billion. The predicted yearly growth rate for blockchain technology is 85.9% from 2022 to 2030. Moreover, as per Grandview and Triple-A

According to studies, over 300 million individuals will have some kind of cryptocurrency holding or using it in 2021.

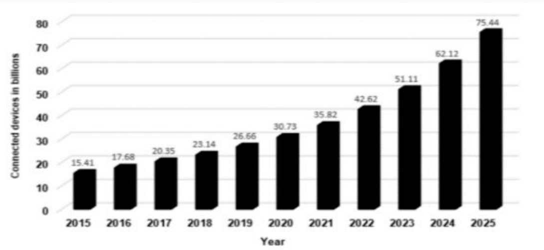

Figure 6: IoT Expansion Forecasts: 2015-2025.

The blockchain industry is much bigger than most experts had thought, according to Grandview Research. Contactless blockchain event tickets and the extensive digitization of the BPFSI sector are two more potential drivers of blockchain market development. According to Grandview Research, industry-specific trade estimates are projected to reach $1,431.54 billion between 2022 and 2030, representing an annual growth rate of 85.9 percent[113].

X. CURRENT SCENARIO AND FUTURE PERSPECTIVE

New and strong, blockchain technology is on the rise. The decentralization, auditability, and high security of blockchain-based systems are unparalleled. Despite these benefits, there are several obstacles to blockchain technology's widespread use in IIOT systems. Here, under the framework of blockchain integration with IIoT networks, we will go over these obstacles and some potential avenues for further study.

Nodes in both public and private networks must actively participate in consensus procedures to maintain a complete record of all network transactions.

When it comes to scalability, it sacrifices security for decentralization and fault tolerance. When the number of records in a conventional database increases, the only thing that needs to be done is to expand storage space. In contrast, blockchain-based systems need greater processing capacity to expedite the transactions [114].

Blockchain scaling's high performance and networking overheads provide a significant challenge to the adoption of digital banking and IIoT applications. One possible avenue for further investigation into blockchain scalability is vertical scaling, while the most attractive answer is horizontal scaling. Therefore, further study on inter-blockchain communication that is semantically independent might be in order.

Also created were the responsibilities of nodes in blockchain networks[115]. Furthermore, there is no need for IoT devices to keep a complete record of blockchain transactions, hence they serve a limited purpose. The solutions that are generated from this work better when applied to private blockchains. In the meanwhile, one option for public blockchains is to use the IoT gateway to put transactions onto the blockchain. Internet of Things (IoT) gateways with sufficient processing power to engage in public blockchain activities will be necessary in this setting. An additional avenue for future study might be to bring blockchain technology to the periphery of the Internet of Things. When it comes to resource-constrained Internet of Things devices, the blockchain's high speed and networking overhead make it unsuitable. To get over this problem, Internet of Things gateways may utilize lightweight clients to send transactions across the blockchain network.

Furthermore, a new chance to lessen the impact of blockchain's flaws has emerged with the rise of edge computing in IIoT environments. Edge computing improves scalability and speed by processing data closer to the source of data generation, which reduces network load and latency issues related to blockchain transactions. Together, blockchain and edge computing could revolutionize the processing of IIoT data, enhancing the safety, efficiency, and security of dispersed networks for all transactions.

One of the most important factors in the development of blockchain applications in IIoT is artificial intelligence (AI). We can automate smart contracts, optimise consensus methods, and boost security protocols by merging AI algorithms with blockchain. By spotting any security flaws in IIoT systems before they are attacked, AI's predictive analytics skills can help with proactive maintenance even more. An age of intelligent, autonomous IIoT systems that can self-regulate, self-optimize, and self-heal is dawning with the combination of AI and blockchain.

Integrating blockchain technology with the Industrial Internet of Things (IIoT) is also the target of increasing regulatory and standardization initiatives. To address concerns about privacy, security, interoperability, and ethics, lawmakers and business groups are collaborating to create worldwide standards and frameworks. If we want to build confidence, encourage technology adoption, and make sure blockchain and IIoT can live peacefully together across different industries, we need these legal developments.

As a result of not offering completely decentralized systems, private blockchains have a very high transaction rate. To provide Byzantine fault tolerance, private blockchain consensus algorithms use a voting system. For public blockchain networks, this method does not function. Everyone uses the public blockchain equally and there is no central authority, according to its guiding principle. As a result of the usage of a consensus process based on a lottery to establish a safe and permission-less transaction platform, the public blockchain has been delayed. Consequently, blockchain consensus algorithms lead to a compromise between decentralization and fast transactions. Applications outside of cryptocurrency should provide many use cases while also protecting user privacy. Applications like IIoT need the usage of several blockchains due to the distributed nature of blockchain technology and the fact that it spans regions and use cases. Successful interoperability across blockchains allows them to provide a wide range of Internet of Things (IoT) services.

Finally, new blockchain designs and consensus methods are being investigated, which would be a good way to get around the problems that are already there. Sharing, layer-2 scaling solutions, and hybrid blockchain models are some of the innovations that could help strike that balance between decentralization, security, and scalability. In addition, for different blockchain platforms and IIoT ecosystems to communicate and exchange data seamlessly, cross-chain technologies and blockchain interoperability protocols must be developed.

XI. Conclusion

Blockchain technology has the opportunity to significantly improve IIoT frameworks in terms of decentralization, auditability, and security; this study investigates its integration with IIoT. Despite the potential benefits of blockchain technology and the Industrial Internet of Things (IIoT), our research has shown important obstacles to their full integration, such as limited scalability, high networking overheads, and complicated consensus processes. The article explores possible answers to these problems, such as using Internet of Things (IoT) gateways for blockchain transactions, adopting horizontal and vertical scaling methods, and distinguishing between public and private blockchain applications. We cannot overstate the importance of conducting cutting-edge research on blockchain scalability, interoperability, and IIoT-specific applications. The investigation highlights the fact that overcoming these operational and technological challenges is crucial to the future of blockchain in the IIoT. To tackle the intricacies of blockchain technology and fully tap into its revolutionary potential in IIoT ecosystems, ongoing critical analysis and study are crucial moving forward. In order to overcome these obstacles and investigate the many ways in which blockchain technology can transform IIoT, the paper suggests a complicated but potentially fruitful way to use blockchain to build IIoT systems that are more secure, efficient, and dependable.

References

[1] Saraji, S., *Introduction to Blockchain*, in *Sustainable Oil and Gas Using Blockchain*. 2023, Springer. p. 57-74.

[2] Bellini, P., P. Nesi, and G. Pantaleo, *IoT-enabled smart cities: A review of concepts, frameworks and key technologies.* Applied Sciences, 2022. 12(3): p. 1607.

[3] Kopetz, H. and W. Steiner, *Internet of things*, in *Real-time systems: design principles for distributed embedded applications*. 2022, Springer. p. 325-341.

[4] Javaid, M., et al., *Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT).* Sensors International, 2021. 2: p. 100129.

[5] Lombardi, M., F. Pascale, and D. Santaniello, *Internet of things: A general overview between architectures, protocols and applications.* Information, 2021. 12(2): p. 87.

[6] Mouha, R.A., *Internet of things (IoT).* Journal of Data Analysis and Information Processing, 2021. 9(2): p. 77-101.

[7] Laghari, A.A., et al., *A review and state of art of Internet of Things (IoT).* Archives of Computational Methods in Engineering, 2021: p. 1-19.

[8] Mozumder, M.A.I., et al., *Metaverse for digital anti-aging healthcare: an overview of potential use cases based on artificial intelligence, blockchain, IoT technologies, its challenges, and future directions.* Applied Sciences, 2023. 13(8): p. 5127.

[9] Uma, S., *Blockchain and AI: disruptive digital technologies in designing the potential growth of healthcare industries*, in *AI and Blockchain in Healthcare*. 2023, Springer. p. 137-150.

[10] Akkaoui, R., et al., *A Taxonomy and Lessons Learned From Blockchain Adoption Within the Internet of Energy Paradigm.* IEEE Access, 2022. 10: p. 106708-106739.

[11] Paul, A.K., X. Qu, and Z. Wen, *Blockchain–a promising solution to internet of things: A comprehensive analysis, opportunities, challenges and future research issues.* Peer-to-Peer Networking and Applications, 2021. 14(5): p. 2926-2951.

[12] Gad, A.G., et al., *Emerging trends in blockchain technology and applications: A review and outlook.* Journal of King Saud University-Computer and Information Sciences, 2022. 34(9): p. 6719-6742.

[13] Khan, M., et al., *Integration of internet-of-things with blockchain technology to enhance humanitarian logistics performance.* IEEE Access, 2021. 9: p. 25422-25436.

[14] Torky, M. and A.E. Hassanein, *Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges.* Computers and Electronics in Agriculture, 2020. 178: p. 105476.

[15] Omolara, A.E., et al., *The internet of things security: A survey encompassing unexplored areas and new insights.* Computers & Security, 2022. 112: p. 102494.

[16] Baiyere, A., et al., *The internet of things (IoT): A research agenda for information systems.* Communications of the Association for Information Systems, 2020. 47.

[17] Broad, G.M., W. Marschall, and M. Ezzeddine, *Perceptions of high-tech controlled environment agriculture among local food consumers: using interviews to explore sense-making and connections to good food.* Agriculture and Human Values, 2022. 39(1): p. 417-433.

[18] Khan, Y., et al., *Application of Internet of Things (IoT) in sustainable supply chain management.* Sustainability, 2022. 15(1): p. 694.

[19] Andås, H.E., *Emerging technology trends for defence and security.* 2020.

[20] Syed, A.S., et al., *IoT in smart cities: A survey of technologies, practices and challenges.* Smart Cities, 2021. 4(2): p. 429-475.

[21] Ahmad, T. and D. Zhang, *Using the internet of things in smart energy systems and networks.* Sustainable Cities and Society, 2021. 68: p. 102783.

[22] Kanellopoulos, D., et al., *Networking architectures and protocols for IoT applications in smart cities: Recent developments and perspectives.* Electronics, 2023. 12(11): p. 2490.

[23] Ogonji, M.M., G. Okeyo, and J.M. Wafula, *A survey on privacy and security of Internet of Things.* Computer Science Review, 2020. 38: p. 100312.

[24] Park, A. and H. Li, *The effect of blockchain technology on supply chain sustainability performances.* Sustainability, 2021. 13(4): p. 1726.

[25] Kumar, R., et al., *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*. 2024: CRC Press.

[26] Al Sadawi, A., M.S. Hassan, and M. Ndiaye, *On the integration of blockchain with IoT and the role of oracle in the combined system: The full picture.* IEEE Access, 2022. 10: p. 92532-92558.

[27] Musaddiq, A., T. Olsson, and F. Ahlgren, *Reinforcement-Learning-Based Routing and Resource Management for Internet of Things Environments: Theoretical Perspective and Challenges.* Sensors, 2023. 23(19): p. 8263.

[28] Birkel, H.S. and E. Hartmann, *Impact of IoT challenges and risks for SCM.* Supply Chain Management: An International Journal, 2019. 24(1): p. 39-61.

[29] Maheepala, M., M.A. Joordens, and A.Z. Kouzani, *Low power processors and image*

sensors for vision-based iot devices: a review. IEEE Sensors Journal, 2020. 21(2): p. 1172-1186.

[30] HaddadPajouh, H., et al., *A survey on internet of things security: Requirements, challenges, and solutions.* Internet of Things, 2021. 14: p. 100129.

[31] Babun, L., et al., *A survey on IoT platforms: Communication, security, and privacy perspectives.* Computer Networks, 2021. 192: p. 108040.

[32] Buckwald, J.M. and G.E. Marchant, *Improving Soft Law Governance of the Internet of Things.* IEEE Technology and Society Magazine, 2021. 40(4): p. 101-114.

[33] Alwarafy, A., et al., *A survey on security and privacy issues in edge-computing-assisted internet of things.* IEEE Internet of Things Journal, 2020. 8(6): p. 4004-4022.

[34] Gadekallu, T.R., et al., *Blockchain for edge of things: Applications, opportunities, and challenges.* IEEE Internet of Things Journal, 2021. 9(2): p. 964-988.

[35] Javed, A.R., et al., *Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects.* Cities, 2022. 129: p. 103794.

[36] Bhushan, B., et al., *Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions.* Wireless Networks, 2021. 27: p. 55-90.

[37] Kamran, M., et al., *Blockchain and Internet of Things: A bibliometric study.* Computers & Electrical Engineering, 2020. 81: p. 106525.

[38] König, L., et al., *The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks.* J. Internet Serv. Inf. Secur., 2020. 10(3): p. 110-127.

[39] Sodhro, A.H., et al., *Towards blockchain-enabled security technique for industrial internet of things based decentralized applications.* Journal of Grid Computing, 2020. 18(4): p. 615-628.

[40] Auhl, Z., et al., *A Comparative study of consensus mechanisms in blockchain for IoT networks.* Electronics, 2022. 11(17): p. 2694.

[41] Swamy, S.N. and S.R. Kota, *An empirical study on system level aspects of Internet of Things (IoT).* IEEE Access, 2020. 8: p. 188082-188134.

[42] Yu, Y., et al., *LayerChain: A hierarchical edge-cloud blockchain for large-scale low-delay Industrial Internet of Things applications.* IEEE Transactions on Industrial Informatics, 2020. 17(7): p. 5077-5086.

[43] Javaid, U. and B. Sikdar, *A checkpoint enabled scalable blockchain architecture for industrial internet of things.* IEEE Transactions on Industrial Informatics, 2020. 17(11): p. 7679-7687.

[44] Badari, A. and A. Chaudhury, *An overview of bitcoin and ethereum white-papers, forks, and prices.* Forks, and Prices (April 26, 2021), 2021.

[45] Salimitari, M., M. Chatterjee, and Y.P. Fallah, *A survey on consensus methods in blockchain for resource-constrained IoT networks.* Internet of Things, 2020. 11: p. 100212.

[46] Abdelmaboud, A., et al., *Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions.* Electronics, 2022. 11(4): p. 630.

[47] Tran-Dang, H., et al., *Toward the internet of things for physical internet: Perspectives and challenges.* IEEE internet of things journal, 2020. 7(6): p. 4711-4736.

[48] Bamakan, S.M.H., A. Motavali, and A.B. Bondarti, *A survey of blockchain consensus algorithms performance evaluation criteria.* Expert Systems with Applications, 2020. 154: p. 113385.

[49] Brotsis, S., et al., *On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance.* Computer Networks, 2021. 191: p. 108005.

[50] Ahmad, N., *Internet of Things: Tapping into security and privacy issues associated with the internet of things*. 2021.

[51] Lin, Q., et al., *Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking.* Information Sciences, 2024. 654: p. 119783.

[52] Romano, D. and G. Schmid, *Beyond bitcoin: recent trends and perspectives in distributed ledger technology.* Cryptography, 2021. 5(4): p. 36.

[53] Sethi, P., *Reinforcement Learning assisted Adaptive difficulty of Proof of Work (PoW) in Blockchain-enabled Federated Learning*. 2023, Virginia Tech.

[54] Navaroj, G.I., E.G. Julie, and Y.H. Robinson, *Adaptive practical Byzantine fault tolerance consensus algorithm in permission blockchain network.* International Journal of Web and Grid Services, 2022. 18(1): p. 62-82.

[55] Nassereddine, M. and A. Khang, *Applications of Internet of Things (IoT) in smart cities*, in *Advanced IoT technologies and applications in the industry 4.0 digital economy*. 2024, CRC Press. p. 109-136.

[56] Strathausen, R. and I. Nikkels, *Contract Is Code! How Smart Contracting Automates the CLM Process.* Liquid Legal: Towards a Common Legal Platform, 2020: p. 371-391.

[57] Dahiya, A., et al., *A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media*. International Journal of Intelligent Systems, 2022. 37(12): p. 11037-11077.

[58] Adow, A.H., et al., *Analysis of agriculture and food supply chain through blockchain and IoT with light weight cluster head.* Computational intelligence and neuroscience, 2022. 2022.

[59] Lashkari, B. and P. Musilek, *A comprehensive review of blockchain consensus mechanisms.* IEEE access, 2021. 9: p. 43620-43652.

[60] Alshaikhli, M., et al., *Evolution of Internet of Things from blockchain to IOTA: A survey.* IEEE Access, 2021. 10: p. 844-866.

[61] Honkamäki, S., *Evaluating Ethereum development environments*. 2022, S. Honkamäki.

[62] Kumar, S., P. Tiwari, and M. Zymbler, *Internet of Things is a revolutionary approach for future technology enhancement: a review.* Journal of Big data, 2019. 6(1): p. 1-21.

[63] Aceto, G., V. Persico, and A. Pescapé, *Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0.* Journal of Industrial Information Integration, 2020. 18: p. 100129.

[64] Guggenberger, T., et al., *An in-depth investigation of the performance characteristics of Hyperledger Fabric.* Computers & Industrial Engineering, 2022. 173: p. 108716.

[65] Bello, O., H. Al-Aqrabi, and R. Hill, *Establishing trustworthy relationships in multiparty industrial internet of things applications*, in *Digital Forensic Investigation of Internet of Things (IoT) Devices*. 2020, Springer. p. 205-221.

[66] Fan, C., et al., *Performance analysis of the IOTA DAG-based distributed ledger.* ACM Transactions on Modeling and Performance Evaluation of Computing Systems, 2021. 6(3): p. 1-20.

[67] Silvano, W.F. and R. Marcelino, *Iota Tangle: A cryptocurrency to communicate Internet-of-Things data.* Future generation computer systems, 2020. 112: p. 307-319.

[68] Akhtar, M.M., et al., *Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy.* Sensors, 2021. 21(13): p. 4354.

[69] STEINER, B. and V. NEIDLINGER, *Impact of the Distributed Ledger Technology (DLT) IOTA on Smart Cities*. 2021.

[70] Pal, S., et al., *Security requirements for the internet of things: A systematic approach.* Sensors, 2020. 20(20): p. 5897.

[71] Reyna, A., et al., *On blockchain and its integration with IoT. Challenges and opportunities.* Future generation computer systems, 2018. 88: p. 173-190.

[72] Helliar, C.V., et al., *Permissionless and permissioned blockchain diffusion.* International Journal of Information Management, 2020. 54: p. 102136.

[73] Bernabe, J.B., et al., *Privacy-preserving solutions for blockchain: Review and challenges.* IEEE Access, 2019. 7: p. 164908-164940.

[74] Sadeeq, M.M., et al., *IoT and Cloud computing issues, challenges and opportunities: A review.* Qubahan Academic Journal, 2021. 1(2): p. 1-7.

[75] Treiblmaier, H., et al., *What's Next in Blockchain Research? -An Identification of Key Topics Using a Multidisciplinary Perspective.* ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2021. 52(1): p. 27-52.

[76] Cai, L., Q. Li, and X. Liang, *Introduction to blockchain basics*, in *Advanced Blockchain Technology: Frameworks and Enterprise-Level Practices*. 2022, Springer. p. 3-43.

[77] Euchi, J., *Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems?* 2021, Elsevier. p. 182-190.

[78] Mishra, N., S.H. Islam, and S. Zeadally, *A survey on security and cryptographic perspective of Industrial-Internet-of-Things.* Internet of Things, 2023: p. 101037.

[79] Richter, M.A., et al., *Smart cities, urban mobility and autonomous vehicles: How different cities needs different sustainable investment strategies.* Technological Forecasting and Social Change, 2022. 184: p. 121857.

[80] Javadpour, A., et al., *Improving load balancing for data-duplication in big data cloud computing networks.* Cluster Computing, 2022. 25(4): p. 2613-2631.

[81] Tseng, C.-T. and S.S. Shang, *Exploring the sustainability of the intermediary role in blockchain.* Sustainability, 2021. 13(4): p. 1936.

[82] Al Sadawi, A., M.S. Hassan, and M. Ndiaye, *A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges.* IEEE Access, 2021. 9: p. 54478-54497.

[83] Zafar, S., et al., *Integration of blockchain and Internet of Things: Challenges and solutions.* Annals of Telecommunications, 2022: p. 1-20.

[84] Moin, S., et al., *Securing IoTs in distributed blockchain: Analysis, requirements and open issues.* Future Generation Computer Systems, 2019. 100: p. 325-343.

[85] Politou, E., et al., *Blockchain mutability: Challenges and proposed solutions.* IEEE Transactions on Emerging Topics in Computing, 2019. 9(4): p. 1972-1986.

[86] Sanka, A.I. and R.C. Cheung, *A systematic review of blockchain scalability: Issues, solutions, analysis and future research.* Journal of Network and Computer Applications, 2021. 195: p. 103232.

[87] Shrimali, B. and H.B. Patel, *Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities.* Journal of King Saud University-Computer and Information Sciences, 2022. 34(9): p. 6793-6807.

[88] Miraz, M.H., *Blockchain of things (BCoT): The fusion of blockchain and IoT technologies*. 2020: Springer.

[89] Singh, P. and S. Mishra, *A comprehensive study of security aspects in blockchain*, in *Predictive data security using AI: insights and issues of blockchain, IoT, and DevOps*. 2022, Springer. p. 1-24.

[90] Kernahan, A., U. Bernskov, and R. Beck. *Blockchain out of the Box–Where is the Blockchain in Blockchain-as-a-Service?* in *Proceedings of the Annual Hawaii International Conference on System Sciences*. 2021. IEEE Computer Society Press.

[91] Munirathinam, S., *Industry 4.0: Industrial internet of things (IIOT)*, in *Advances in computers*. 2020, Elsevier. p. 129-164.

[92] Ahmad, K., et al., *Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges.* Computer Science Review, 2022. 43: p. 100452.

[93] Kasrin, N., et al., *Data-sharing markets for integrating IoT data processing functionalities.* CCF Transactions on Pervasive Computing and Interaction, 2021. 3: p. 76-93.

[94] Novo, O., *Blockchain meets IoT: An architecture for scalable access management in IoT.* IEEE internet of things journal, 2018. 5(2): p. 1184-1195.

[95] Dang, L.M., et al., *A survey on internet of things and cloud computing for healthcare.* Electronics, 2019. 8(7): p. 768.

[96] Wu, Y., H.-N. Dai, and H. Wang, *Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0.* IEEE Internet of Things Journal, 2020. 8(4): p. 2300-2317.

[97] Fernández-Caramés, T.M. and P. Fraga-Lamas, *A Review on the Use of Blockchain for the Internet of Things.* Ieee Access, 2018. 6: p. 32979-33001.

[98] Laroiya, C., D. Saxena, and C. Komalavalli, *Applications of blockchain technology*, in *Handbook of research on blockchain technology*. 2020, Elsevier. p. 213-243.

[99] Atlam, H.F. and G.B. Wills, *Technical aspects of blockchain and IoT*, in *Advances in computers*. 2019, Elsevier. p. 1-39.

[100] Boudguiga, A., et al. *Towards better availability and accountability for iot updates by means of a blockchain*. in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2017. IEEE.

[101] Halgamuge, M.N., *Estimation of the success probability of a malicious attacker on blockchain-based edge network.* Computer Networks, 2022. 219: p. 109402.

[102] Zafar, S., et al., *Integration of blockchain and Internet of Things: Challenges and solutions.* Annals of Telecommunications, 2022. 77(1): p. 13-32.

[103] Dorri, A., S.S. Kanhere, and R. Jurdak. *Towards an optimized blockchain for IoT*. in *Proceedings of the second international conference on Internet-of-Things design and implementation*. 2017.

[104] Tran, N.K., M.A. Babar, and J. Boan, *Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs.* Journal of Network and Computer Applications, 2021. 173: p. 102844.

[105] Uddin, M.A., et al., *A survey on the adoption of blockchain in iot: Challenges and solutions.* Blockchain: Research and Applications, 2021. 2(2): p. 100006.

[106] Chaieb, M. and S. Yousfi. *Loki vote: A blockchain-based coercion resistant e-voting protocol*. in *Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, November 25–26, 2020, Proceedings 17*. 2020. Springer.

[107] Li, C., et al., *Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices.* Information Processing & Management, 2021. 58(4): p. 102602.

[108] Samaniego, M., U. Jamsrandorj, and R. Deters. *Blockchain as a Service for IoT*. in *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. 2016. IEEE.

[109] Zhou, J., G. Feng, and Y. Wang, *Optimal deployment mechanism of blockchain in resource-constrained IoT systems.* IEEE Internet of Things Journal, 2021. 9(11): p. 8168-8177.

[110] Tariq, N., et al., *The security of big data in fog-enabled IoT applications including blockchain: A survey.* Sensors, 2019. 19(8): p. 1788.

[111] Meshcheryakov, Y., et al., *On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices.* IEEE Access, 2021. 9: p. 80559-80570.

[112] Chui, M., M. Collins, and M. Patel, *The Internet of Things: Catching up to an accelerating opportunity.* 2021.

[113] Atlam, H.F., et al., *A Review of Blockchain in Internet of Things and AI.* Big Data and Cognitive Computing, 2020. 4(4): p. 28.

[114] Latif, S., et al., *Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions.* Transactions on Emerging Telecommunications Technologies, 2021. 32(11): p. e4337.

[115] Michalski, R., D. Dziubałtowska, and P. Macek, *Revealing the character of nodes in a blockchain with supervised learning.* Ieee Access, 2020. **8**: p. 109639-109647.