ISSN: 2723-9535

Available online at www.HighTechJournal.org

HighTech and Innovation Journal

Vol. 4, No. 1, March, 2023

Development, Service-Oriented Architecture, and Security of Blockchain Technology for Industry 4.0 IoT Application

Satyanand Singh [1*], Joanna Rosak-Szyrocka [2], László Tamàndl [3]

[1] School of Electrical & Electronics Engineering, Fiji National University, Fiji Island.

[2] Department of Production Engineering and Safety Faculty of Management, Czestochowa University of Technology, Poland.

[3] Faculty of Economics, Széchenyi Istvàn University, Egyetem ter. 1, 9026 Győr, Hungary.

Received 23 December 2022; Revised 16 February 2023; Accepted 21 February 2023; Published 01 March 2023

Abstract

The Internet of Things (IoT) paradigm is laying the groundwork for a world in which many of our everyday devices will be connected and will interact with their surroundings to gather data and automate some operations. Among other things, such a concept necessitates seamless authentication, data privacy, security, attack resilience, simplicity of deployment, and self-maintenance. Blockchain, a technology created with the Bitcoin cryptocurrency, can provide such advantages. To create blockchain-based IoT (BIoT) applications, a full discussion of how to modify blockchain to meet the unique requirements of IoT is offered in this paper. The most important BIoT applications are detailed after a brief introduction to blockchain, with the goal of highlighting how blockchain can affect conventional cloud-based IoT applications. Then, several factors that have an impact on the design, development, and deployment of a BIoT application are covered, along with present obstacles and potential improvements. Lastly, a list of recommendations is provided to help future BIoT researchers and developers understand some of the problems that need to be solved before deploying the upcoming generation of BIoT applications.

Keywords: IoT; Blockchain; Traceability; Consensus; Distributed Systems; BIoT; Fog Computing; Edge Computing.

1. Introduction

Understanding blockchain and its value is essential in the current environment for the successful adoption of Industry 4.0. Blockchain technology has potential applications in some industries, such as financial transactions, where it might give confidence. Problems with fiat currencies and foreign currencies are not present, and a controlled supply transaction is possible. Industry 4.0's Blockchain technology can also be connected to the product itself and the identifying components of its assembly. It serves as a reminder of situations in which being able to identify products with problems may be advantageous. Here, blockchain will safeguard every component of a product, including its sub-assemblies, parts, and distribution channels. Retrieval at any point in the supply chain is less expensive and disruptive. By using cameras and sensors, new information has been acquired that might be used to build the blockchain's network. We have access to more information thanks to it than we could ever learn in a short period of time [1].

There must also be a matching structural change within an organization to sustain end-user support. One of the most important technological developments nowadays is blockchain [2]. This technology has significantly advanced in recent years and has a wide range of manufacturing applications [3]. It is frequently used in conjunction with phrases like

* Corresponding author: satyanand.singh@fnu.ac.fj

http://dx.doi.org/10.28991/HIJ-2023-04-01-010

Industry 4.0 and intelligent factories. Blockchain is a decentralized, encrypted, distributed ledger for filing computers that enables the creation of temper-proof, real-time logs.

Several aspects of Industry 4.0 are still poorly understood and explained. The future effects of intelligent manufacturing solutions will be increased thanks to this new technology. Much has been learned from both the current deployments and the early sales experiences. It offers a comprehensive distribution strategy, applying and combining these new technologies that are supported and encouraged as resources to achieve more general corporate objectives. Since blockchain may make the patent environment more simple, transparent, and less intermediate, it could aid SMEs (small and medium enterprises) in defending their discoveries. This would promote rivalry among businesses that find it more challenging to enter the patent world. Individuals will be able to produce green energy through a freely negotiated agreement [4, 5].

This technology is special because it avoids middlemen in transactions, potentially resulting in an efficient and affordable flow of products and services. Since this record is linked to the preceding block, it cannot be modified or changed in the future. The term "non-authorized" refers to a decentralized forum that is public and participatory and where anybody can read and submit transactions. In contrast, blockchain is designed with the benefit of reading from and writing to a closed network for specific users. Between a private and a public blockchain, this is the key distinction in how users are positioned and given incentives to engage with the system. The supply chain is a flexible framework made up of numerous companies that collaborate to meet customer demands by bringing value at every stage of the production process, from raw materials to finished goods [6, 7]. The subsidiary and tertiary chains that work together to build the supply chain network—an ecosystem—sustain the primary chain. Information and business transactions contribute to the complexity of the chain, which must be balanced. It is crucial to think that blockchain offers consistency and traceability throughout the supply chain [8].

A decentralized, distributed directory that powers smart contracts and offers the chance to aid traceability in record management, supply chain automation, payment applications, and other commercial processes can be described as a blockchain. Blockchain offers an immutable record that is duplicated in almost real-time between a network of business partners. The procedure uses data that would have previously been kept in the business Enterprise Resource Planning (ERP) system [9]. It now makes it accessible through a distributed network of records held by many businesses. Organizations can better understand their customers thanks to several blockchain advantages, especially on the demand side. Applications for both data analytics and artificial intelligence (AI) are well known. When it comes to technological viability, it can also hit a ceiling, yet many companies aim for convenience. It demands greater endurance and resilience than accelerated financial repercussions and enhances the protection and efficiency of procedures [10].

A chain of digital blocks linked to and related to one another to form an open distributed ledger is what is meant by the term “blockchain” in layman’s terms. It was initially just used to hold digital money transactions, but over time, it began to be used for purposes other than currency and payments [11]. Additionally, there are other blockchain varieties based on their functions and distinctive characteristics: Public, private, and consortium blockchains are the three different forms of blockchains. Since anyone can join the network and participate in network management, public blockchains are truly decentralized systems. In private blockchains, the network can only be joined and managed by invited members of a single organization. A mix of public and private blockchains, the consortium blockchain is also known as the “Federated Blockchain”. In terms of management and rights, the consortium blockchain, also known as the "Federated Blockchain," falls somewhere between public and private blockchains. It is possible for invited individuals from various organizations to join this blockchain. In a later section of this article, these various blockchain types are described in more detail. Blockchain's qualities or features, such as decentralization, pseudonymity, transparency, democratization, immutability, auditability, fault tolerance, and security, are what make it most applicable to such a broad range of fields. The accessibility of application development frameworks (ADFs) is crucial for the success of blockchain technology.

There are still many unresolved security and privacy issues related to Blockchain innovation, despite it being one of the modern technologies that has managed to achieve significant fame.

1.1. What this Survey Contributes and How it Compares to Other Survey Articles?

This work primarily adds to the body of knowledge in two ways. The evolution and architecture of Blockchain in relation to cryptocurrencies, as well as related architecture and research advancements for Smart Contracts (Blockchain 2.0), and Blockchain-based applications or ecosystems generally (Blockchain 3.0), are first discussed. Second, in this single document, we also provide a comparative review of the blockchain frameworks already in use, the consensus algorithms, the security threats, and the implications for the future. Numerous survey papers have recently tried to analyze blockchain technology in various depths and with a specific focus. A review of consensus methods, security concerns, and specifics of various Blockchain technology versions haven't all been covered in a single survey paper, according to the literature review. This gap in coverage inspires us to contribute with this paper's in-depth analysis of blockchain evolution, design, consensus, and security.

In the recent past, many survey studies were written with a sole emphasis on cryptocurrencies [12-14] or simply consensus algorithms [15-17]. Smart contracts and the architecture of blockchain applications have been briefly explored in a few articles (e.g., [8]. While the main review focus has been on Blockchain applications with other technologies like IoT and smart cities [18-20] other survey publications have also presented various Blockchain applications [21, 20]. Additionally, the security of the blockchain is discussed in a few survey studies, including [22, 23].

On the other hand, this survey's contribution is as follows: introductory technical concepts, issues, and characteristics are covered to help the reader comprehend Blockchain principles clearly. To ensure that information is understood holistically, the architecture of all Blockchain implementations, including cryptocurrencies, smart contracts, and generic applications, is thoroughly examined. All Blockchain versions' designs and workings are laid forth with distinct explanations for various regions. The research on development frameworks, security, and consensus methods is then thoroughly reviewed in this study.

The ultimate objective of this study is to familiarize the researchers with the inner technical specifics and research developments of all Blockchain technology variations. Figure 1 highlights the similarities and contrasts between the study topics included in this survey and those in earlier survey articles.

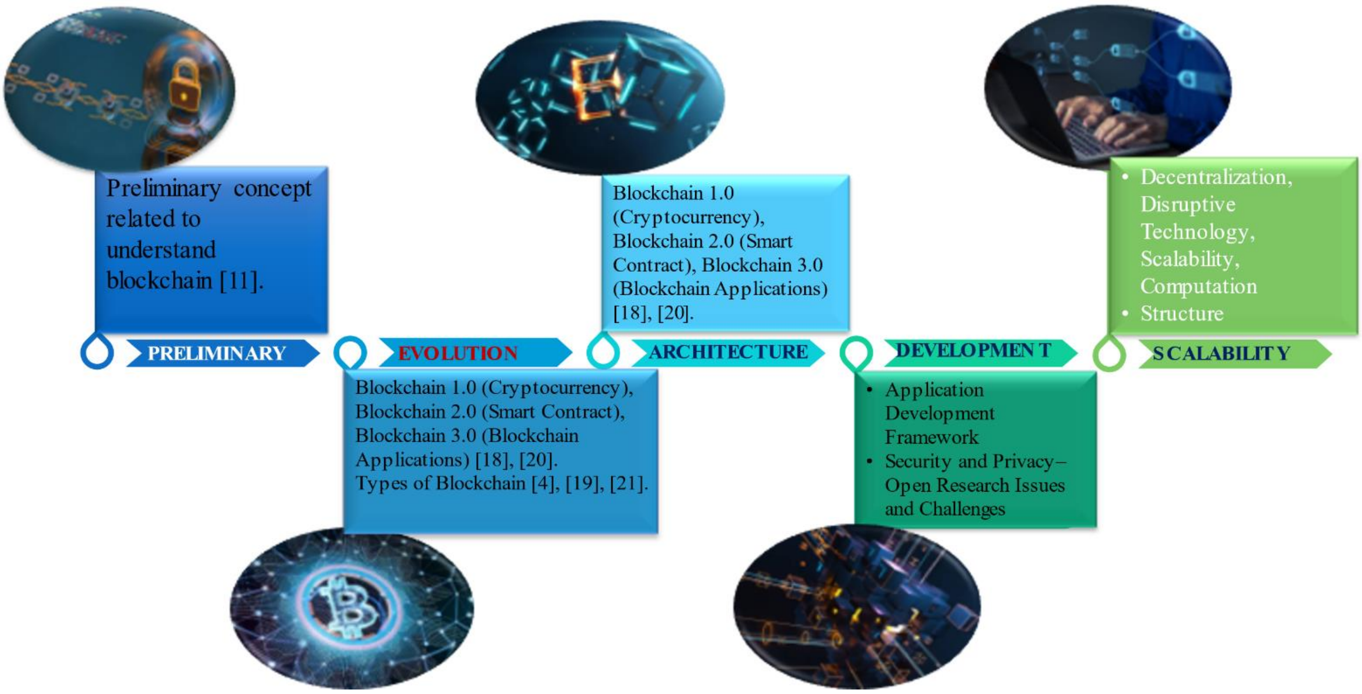

Figure 1. This survey paper compares recent Blockchain survey articles

1.2. Organization of This Research

The background, characteristics, and challenges of Blockchain properties is covered in Section 2 as an introduction to help readers grasp the main ideas of this article. The difficulties and problems with blockchain technology are also highlighted in this section. The application of Blockchain in different sectors is covered in detail in Section 3. Regarding the proposed framework model for Industry 4.0 Industrial Internet of Things and blockchain applications in general, Section 4 discusses current blockchain applications in the Industrial Internet of Things. Section 5 highlights the experimental analysis and future direction of the application of Blockchain.

2. Background, Characteristics, and Challenges of Blockchain

Although there are many obstacles to overcome, blockchain has a lot of potential and its widespread adoption may be prevented. Everyone connected to the network can view the transaction records and upload new data to the database thanks to the distributed peer-to-peer nature of the Blockchain. The system's fundamentals of openness and lack of centralized coordination have detrimental effects and restrict the adoption of Blockchain [24]. One can bring up challenges like scalability, security, privacy, latency, and the fact that the financial markets are still having trouble coming up with effective solutions [25].

2.1. Preliminary Network Concepts

2.1.1. Role of Peer-to-Peer (P2P) Networks in Blockchain

P2P technology is built on the decentralization principle, which is a straightforward idea. Blockchain's peer-to-peer architecture enables global cryptocurrency transfers without the use of middlemen, brokers, or centralized servers.

Anyone who wants to take part in the process of confirming and validating blocks can set up a Bitcoin node using the decentralized peer-to-peer network [26].

A peer-to-peer network that monitors one or more digital assets on a blockchain is decentralized. The term "peer-to-peer network" refers to a decentralized peer-to-peer system where each computer keeps a complete copy of the ledger and verifies it with other devices to guarantee the data is accurate.

2.1.2. Cryptography on the Blockchain

Data security using cryptography prevents illegal access. Cryptography is employed in the blockchain to safeguard transactions between two nodes in a blockchain network. The two key ideas in a blockchain are cryptography and hashing, as was previously discussed. In a P2P network, messages are encrypted using cryptography, and a blockchain's block data and link blocks are secured using hashing [27].

Security of participants, transactions, and precautions against double-spending are the main goals of cryptography. It aids in safeguarding various blockchain network transactions. It guarantees that the transaction data can only be obtained, read, and processed by the people for whom it is intended.

2.1.3. Cryptography Makes Use of Encryption and Decryption

The process of transforming plain text into a coded ciphertext that can only be read by the sender is known as encryption (keyholder). Decryption, on the other hand, is the process of making the coded ciphertext readable to the recipient. These two components guarantee the security of the cryptographic technique for usage by all users. This provides the blockchain with an avalanche effect, which means a small modification in the data can have a big impact on the final product [28].

2.1.4. Hash Functions

Common hash functions accept variable-length inputs and produce outputs with fixed lengths. Hash functions' message-passing abilities are combined with security features in cryptographic hash functions. In computing systems, hash functions are frequently used data structures for activities including verifying the accuracy of communications and authenticating data. Since they can be cracked in polynomial time, they are regarded as cryptographically “weak,” but they are difficult to crack. Traditional hash functions are strengthened with security features by cryptographic hash functions, making it more challenging to decipher message content or sender and receiver information [28].

2.1.5. Hash Chain

A hash chain is a collection of values obtained by applying a cryptographic hash function repeatedly to an input. Because of the characteristics of the hash function, it is possible to calculate subsequent values in a chain reasonably easily, but it is difficult to know what came before a given value. When an attacker can listen in on communications, Leslie Lamport first suggested employing hash chains to create a safe method of authentication using one-time passwords. A prototype authentication system for UNIX systems based on Lamport's plan was later described by Haller. Since then, researchers have discovered a variety of situations where hash chains are advantageous, including network routing, micropayment systems, and effective authentication in a variety of settings [29].

2.1.6. Merkle Tree

A hash tree also referred to as a Merkle tree, is a tree where each leaf node is labeled with the cryptographic hash of a data block and where each non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Although most hash tree implementations are binary (each node has two child nodes), they can also contain a large number more child nodes. The user can confirm whether it contains a transaction in the block by using a Merkle tree, which adds up all of the transactions in a block and creates a digital fingerprint of the complete set of activities.

2.1.7. Blockchain Timestamp and Document Verification

In order to authenticate the proof of work for ownership transfers of monies made possible by blockchain (Bitcoin blockchain), owners were initially required to digitally sign the transaction and send it through the public network. It required time and a brief phrase or piece of information to incorporate them into the block once it had been digitally authenticated. This also contributed significantly to a high level of transaction expenses. Only tiny quantities of metadata can be added to unchangeable digital data for a price. The new protocol timestamp system establishes a new digital platform for the transaction's signing and speedy verification. Take a document in linear form, for instance.

2.2. Key Features of Blockchain Technology

Blockchain technology has been around for a while and is still very much in the news. No one can completely underestimate this technology's impact on the world's economic environment, even though there are some conflicting opinions about it[30]. The popular cryptocurrency bitcoin is responsible for bringing the technology to public attention. Sadly, compared to other cryptocurrencies, it has now become overvalued and volatile. But the blockchain technology itself is what Bitcoin brought to our notice. Six key features of Blockchain technology are shown in Figure 2.

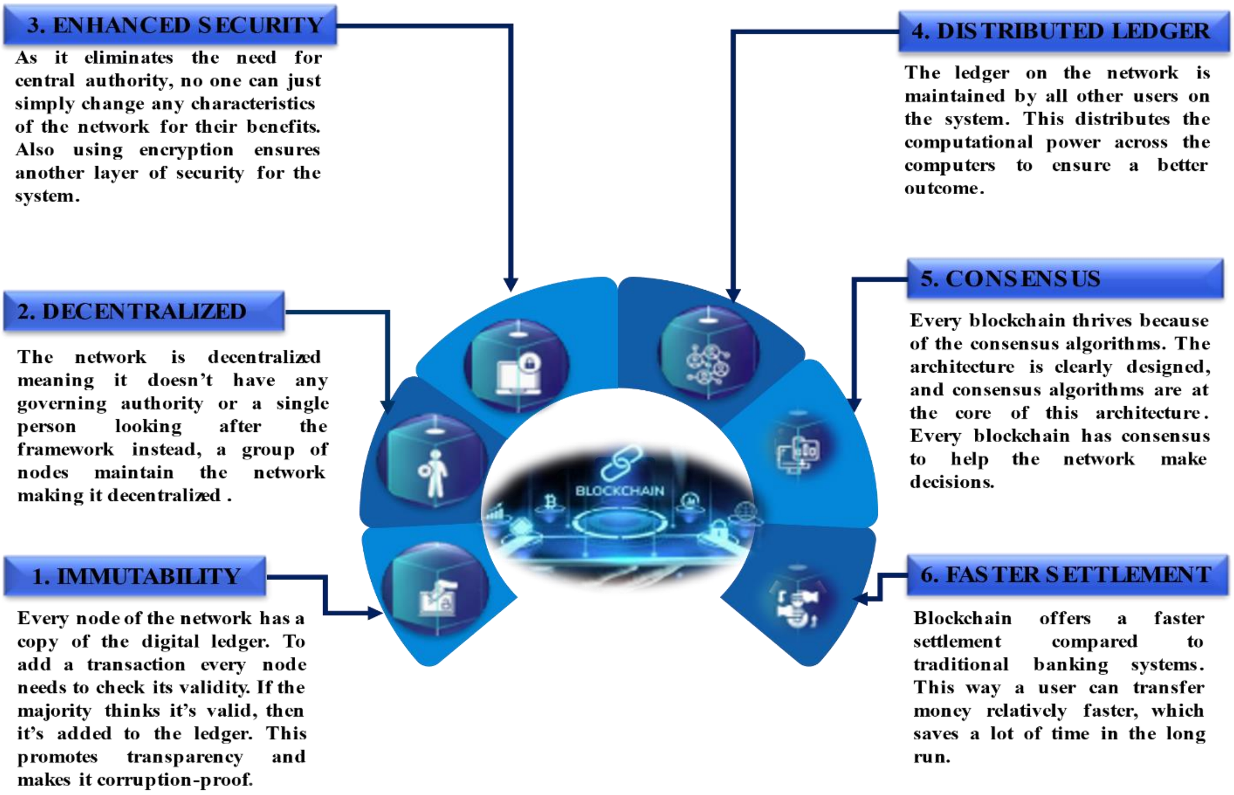

Figure 2. Six key features of Blockchain technology

2.2.1. Immutability

While there are many intriguing aspects of blockchain technology, "immutability" is unquestionably one of the most important ones. Why, though, is this technology untainted? Let's begin with an immutable connected blockchain. Immutability is the quality of not being able to be altered or modified. This is one of the top characteristics of the blockchain that helps to guarantee that the technology will continue to function as a permanent, unchangeable network. The way blockchain technology operates differs slightly from how traditional financial systems operate. A network of nodes is used to guarantee the blockchain's functionalities rather than depending on centralized authorities [31].

A copy of the digital ledger is stored on each node in the system. Every node must verify a transaction's authenticity before adding it. If the majority agrees that it is legitimate, it is recorded in the ledger. This encourages transparency and makes it impervious to corruption. As a result, no one can add any transaction blocks to the ledger without the approval of most nodes. The fact that no one can simply go back and modify transaction blocks once they are published to the ledger adds to the list of important blockchain features. As a result, it will be protected from editing, deleting, or updating by any network user [18, 31, 32].

Therefore, it is safe to infer that blockchain technology can significantly alter many of these scenarios when it comes to a corruption-free environment. Businesses' internal networking systems could not be breached, altered, or even had information stolen from them if blockchain technology was implemented. Public blockchains are the ideal illustration of this. The transactions on the public blockchain are completely transparent and visible to everyone. On the other hand, private or federated blockchain may be the best option for businesses that wish to maintain employee transparency and shield their private data from prying eyes.

2.2.2. Decentralized

The network is decentralized, which means that there isn't a single individual in charge of running it or any governing body. Instead, the network is maintained by a number of nodes, making it decentralized. One of the most important aspects of blockchain technology that functions flawlessly is this. Let me simplify things for you. Users are put in an easy situation by blockchain. We may immediately access the system via the web and put our assets there because it doesn't need any sort of regulating body [33].

Anything can be stored, including bitcoins, significant papers, contracts, and other priceless digital assets. And utilizing your private key and the blockchain, you'll have full control over them. So, you can see, the decentralized structure is returning control and rights over assets to the general populace [16, 17].

2.2.3. Enhanced Security

No one may simply alter any network properties for their benefit since there is no longer a requirement for a central authority. An additional layer of protection is provided for the system by using encryption. But how does it provide so much security in comparison to current technology? As a result of the unique cryptography it offers, it is very secure. Decentralization and cryptography together increase user security by one level. A mathematical algorithm known as cryptography serves as a firewall against intrusions. Every bit of data on the blockchain has been cryptographically hashed. Simply said, the network information masks the underlying nature of the data [33].

Any input data is placed through a mathematical procedure for this process, which results in a different form of value but whose length is always fixed. You may think of it as giving each piece of data a special identification. Each block in the ledger has its own distinct hash and includes the hash of the block before it [34]. Therefore, altering the data or attempting to tamper with it will require altering every hash ID. And that's pretty much not conceivable. To make transactions, you will need a public key, but you will need a private key to view the data [35].

2.2.4. Distributed Ledgers

Normally, a public ledger will include all the necessary details regarding a transaction and its parties. There is nowhere to hide as everything is in the open. Many individuals can observe what happens in the ledger in certain situations, even though the situation for private or federated blockchain is somewhat different [35]. This is so that all other system users can maintain the network's ledger. To ensure a better result, this divided processing power among the computers. It is regarded as one of the key components of the blockchain for this reason. The result will always be a ledger system that is more effective and can compete with the established ones [32-35].

2.2.5. Consensus

Consensus algorithms are essential to the success of every blockchain. Consensus algorithms are at the heart of this system, which is intelligently built. Every blockchain has a consensus mechanism to aid in network decision-making. Consensus can be defined as the collective decision-making process of the network's active nodes. The nodes can reach an agreement in this situation rapidly. For a system to function properly when millions of nodes are validating a transaction, a consensus is unavoidably required. It may be compared to a voting process where the majority wins and the minority is required to support it [36].

The consensus oversees the network's lack of trust. Although nodes might not trust one another, they can have faith in the algorithms that power the system. Because of this, every action taken on the network favors the blockchain. One advantage of blockchain technology is this. Blockchains all throughout the world use a variety of consensus algorithms. Each makes decisions in a special way and refines errors that have already been made. On the web, a zone of fairness is created by the architecture. Every blockchain must, however, have a consensus mechanism to maintain decentralization; otherwise, the blockchain's primary value is lost [16, 17, 21].

Different consensus algorithms each have their own benefits and drawbacks. Vukoli et al. employ the following characteristics to distinguish distinct consensus processes in Table 1, which shows a comparison between different consensus algorithms [37].

- Proof-of-work (PoW) is a consensus algorithm that relies on proofs. The fundamental idea behind the consensus technique is to discover and decide which node will be granted permission to add a new block to the current chain by demonstrating adequate evidence of its effort [15, 38].
- Proof-of-stake (PoS) can be a more energy-efficient alternative to proof-of-work (PoW). The miner doesn't have to use a lot of computer power to solve the mathematical problem using this consensus technique. Instead, participation in the block building process depends on holding a large enough interest in the system [39].
- Delegated proof-of-stake (DPoS) is an elective consensus method in which each node with a stake in the network can vote to assign another node the responsibility of validating transactions [40]. DPoS is a representation democratic process, whereas PoS adopts a direct democratic approach. The delegates, often referred to as witnesses, are chosen by the stakeholders to create and authenticate a block.
- Byzantine fault tolerance (BFT) is the ability of two nodes to successfully communicate across a distributed network in the presence of malicious or deceptive nodes [41]. One example of BFT, a replication algorithm capable of tolerating Byzantine errors, is practical byzantine fault tolerance (PBFT). PBFT was created to be a high-performance consensus method that may rely on a group of trusted nodes in the network and assumes that some nodes are dishonest or flawed [42].

- Byzantine consensus algorithm based Tendermint was proposed by Kwon & Buchman [43]. Each round determines a new block. In this round, a proposer would be chosen to broadcast an unconfirmed block. Therefore, for proposer selection, all nodes must be known. The prevote phase, precommit step, and commit step can all be broken down into one block. Validators decide whether to broadcast a prevote for the proposed block during the prevote process.

Table 1. The contrast between several consensus algorithms

Property	Proof of Work (PoW)	Proof of Stake (PoS)	Practical Byzantine fault tolerance (PFBT)	Delegated proof-of-stake (DPoS)	Tendermint
Identity Management of Node	Open	Open	Permissioned	Open	Permissioned
Energy Consumption	High	Low	Very low	Very low	Very low
Adversary Tolerance	$\leq 25\%$	$< 51\%$	$\leq 33.3\%$	$< 51\%$	$\leq 33.3\%$
Scalability	Strong	Strong	Weak	Strong	Strong
Performance (Transaction per second)	< 20	< 20	< 1000	< 500	< 1000
Forking	While two nodes identify the suitable nonce at the same time	Very difficult	Probably	Consistent if less than one third nodes are byzantine	Highly unlikely
Consensus confirmation time	High	High	Low	Medium	Low
Block creation speed	Slow	Fast	Fast	Depends on variant	Fast
Example	Bitcoin, Ethereum	Peercoin, Nextcoin	Hyperledger fabric	Bitshares	Tendermint

2.2.6. Faster Settlement

Traditional banking procedures are very cumbersome. After all settlements have been completed, it might occasionally take days to finalize a transaction. Additionally, it is easily corruptible. In comparison to conventional financial systems, blockchain provides a speedier settlement. In this manner, a user can transfer money somewhat more quickly, which ultimately saves a lot of time [28, 32, 36].

These blockchain capabilities simplify life for international employees and shed light on the significance of blockchain technology. Many people leave their family behind and go to another country in pursuit of a better life and job. However, it takes a long time to send money to their families who live abroad and doing so could be fatal in an emergency.

Blockchains are now far too quick, and people can send money to their loved ones using them with ease. The smart contract system is another interesting fact. This may enable quicker contract settlements of any kind. One of the greatest advantages of blockchain technology now is this. People can send money with a low cost if the middleman is eliminated [17].

2.3. Challenges and Tradeoff of Blockchain

One of the most popular buzzwords in business and technology right now is blockchain. With its capacity to operate without a centralized authority or middleman, it is seen as the technology that will revolutionize the financial industry. Blockchain is also seen to be advantageous for other businesses because of its capacity for storing tamper-proof data and managing a massive trail of records in a productive manner. However, blockchain has its limitations and is not practical for many different company models, much like previous new technologies [44].

Performance and scalability, privacy, interoperability, energy consumption, selfish mining, and current regulatory hurdles are the issues and challenges of blockchain technology that are covered in this section.

2.3.1. Performance and Scalability of Blockchain Technology

Solutions based on blockchain and cryptocurrencies for various business models are becoming more and more popular. Its performance and scalability raise questions about whether it will be able to fulfill the growing demand from various commercial and government-based sectors. Recently, researchers have been focusing on performance issues including throughput (the number of transactions per second) and latency (the amount of time needed to add a block of transactions to the blockchain) as well as scalability challenges relating to the number of replicas in the network [45]. Because the network must handle the higher volume of message exchange and processing, increasing the number of replicas can negatively impact throughput and latency. Although scalability can be guaranteed by protocols like PoW, they have a poor throughput and a significant latency. The resources used to solve the cryptographic conundrum required to publish a block and append it to the chain are the cause of this bottleneck.

For instance, the PoW-based system used by Bitcoin can grow to support many replicas. On the other hand, it has a low throughput, considering just 6–10 transactions per second (may be less depending on the network's complexity), and it can generate a block in an average of 10 minutes. The fact that this consensus process consumes a lot of CPU power and uses a lot of electricity is another disadvantage.

2.3.2. Privacy of Blockchain Technology

Given that users can conduct transactions using created addresses rather than their actual identities, blockchain is regarded as offering security and anonymity for sensitive personal data. However, some academics have hypothesized that due to network peers being able to see the public key used to start a transaction, blockchain may be vulnerable in terms of transactional privacy [46]. Although it is asserted that a peer can maintain their anonymity within the Blockchain network, new research on the Bitcoin platform has demonstrated that a member's real identity can be ascertained by linking their transaction history [47]. Additionally, when peers are protected by firewalls or network address translation (NAT), Biryukov et al. suggested a way to link peers' pseudonyms to IP addresses [48]. He also noted that peers' connected network of nodes can be used to uniquely identify them. The fact that all public key balances and details are visible to everyone in the network is the primary factor behind blockchain's susceptibility to information leaking. Therefore, the needs for privacy and security should be established at the beginning of blockchain applications.

2.3.3. Interoperability in Blockchain Technology

It is clear from Deloitte's 2018 research that a wide range of sectors are now considering implementing blockchain technology. There isn't a set protocol, though, that would enable them to cooperate and integrate. This circumstance, known as "lack of interoperability," has a negative effect on the development of the blockchain business. For this reason, cryptocurrency is still the primary platform for blockchain technology rather than providing various practical answers to a variety of business models. Although the lack of interoperability enables blockchain programmers to write code in a variety of computer languages, all these networks are closed off from one another and are unable to communicate. As an illustration, GitHub is home to more than 6,500 active blockchain projects that make use of various platforms, programming languages, consensus algorithms, protocols, and privacy features. In order to share blockchain-based solutions and interface with current systems, standardization is necessary for enterprise collaboration on application development.

2.3.4. Energy Consumption in Blockchain Technology

Bitcoin's proof-of-work (PoW) algorithm has made it possible to conduct peer-to-peer transactions in a distributed, decentralized, and trustless system. However, miner computers use a significant amount of electricity while performing this operation [49]. The Bitcoin energy consumption index was developed to shed light on the PoW algorithm's very unsustainable nature. People all throughout the world are motivated to mine Bitcoin by the incentive system. People are drawn to using power-hungry equipment to mine because it offers a reliable source of income. As a result, both the price of bitcoin and the network's overall energy consumption rate increased to a new high. The aggregate consumption of the Bitcoin network is more than that of a handful of nations, according to research released by the International Energy Agency [50].

2.3.5. Fairness and Security of Blockchain Technology

Because of technology's infancy, security holes leave consumers vulnerable to cybercrime. One of the most well-known problems with blockchain security is 51 percent of attacks. Such an attack occurs when one or more malicious parties' control most of a blockchain's hash rate. With most of hash rate, they may commit double-spends by reversing transactions and stopping other miners from confirming blocks.

Another unfair strategy used by mining pools to raise block rewards is known as selfish mining [51], which compromises the trustworthiness of a blockchain network. Eyal & Sirer (2018) presented a blockchain network that can still be vulnerable if someone wishes to cheat with a tiny amount of hashing power, even though malevolent nodes that have over 51% of computing power are thought to be able to take control of the blockchain network [52].

2.3.6. Problems with Current Regulation for Blockchain Technology

Cryptocurrencies and blockchain platforms in general are having consistency problems. Because the characteristics of this decentralized system make it harder for central banks to control economic policy, the government is wary about blockchain technology [53]. For instance, numerous governments have threatened to outlaw cryptocurrencies or have already done so. Several nations, including Pakistan, Iran, Ecuador, Morocco, and others have outlawed bitcoin, while Bangladesh has detained several bitcoin owners. The global legality of bitcoin is depicted in Figure. 3. Innovative distributed technologies face regulatory obstacles that negatively affect them, particularly in the EU and the USA, as demonstrated by Yeoh [54].

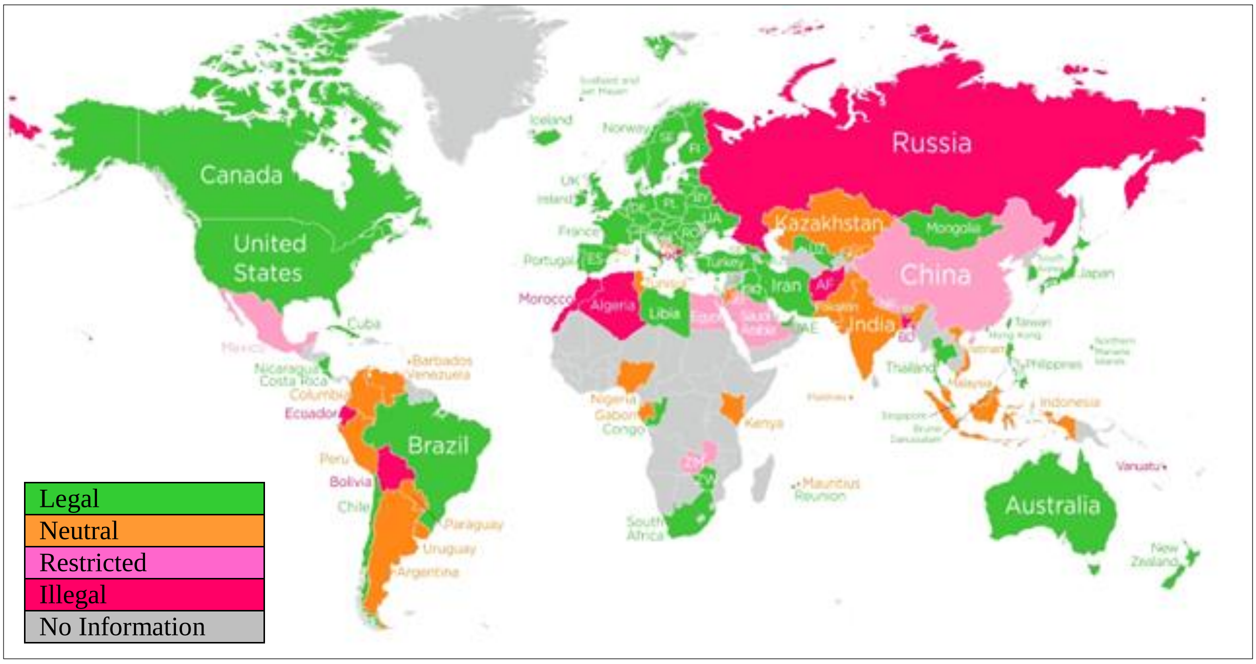

Figure 3. The legality of Bitcoin globally

Limitations provided by technical/scalability issues, business model issues, scandals and public perception, regulatory issues, and privacy issues for personal records could prevent blockchain from having wider and deeper applications.

3. Application of Blockchain in Different Sector

It is crucial to have ecosystem-level coordination and optimization as firms adapt to a novel and unique sense of normality to sustain ongoing growth. Across numerous enterprises and industries, one may create business outcomes using reliable data, end-to-end visibility, and workflow automation. Blockchain technology has a wide range of potential uses. It's critical to realize that bitcoin is not the same as blockchain; rather, it is one of technology's most widely used applications. The open, public, and anonymous blockchain network is used to conduct transactions involving digital money known as Bitcoin. However, according to experts, this technology can be used to identify answers for a variety of issues, including governance, supply chains, healthcare, voting, and other areas like identity management and energy resources. Additionally, some futurists assert that blockchain might influence the digital sphere similarly to how the internet did. We had no notion how the advent of the internet would alter our lives in the long run. No one anticipated the way the development of the Internet would alter the course of history, from smart phones and text messages to streaming movies and video conferencing with loved ones, as well as attending meetings and interviews. Since blockchain technology is still in its infancy, there is a lot of untapped potential. Some of the blockchain application domains suggested by various specialists are shown in Figure. 4. This section has covered a few blockchain use cases that have been proposed by researchers from around the world.

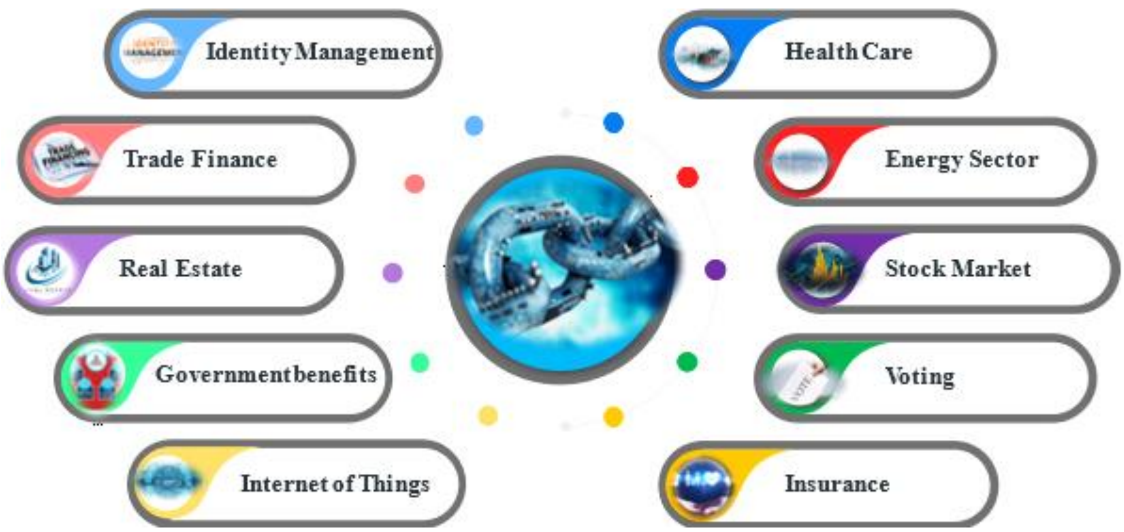

Figure 4. The legality of Bitcoin globally

3.1. Blockchain Assisting to Develop Faith in Healthcare System

The healthcare and life sciences sectors already had serious problems, like interoperability, privacy, and supply chain traceability, before COVID-19 became a prominent issue. Another significant issue is the frequent lack of interoperability across the proprietary electronic health record systems offered by more than 700 manufacturers [55]. And in 2018, there were 1,750 instances of drug counterfeiting in the United States alone [56].

As the epidemic persists, healthcare and the life sciences must alter supply chains to deliver protective gear and keep up with the rapid development of therapies, diagnostics, and vaccinations. Healthcare professionals are currently struggling with how to handle permission and safeguard personal health information as they attempt to use health data to open for business again in a secure manner. By fostering trust and collaboration, blockchain has already shown its worth in healthcare and the life sciences, and it will continue to be at the forefront of tackling new problems.

3.2. Reliability and Efficiency of Energy Sector

Microgrids are one of the key areas where blockchains are used in energy-related applications. A microgrid is a small, integrated system of electric power sources and loads that is designed to increase the reliability and efficiency of energy production and consumption [57]. The electric power sources may include distributed power plants, renewable energy facilities, and energy storage units housed in buildings built and owned by various businesses or energy suppliers. The ability of households and other electric power consumers, such as companies, to acquire the required energy while also producing and reselling extra energy to the grid is one of the key benefits of microgrid technology. Power buying and selling transactions in microgrids can be facilitated, recorded, and validated via blockchain. Like this, larger scale blockchain implementations can be utilized to support energy trade in smart grids [8]. Blockchain can be utilized in smart grids with bidirectional communication flow to provide private and secure consumption monitoring and energy trade without the requirement for a central middleman [58]. The programmatic articulation of anticipated levels of power flexibility, the verification and traceability of demand response agreements, and the equilibrium between power generation and demand can all be achieved with smart contracts. Furthermore, the Industrial Internet of Things (IIoT) can employ blockchain to enable energy trade [59]. Applying blockchain technology to energy-related applications has the potential to lower energy costs and boost resilience.

3.3. Stock Market

In the current market, trading in currencies and stocks is typically done through third-party clearing houses and brokering websites that facilitate orders in return for predetermined commission costs. For financial institutions, this can be a somewhat drawn-out procedure that can also result in higher fees when there are multiple middlemen involved.

However, blockchain technology would establish a direct connection between participants who may carry out their transactions through a peer-to-peer network of brokers and independent traders by utilizing a transparent and decentralized ledger.

While participants will still use an online trading platform to place orders, blockchain will be used for the underlying, back-office tasks, and ultimate settlement, improving efficiency and market liquidity. Although this method's use would differ between stocks and currencies due to these assets' diversity, it has many advantages. However, the use of blockchain would universally result in a more effective and economical trading procedure, reducing delays caused by third parties or custodians and essentially eliminating related auditing expenses. Additionally, this would be conducive to fast and real-time deals, which may be essential in a field as volatile and dynamic as foreign currency [60].

Blockchain technology may also provide timely benefits in the form of transparency, given the recent scrutiny of dubious actions by banks and other financial organizations. This would address a fundamental problem with financial market trading in the digital era, especially regarding liquid and malleable products like foreign exchange. For the sake of transparency, compliance, and accountability, blockchain would serve as a decentralized and almost impenetrable record of completed transactions, listing encrypted orders that are then distributed across a public network [61].

3.4. Transformation of Voting System

With the use of blockchain technology, flaws in the current electoral system can be corrected. Illegal voting was prevented, data safety was strengthened, and the election results were verified. The adoption of the electronic voting process on the blockchain is a major development [62]. Electronic voting does, however, come with some serious security issues, such as the possibility of vote manipulation and abuse if a voting system is infiltrated. Considering all of its potential benefits, electronic voting has not yet been widely used at the national level. Blockchain technology offers a workable solution to today's problems with computerized voting. Figure 5 depicts a Blockchain-based e-voting system architecture. The ability to vote is centralized in traditional voting systems. No one is aware of how to validate that document, so if someone wants to alter or change it, they can do it swiftly. Since the information is kept among numerous nodes, there is no one point of authority. All nodes cannot be compromised to alter the data. This makes it impossible to invalidate votes and effectively confirm them by tallying with other nodes.

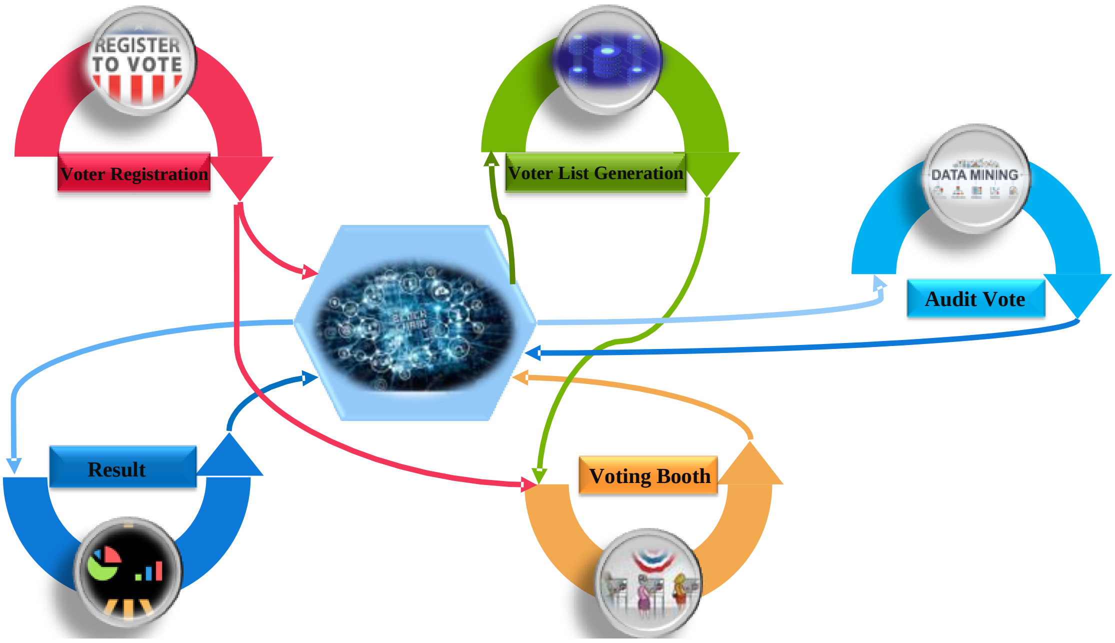

Figure 5. Blockchain voting systems architectural overview

3.5. Blockchain Based Insurance System

The insurance sector benefits from increased efficiency, security, and transparency thanks to blockchain. Distributed ledger technology can be used to improve cybersecurity measures, expedite payment processes, and streamline the processing of insurance claims. Blockchain users can transfer anything of value transparently and without a middleman's meddling thanks to smart contracts. Smart contracts specify the ground conditions between two parties, just like traditional contracts do. Smart contracts, as opposed to traditional ones, may monitor insurance claims, and hold both parties responsible.

A user could agree to pay an insurance company money in exchange for the firm's pledge to help pay for their future medical expenses by coding insurance plans as decentralized smart contracts. Based on the records of the owner of an insurance policy, blockchain smart contracts will provide immutable data that will instantly accept or reject any insurance claims submitted to the company [63]. A smart contract will immediately collapse, and the premium payments will be returned to the individual if the policy owner makes any false or fraudulent claims (or if an insurance provider decides not to cover a condition that was previously agreed upon). Due to the transparent disclosure of all data and the guarantee that any contractual departure would result in compensation for the affected party, the process fosters mutual trust between the two parties.

The insurance sector is susceptible to becoming mired down by time- and money-wasting inefficiencies brought on by the billions of forms, human error, and poor communication between parties because the insurance ecosystem consists of millions of insurers, healthcare providers, and patients [63].

Because all documentation and data are securely saved along the chain, digital ledger solutions like blockchain can assist automate antiquated procedures, saving billions of hours of paperwork every year, and lowering human error. Distributed ledger technology can help enhance communication between key players in an insurance claim. Doctors and insurance can safely see a patient's medical history to decide the best policies and practices moving forward if it is recorded on a blockchain. A sector that significantly relies on data gathered from being at the nexus of health, work, and personal life is especially drawn to blockchain's capacity to protect sensitive information [64]. Decentralized ledgers on the blockchain prevent corruption or manipulation by a single authority. Instead, all information is timestamped in chronological order to guarantee an accurate record of events.

3.6. Blockchain based Industrial IoT (IIoT)

The IIoT platform is essential in enabling electronic devices with the following capabilities: connectivity, big data analytics, and application development. It can deliver smart linked operations, connect assets, and enable IIoT. Most current industrial facilities, including micro-grids, smart-grids, vehicular ad-hoc networks (VANETs), etc., are developed without built-in intelligence to connect to IIoT, which requires interfaces to communicate with IIoT. On the other hand, emerging technologies like augmented reality (AR) help IIoT operators by improving the interaction and forecasting of process behaviors, which leads to their simplification and increased efficiency [65].

The first blockchain platform to offer a traceable, affordable, and reliable way to exchange bitcoins was Bitcoin. Smart IoT devices can use Bitcoin-based solutions in the IIoT space to record and exchange transactional actions. With integrated smart contract functionality and a flexible consensus approach, the Ethereum platform's Ethereum virtual machine (EVM) is widely utilized in the IoT. The smart contract offers IIoT applications that are down compatible. The Hyperledger is a well-known open source blockchain platform created by IBM that supports IBM Watson IoT Platforms and delivers distributed industrial components with consensus and membership procedures. IIoT applications can be considerably accelerated by the Hyperledger [66].

3.7. Blockchain for Government Public Application

Numerous pieces of personal data are kept on file by governments. Hackers frequently target personal information to get access to the benefits associated with it through fraud or exploited access keys. Blockchains present prospects for self-sovereign identity in circumstances where security is an issue or where governments cannot be trusted with the aforementioned information. More individual control over personal data is promised by this method of data storage. Our analysis makes it clear that, in most cases, the government or another reliable authority is required to authenticate the personal data kept in decentralized services. At this stage, most such applications are still purely conceptual.

Placing personal data, such as social security numbers and physical birth certificates, on a blockchain is one-way governments can leverage the technology. The fact that social security numbers are used for minor identity checks and other uses outside of direct government identification presents a security risk. It causes errors in record-keeping and security risks (as humans remain a weak link). Blockchain can offer higher security in these decentralized applications (such opening bank accounts, checking credit scores, etc.) since the records can be validated by a distributed rather than centralized procedure, even though encryption cannot be guaranteed [67].

Governments can assist those who save their personal data on blockchain-based systems. In such cases, the provision of the service of posting information to a blockchain is made privately, with governments assisting such efforts by, for example, establishing identity. Blockchain networks are already in place to protect personal data. A key to each person's personal data is provided. Using an app like a digital vault, people can back up their keys. Service providers can verify information via a person's smartphone or other device once their information has been coded into the network and confirmed (they must prove who they are). All of this can be connected to biometric information, guaranteeing that anyone who loses their identification can quickly and readily establish their identity (and fraudsters would have an extremely hard time faking biometric data). Data portability, decentralization, and a bare minimum of security are benefits of blockchain identity. Digital identity is also a crucial entry point for blockchain-based applications like voting [62].

3.8. Blockchain Application in the Real Estate Business

Blockchain is the best technology for real estate since it has a built-in system of trust. The blockchain's smart contracts and ledger capabilities are being used by real estate organizations all around the world to allow renting, purchasing, investing, and even financing transparently and effectively. A unified database of leases and acquisitions is more important than ever because of the enormous daily rate of real estate transactions. Blockchain can be useful here. Brokers and agents would be able to access the whole transaction history of a property if the traditional Multiple Listing Service database was upgraded to a blockchain-based one. Blockchain is being embraced by the expanding property-sharing business in addition to assisting the traditional real estate industry.

3.9. Blockchain Should be Embraced by Trade Finance to Realize its Digital Goals

It is past time for the trade financing industry to go digital. In addition to the enterprises, corporations, and other supply chain actors that banks and financial institutions service, the requirement to gather and effectively process trade data has never been greater.

There are numerous explanations for this. First, faster processing rates are required by trading partners, which can only be accomplished by switching to a more digital strategy and eliminating paper-based documentation. Second, after being disrupted by the pandemic for two years, supply networks are in severe need of stability. In addition, there is a stronger emphasis on offering workable solutions to the industry's changing environmental, social, and governance (ESG) needs and contributing to the solution of the climate emergency.

To this purpose, the field of trade finance may greatly benefit from digital alternatives like blockchain. Blockchain can offer the technological infrastructure to manage massive amounts of data rapidly, efficiently, and securely in an industry that is still mostly manual, and paper based. It can also connect numerous individual stakeholders through a decentralized network. For trade participants, obtaining trade data that covers both the material and financial facets of the supply chain opens a world of possibilities. For banks, it enables us to provide our customers with smart, individualized trade finance solutions.

Blockchain technology also makes it simpler for participants to build digital ecosystems, where bank, non-bank, and fintech businesses may cooperate to develop innovative solutions and add value. Such ecosystems go beyond what would typically be considered banking services and enable deeper connections and broader client engagement. With blockchain, we can implement the optimization that the sector has been calling for, enhancing supply chain transparency, and meeting critical needs for time and cost savings. Eliminating paper-based procedures may potentially strengthen links between participants throughout supply chains in the context of trade financing.

3.10. Practical Considerations on Identity and Blockchain

Blockchain is viewed as a brand-new, very distinctive technology that has the potential to disrupt a wide range of sectors, including identity. The development of new transformational concepts and ideas is ongoing, even as blockchain technology is still in its infancy.

This whitepaper summarizes the existing identification landscape, examines the distinctive features of blockchain, and explains how it can alleviate many of these identity-related concerns. Additionally, it discusses some cutting-edge and intriguing use cases that are currently being investigated and tested for blockchain-based identity transformation.

A digital version of the user's offline identification, like a passport or a driver's license, is not yet widely accepted. Every online application a user uses is assigned a separate digital identity. Users now have to remember all of their usernames and passwords, which is challenging and counterproductive. The user is vulnerable to a range of security risks due to multiple credentials.

By enabling the transparent transfer of a user identification from one domain to another, the federation has partially overcome this issue. For the end user, it often implies they can use an active or valid session with an identity provider to effortlessly access online services. Large social media firms like Facebook have recently contributed to the development of the idea of a social identity for users, which can be used as an alternative in specific use cases. Digital IDs are being issued by several nations, including Singapore and Estonia, so that people can identify themselves when utilizing e-services in a secure manner.

A series of assertions made about oneself, or other digital topics constitute a digital identity. A person with an identity, like Satyanand Singh, might have characteristics like gender, height, weight, mailing address, email address, date of birth, place of birth, citizenship, driver's license number, etc. Because they are specifically linked to Satyanand' s identification, some of these characteristics (such as his email address, SSN, passport number, etc.) will be unique identifiers.

It is important to note that some identities might last a lifetime, and some are permanent (like the license or passport number). However, a lot of identifiers can be changed (like cell phone numbers), thus it's possible that the same identifier is linked to a different identity at various points in time. Users and enterprises are burdened with needing to keep the attributes and identifiers in sync across the silos whenever there is a change due to the duplication of identities for every entity.

4. Introduction to the Industrial Internet of Things

The modern business environment presents hurdles for new business establishments in the form of new standards, novel trade practices, competitive pressure, and the requirement for timely delivery of goods. Because of this, a lot of businesses rely on the Industrial Internet of Things (IIoT) [68], which describes all or any actions taken by businesses to model, monitor, and improve their business processes using insights gathered from thousands of connected machines, things, and computers to help them realize financial success. IIoT, as its name suggests, is a concept that uses the Internet to link and manage machines, computers, devices, and other industrial items [69].

The term “Industry 4.0” refers to the union of the industrial value chain and IoT. The IIoT is the most effective innovation driver because it can be utilized to reduce operating and capital expenditures (OPEX and CAPEX), observe, and improve company processes regardless of how challenging they are, and support creative business models [70]. IIoT has profited from the increased interest it has received from academics and business, which has led to exponential developments in fresh approaches used in the sector. For instance, big data techniques are used to collect and send sensor data to the cloud to make a wise decision. The manufacturing process of 3D printing also produces modified items in a variety of shapes at lower costs and with shorter lead times [71].

Industrial IoT has grown quickly over the past few years because of numerous technological and industrial breakthroughs. The invention of steam engines in the 18th century served as a catalyst for the most significant industrial advancement. The steam engines' ability to mechanize enhanced industrial manufacture from the era of sanitized manual labor to the era of automation, which led to a significant boost in output. Electrical energy was used to replace steam power in the 1870s, and at the same time, the division of labor into specialized industries led to an explosion in production, which was another industrial breakthrough. The third industrial revolution, often known as "digitalization," took place around the 1960s. Innovative automation systems were created during this era because of programmable logic controllers and improved electronics used to increase manufacturing efficiency.

Information and communication methodologies significantly changed from the 20th century to the beginning of the 21st century, creating newer technical horizons [72]. By enhancing intelligence in sensing, networking, decision-making, and manufacturing, these strategies dramatically enhanced industrial productivity [73, 74]. The Industrial Internet of Things has lately become a standard in the industrial and educational sectors with the aim of integration and enhanced data gathering strategies inside traditional industries. To introduce the fourth industrial revolution and raise awareness in Europe, Industry 4.0 was principally utilized during the Hanover Fair in 2011. The IIoT milestones are shown in Figure 6.

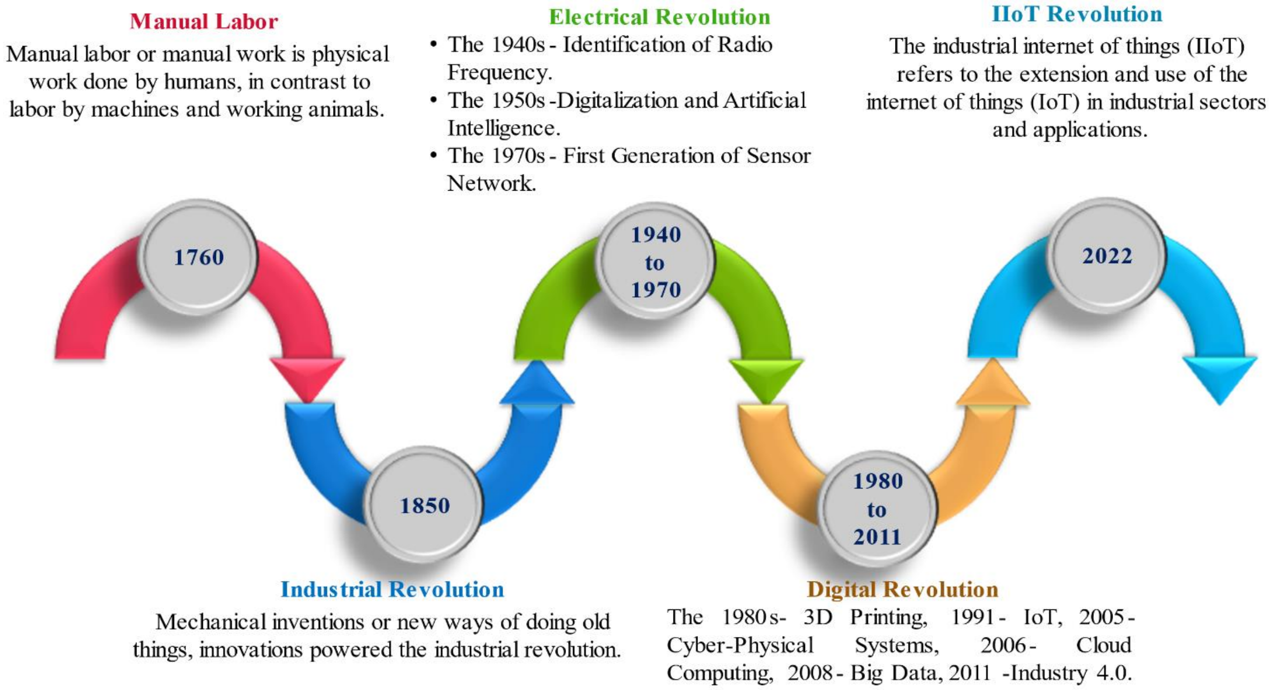

Figure 6. Timeline of key milestones of the Industrial Internet of Things

Intelligent machines for a variety of application scenarios in healthcare, manufacturing, and supply chain connect with one another in the IIoT to execute tasks without human intervention. automation of the home. IoT nodes can exchange data independently thanks to machine-to-machine (M2M) communication [75]. When "Big Data" technology developed by machines is used effectively, it improves the way that plans are carried out by gaining important domain knowledge. The IIoT's ubiquitous sensing, information sharing, and information collection with investigative capabilities are seen as a viable way to update existing applications by linking things, enabling integrated mechanization amongst things, and intelligently improving industrial processes [76]. By connecting things and enabling combined mechanization between them, the IIoT's omnipresent sense, information communication, and information gathering with investigation features are seen as a promising way to modernize successful applications while also intelligently improving industrial processes [76].

4.1. Proposed Framework Model for Industry 4.0 Industrial Internet of Things

In the future of digitalized smart manufacturing, this paper's major themes are digital transformation, mobility, and the IIoT consumer. More on-demand, customized, and integrated services that are distinct from those in the existing consumer market are required for the IIoT industry in the future. The IIoT industry's manufacturing process and the current business model may both alter because of the digitalization era. In the future, integrated services and transactions will be made possible by smart cities, electrical appliances, and electric cars, which will call for a new manner of interacting with the environment. Consumer behavior is evolving because of the expansion of on-demand and e-mobility services; people are becoming more open to sharing their data and using technology to improve their experiences. By merging with the IIoT sector, blockchain could play a bigger role in assisting change by utilizing a transparent, shared, and validated transaction process. In this section, we propose a blockchain-based distributed framework model for the IIoT industry in the smart city to meet current and future requirements. In the following sections, we discuss in detail the distributed framework model and its workflow, as well as the miner selection algorithm.

4.2. Blockchain-Based Distributed Framework Model

Digitalization is widely regarded as being necessary for competitiveness. The IIoT has grown rapidly in recent years; it continues to increase in value and adaptability at a rapid rate, creating smart ecosystems. Trusted suppliers in the supply chain lifecycle are carefully chosen, managed, audited, and accredited in the industry 4.0 of smart cities to give dependable, consistent, and high-quality services. In this paper, we put forth a proposal for how the blockchain structure model enables the creation of secure digital product memory records, from the sourcing of raw materials and production to the stages of upkeep and recycling in the supply chain lifespan.

The complete life cycle of the smart home appliances industry framework model in a smart city using a distributed blockchain-based scalable network is adapted [77]. In the proposed framework model, the entire life cycle is categorized into seven phases. Here, we leveraged the strength of the blockchain-based distributed network architecture from our previous work [77]. In our previous work, we presented a distributed blockchain network architecture to provide secure on-demand access and low-cost, competitive computing infrastructures in an IoT network. It enables high-performance, cost-effective computing by putting computing resources at the edge of the IIoT network and providing secure, low-latency access to large amounts of data. According to the suggested framework model, the regulator oversees producing the new electrical vehicle registration based on governmental laws and uploading it to the network's shared ledger in the first phase. Only the regulator will have the authority to do this, thanks to a smart contract.

The second phase, known as a consensus between the manufacturer and the regulator, is when the manufacturer receives the regulator's certificate of created ownership. After obtaining ownership, the manufacturer uses smart contracts to make the electrical vehicle model, ID, and template accessible in the network for all pertinent parties with the right authority. With the execution of smart contracts in the supply chain, the electrical electric car is transferred to the dealer and leasing firms in the third and fourth phases. The electric car goes through the maintenance and recycling phases in the fifth, sixth, and seventh phases of the supply chain life cycle before being finally released to the user after being passed to the leasing business. The suggested framework model offers services during the maintenance phase, including automated payment processing, insurance and maintenance services, dynamic and real-time data for the smart transportation system, and automated, tailored, and on-demand services to satisfy user needs. During the recycling phase, the scrap merchant executes a smart contract to permit us to scrap the electric car when it has reached the end of its useful life. The end user, maintenance provider, and scrap dealer are all involved in the synchronization process as it moves along the electric car's supply chain.

Figure 7 demonstrates the proposed blockchain-based distributed framework model for the electric car industry in industry 4.0 scenario's step-by-step methodological approach. The government regulator establishes the registration for the new vehicle based on the government rules and policies and creates a new block in the first phase of the supply chain lifecycle. We execute the block using the smart contract to make sure it complies with its terms and conditions and to start the transaction for the new block. Once the transaction is approved, the consensus and ownership transfer to the vehicle manufacturer are published in the distributed network built on the blockchain. Following the transfer of ownership, the vehicle manufacturer starts fabricating the vehicle model, building a new block, and carrying out a smart contract. Initiate the transaction for a new block, which will then be validated by network miner nodes if the newly produced block complies with the regulatory smart contract that is allowed. In this case, the regulator also validates and verifies transactions.

The manufacturer releases the vehicle template with updated visibility and the proper permissions for all pertinent network participants when the transactions have been authenticated. The dealer can get network data on stock availability after publishing the updated templates there. The dealer can then carry out their smart contract to start the transaction of the new block and transfer the vehicle to the dealer. Here, the validation procedure involves involvement from the manufacturer and regulators. Finally, the dealer posts the Vehicle template on the network for all users with the necessary access rights to view. The dealer has the option to also give loyalty points during this stage, which can be used and traded in the network as money. By using the customer's redeemed loyalty points, the dealer may finish the components purchase at a lower cost. After the loyalty points have been used, the dealer account will be updated so that, with the proper authorization, network users can see the rewards. If the newly produced block fulfills the smart contract, the leasing company builds a new block, transfers the vehicle from the dealer, accesses the updated vehicle template from the network, and starts a new transaction.

The regulator, manufacturer, and dealer verify and confirm the transaction, transfer ownership of the electric car to the end user, and broadcast the ownership, rights, and authorization of the vehicle into the network. The suggested framework model links the parties concerned in leasing a electric car to a client in a secure way to carry out know-your-customer checks before leasing the electric car, such as a credit check, ID check, and license check, and to store leasing contracts in the blockchain network. Various personalized, on-demand, and in-the-moment services are made available to the user throughout Phases 5 and 6, including insurance contracts, contracts for routine maintenance, and contracts for an automated gasoline payment system. The suggested concept enables insurance providers to modify vehicle insurance contracts based on actual driving behavior in this phase, automating insurance payment and financial settlement after a claim. Driving habits and safety incidents, such as speed, mileage, damaged parts, and collisions of a vehicle owner, could be kept, shared, and used to compute insurance premiums and payments in the blockchain network. Even after the electric car has been sold, the insurance provider can still use the owner's history to provide future insurance estimates because the record is linked to the owner.

The proposed blockchain-based framework model records and executes agreements and financial transactions for on-demand mobility, fuel payment, and ride-sharing services to enable the vehicle owners to monetize trips, pay at fuel service stations, and exchange data in a seamless, secure, and reliable manner. Vehicle status is accessible to scrap merchants at the conclusion of the lifecycle. Information, governing laws and regulations, the execution of a smart contract, a verification that the newly produced block complies with the smart contract, and the beginning of the new block's transaction were all done in a validated and verified manner. All necessary participants in the supply chain will take part in the validation process. The electric car will be given to the scrap dealer with the necessary license to dispose of the vehicle at the end of its lifecycle and make the associated update in the network once the transaction has been approved. In this section, we go over the distributed blockchain-based network architecture's miner node selection mechanism.

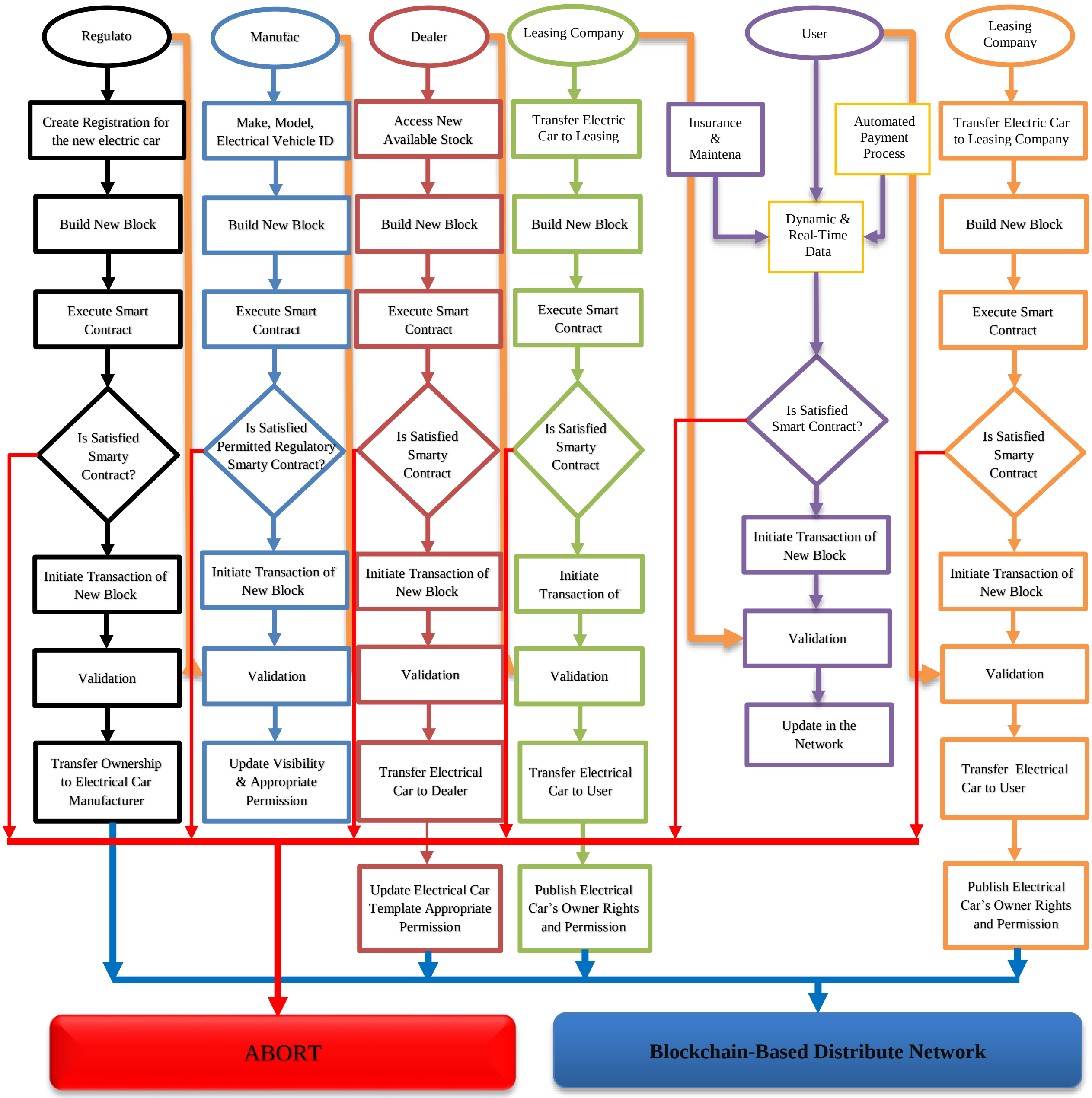

Figure 7. Flowchart illustration of the blockchain-based distributed framework model's methodological approach for the industry of manufacturing electric vehicles Industrial Internet of Things (IIoT) 4.0

5. Experimental Analysis and Future Direction of the Application of Blockchain

When discussing blockchain technology, the word "hashing" or "hash" is frequently used. Hashing is the process by which a particular algorithm converts input data of arbitrary length into a string of a predetermined length. Since the original data cannot be recovered through decryption, this approach is a one-way cryptographic function. The use of a cryptographic hash function is advantageous for storing passwords, preventing fraudulent transactions, and preventing double spending in blockchains. But what exactly is a Bitcoin hash, and what significance does it have in this situation? In other words, this is a unique number that the algorithm says cannot be duplicated. As a result, it is widely used to check the legitimacy of files. To put things into perspective, a hashed file's hash will automatically change if there is a change to the file. Additionally, every hash after that is linked to the one before it, guaranteeing the consistency of all blocks.

So, what exactly is a blockchain hashing algorithm and how does it operate? In a nutshell, a hashing algorithm uses an infinite number of bits to conduct calculations before returning a specific number of bits. No matter how much data input is, the output will always be corrected. As a result, the initial data is referred to as input, and the transformed data is referred to as a hash. Many hashing algorithms in use today only differ in how information is processed.

5.1. Implementing Blockchain as a Service

Having the required infrastructure to support technologies like Blockchain is one of the main obstacles to using them. Initial Blockchain setup necessitates a substantial infrastructure expenditure. In addition to creating your own closed virtual private network, this also entails always making certain servers available for mining and transaction processing, and if necessary, adding additional transaction and mining nodes. Not only is creating this environment time-consuming, difficult, and expensive. It can be challenging for most mid-sized and non-technology enterprises to build their own infrastructure.

This infrastructure issue is somewhat similar to the infrastructure issues that caused the Cloud infrastructure to develop. As a result, new technological infrastructure, also known as Infrastructure as a Service, erupted (IaaS). In order for them to concentrate solely on development and not worry about infrastructure, a number of Blockchain pioneering companies also felt the necessity to supply Blockchain infrastructure in the Cloud. These businesses used an arrangement known as "Blockchain as a Service" (BaaS). Companies that offer BaaS are referred to as BaaS providers, and businesses and individuals that use them are referred to as BaaS consumers. Ideally you should pay for the BaaS infrastructure as you utilize it as a consumer. The introduction of BaaS has facilitated the quick uptake of Blockchain technologies.

R3 Corda, Hyperledger Fabric, Ethereum, and other BaaS platforms are all available from Microsoft and are all hosted on Microsoft Azure. You can choose one of the predefined Azure Blockchain templates based on your business use case to get started. For each of the Blockchain implementations, there are free and premium tiers of BaaS offerings, just like with all other Microsoft Azure products and services.

5.2. Enterprise Ethereum Alliance

Since its launch in 2015, Ethereum has been gradually gaining traction worldwide. The Enterprise Ethereum Alliance was founded in 2017 by influential figures from business, academia, and government who recognised the importance of working together to support Ethereum (EEA). Figure 8 depicts EEA, a non-profit organization that supports Fortune 500 firms and academic institutions worldwide.

Figure 8. The Enterprise Ethereum Alliance's home page. If you haven't been to EEA, we encourage you to do so and explore the list of member businesses who embrace Ethereum

It's crucial to understand why Ethereum has become so well-known and established itself at the enterprise level before we look at the Ethereum words. There are several causes, but the main one is that Ethereum is open source and is better suited to building a private Blockchain. Ethereum is faster at processing transactions than Bitcoin. The Ethereum community's support has significantly grown since this book was written, so developers now receive a lot of aid and support from the community, which speeds up development. Let's quickly review some of the phrases used frequently in the Ethereum community.

The Ethereum network is composed of numerous computers, or substantial decentralized computers, together referred to as the Ethereum Virtual Machine (EVM). Ethereum nodes are all nodes that carry out the Ethereum protocol. These nodes have a full Blockchain installation. The nodes allow you to access the Blockchain in addition to connecting to other nodes. Then, some of the nodes can be used for other jobs like mining and other things. As soon as a new transaction is added, it is immediately replicated to these nodes.

In Ethereum, a consortium is a group. All the Blockchain consortium members who utilize the same infrastructure are a part of this group. You create a consortium with a leader known as a consortia leader when you cooperate within or across an organization using blockchain to set up their own private blockchain. The consortium's other nodes are referred to as consortium nodes. Establishing the consortium leader is the first and most important step in creating an Ethereum consortium. The consortium leader is in charge of putting up a private Blockchain, choosing the requirements for joining the network, and establishing the criterion for allocating ether.

The privately owned Blockchain is run by the consortium leader, and all other consortium members abide by the standards he or she has established. Once the consortium leader is established, additional participants can join using either the existing infrastructure or their own. For a lot of its operations, Asclepius (our hypothetical hospital) uses Blockchain to track a distributed ledger. Additionally, it works closely with several branches and hospitals. Asclepius' primary branch is serving as the consortium's coordinator. The cryptocurrency utilized in Ethereum transactions is called ether. Table 2 illustrates the variety of additional cryptocurrencies that can be used in Ethereum in addition to Ether.

Table 2. The Ether conversion to other Ethereum used cryptocurrencies

Unit	Alternative Name	Wei	Wei Value	Gwei Value	Ether Value
Wei	-	1	1 Wei	10^{-9} Gwei	10^{-18} ETH
Kwei	Babbage	1,000	10^{-3} Wei	10^{-6} Gwei	10^{-15} ETH
Mwei	Lovelace	1,000,000	10^{-6} Wei	10^{-3} Gwei	10^{-12} ETH
Gwei	Shannon	1,000,000,000	10^{-9} Wei	1 Gwei	10^{-9} ETH
Microether	Szabo	1,000,000,000,000	10^{-12} Wei	10^{-3} Gwei	10^{-6} ETH
Milliether	Finney	1,000,000,000,000,000	10^{-15} Wei	10^{-6} Gwei	10^{-3} ETH
Ether	-	1,000,000,000,000,000,000	10^{-18} Wei	10^{-9} Gwei	1 ETH

Each EVM node needs a sizable amount of processing power to run programs. While working on Blockchain, it is crucial to understand the computing effort necessary to run specific code, which is designated as Gas in the Blockchain environment. An EVM node is rewarded with rewards like more Ether for the proof of work after it has enough gas to run the code. Now let's examine how to configure Ethereum using Azure.

The Ethereum network can be set up in a variety of ways. Setting up your own infrastructure is one option. Using a BaaS solution from Azure to swiftly set up Ethereum in a couple of minutes is a simpler method. Several templates are provided by Azure for building Blockchain offerings. Each one of them offers the possibility to be customized and all of them have default templates. The default Azure templates should be your first pick because they handle the majority of the abstraction. With the exception of establishing a genesis block, default templates guarantee that the transaction and mining nodes are separated from one another and a part of the VPN. A genesis block is comparable to a distributed ledger that is empty or that has no data. The transaction can be written on top of the genesis block once it has been made. Additionally, it is crucial that mining nodes cannot be accessed outside of the private network for security reasons. Fortunately, it is completed automatically for you when using the basic Azure template. Let's rapidly construct a consortium leader using one of the Blockchain Azure templates. Other Blockchain Azure offerings can be created by following the same procedures.

5.3. Creating a Blockchain Consortium Leader from the Azure Portal

Visit https://portal.azure.com by opening it. After logging in, select Add a Resource and type “Ethereum” into the search bar to access all templates linked to the cryptocurrency, as shown in Figure 9. Lead the Ethereum Consortium by choosing. Start the Ethereum Consortium leader wizard by clicking Create and using the same deployment model. The following are the steps:

Step 1. To distinguish it from a different template, specify the resource prefix. We'll employ eth for the sake of convenience. You are free to use any prefix you like.

Step 2. A username is necessary to log in to the various nodes. We continue to utilize the gethadmin default username out of convenience. You can choose between using a password or an SSH public key as the password. We are currently using a password for the demo; however, you can also use the SSH public key. At least one uppercase, one lowercase, one numeric, and one special character must be included in the password.

Step 3. Choose the assigned subscription option. You have the Free Trial option if you haven't paid for a subscription. It is preferable to use a paid subscription rather than a free trial if you intend to use it in production. Choose the assigned subscription option. You have the Free Trial option if you haven't paid for a subscription. It is preferable to use a paid subscription rather than a free trial if you intend to use it in production.

Step 4. To ensure that future permissions and policies are consistent, create a new resource group.

Step 5. Use the space as you see fit. People typically like places that are closer to the real execution.

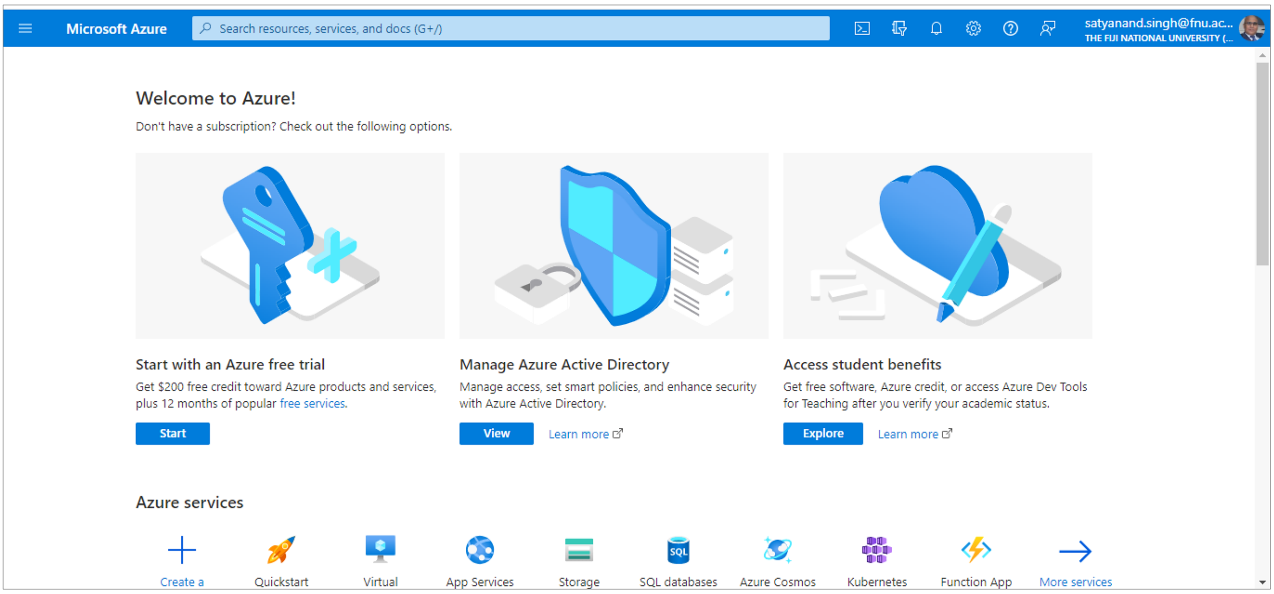

Figure 9. The Azure Portal templates for Ethereum. New templates are being created by Microsoft. More Ethereum-related templates than what is displayed here will be available

6. Conclusion

This decade will likely see a variety of ways that the blockchain grows and expands. One of the key elements of Industry 4.0 is digitalization, which enables businesses to gain efficiency in various areas, from management and technology consulting to supply chain planning and solutions. This blockchain holds potential for many businesses and can be beneficial in addition to other things. These days, banks use technology to speed up transactions and cut down on associated costs. Blockchain implementation extends beyond the banking sector to include the provision of information. This constant ledger verifies that the commodity was produced using the appropriate procedures and resources and that the procedure received approval. Blockchain ensures reliable and effective data sharing as well as the establishment of an immutable database of all communications exchanged by various connected smart devices. A great use case for blockchain is identity protection. Because it is manipulative, this technology enables users to create their own secure and reliable digital identity. People would be able to use their blockchain identities for a variety of things, from simple activities to programs, software, or signing digital signatures. Blockchain might be the answer to simplifying this phase by giving smaller businesses and providers a reliable source of high-quality transactional knowledge.

Also, certain suggestions were made with the intention of advising future BIoT researchers and developers on some of the problems that must be solved before releasing the BIoT applications of the next generation.

7. Declarations

7.1. Author Contributions

Conceptualization, S.S. and J.R.S.; methodology, S.S., J.R.S., and L.T.; formal analysis, S.S. and J.R.S.; investigation, S.S., J.R.S., and L.T.; resources, S.S., J.R.S., and L.T.; writing—original draft preparation, S.S.; writing—review and editing, S.S., J.R.S., and L.T.; visualization, S.S.; supervision, J.R.S.; project administration, L.T. All authors have read and agreed to the published version of the manuscript.

7.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.4. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

8. References

[1] Javaid, M., Haleem, A., Pratap Singh, R., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain: Research and Applications, 2(4). doi:10.1016/j.bcra.2021.100027.

[2] Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6), 3680–3689. doi:10.1109/TII.2019.2903342.

[3] Sandner, P., Lange, A., & Schulden, P. (2020). The role of the CFO of an industrial company: An analysis of the impact of blockchain technology. Future Internet, 12(8). doi:10.3390/FI12080128.

[4] Liu, X. L., Wang, W. M., Guo, H., Barenji, A. V., Li, Z., & Huang, G. Q. (2020). Industrial blockchain based framework for product lifecycle management in industry 4.0. Robotics and Computer-Integrated Manufacturing, 63, 101897. doi:10.1016/j.rcim.2019.101897.

[5] Esmaeilian, B., Sarkis, J., Lewis, K., & Behdad, S. (2020). Blockchain for the future of sustainable supply chain management in Industry 4.0. Resources, Conservation and Recycling, 163, 105064. doi:10.1016/j.resconrec.2020.105064.

[6] Ashraf, M., & Heavey, C. (2023). A Prototype of Supply Chain Traceability using Solana as blockchain and IoT. Procedia Computer Science, 217, 948–959. doi:10.1016/j.procs.2022.12.292.

[7] Cozzio, C., Viglia, G., Lemarie, L., & Cerutti, S. (2023). Toward an integration of blockchain technology in the food supply chain. Journal of Business Research, 162. doi:10.1016/j.jbusres.2023.113909.

[8] Junaidi, N., Abdullah, M. P., Alharbi, B., & Shaaban, M. (2023). Blockchain-based management of demand response in electric energy grids: A systematic review. Energy Reports, 9, 5075–5100. doi:10.1016/j.egyr.2023.04.020.

[9] Szalka, É., & Tamándl, L. (2019). Food industry in EU: Testing the efficiency of business on the example of Hungary. Economic Annals-XXI, 179(9), 66–79. doi:10.21003/ea.V179-06.

[10] Lin, C., He, D., Huang, X., Choo, K. K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications, 116, 42–52. doi:10.1016/j.jnca.2018.05.005.

[11] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly, Sebastopol, United States.

[12] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 21(2), 1676–1717. doi:10.1109/COMST.2018.2886932.

[13] Setyono, J. C., Suryawidjaja, W. S., & Girsang, A. S. (2022). Social Network Analysis of Cryptocurrency using Business Intelligence Dashboard. HighTech and Innovation Journal, 3(2), 220-229. doi: 10.28991/HIJ-2022-03-02-09.

[14] Neudecker, T., & Hartenstein, H. (2019). Network layer aspects of permissionless blockchains. IEEE Communications Surveys and Tutorials, 21(1), 838–857. doi:10.1109/COMST.2018.2852480.

[15] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access, 7, 22328–22370. doi:10.1109/ACCESS.2019.2896108.

[16] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks. IEEE Communications Surveys and Tutorials, 22(2), 1432–1465. doi:10.1109/COMST.2020.2969706.

[17] Wan, S., Li, M., Liu, G., & Wang, C. (2020). Recent advances in consensus protocols for blockchain: a survey. Wireless Networks, 26(8), 5579–5593. doi:10.1007/s11276-019-02195-0.

[18] Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys and Tutorials, 21(3), 2794–2830. doi:10.1109/COMST.2019.2899617.

[19] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. doi:10.1016/j.future.2017.11.022.

[20] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6, 32979–33001. doi:10.1109/ACCESS.2018.2842685.

[21] Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J. P. C., & Ko, K. (2018). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. IEEE Access, 6, 1513–1524. doi:10.1109/ACCESS.2017.2779263.

[22] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853. doi:10.1016/j.future.2017.08.020.

[23] Siddiqui, M. S., Ali, T., Nadeem, A., Nawaz, W., & S., S. (2020). BlockTrack-L: A Lightweight Blockchain-based Provenance Message Tracking in IoT. International Journal of Advanced Computer Science and Applications, 11(4), 463-470. doi:10.14569/ijacsa.2020.0110462.

[24] Drescher, D. (2017). Blockchain Basics. Apress Berkeley, New York, United States. doi:10.1007/978-1-4842-2604-9.

[25] Romano, D., & Schmid, G. (2017). Beyond bitcoin: A critical look at blockchain-based systems. Cryptography, 1(2), 15. doi:10.3390/cryptography1020015.

[26] Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Proceedings First International Conference on Peer-to-Peer Computing. doi:10.1109/p2p.2001.990434.

[27] Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Pearson Education, London, United Kingdom.

[28] Qadir, A. M., & Varol, N. (2019). A Review Paper on Cryptography. 2019 7th International Symposium on Digital Forensics and Security (ISDFS). doi:10.1109/isdfs.2019.8757514.

[29] Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770–772. doi:10.1145/358790.358797.

[30] Filep, B., Tamándl, L., Rámháp, S., & Kovács, Z. (2012). The Economical and Social Impact of Széchenyi István University (Győr, Hungary) on Regional Development. The 7th International Scientific Conference "Business and Management 2012". doi:10.3846/bm.2012.073.

[31] Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. Internet of Things, 8, 100107. doi:10.1016/j.iot.2019.100107.

[32] Farion, O., Balendr, A., Androshchuk, O., Mostovyi, A., & Grinchenko, V. (2022). Methods of Extraction and Analysis of Intelligence to Combat Threats of Organized Crime at the Border. Journal of Human, Earth, and Future, 3(3), 345-360. doi:10.28991/HEF-2022-03-03-07.

[33] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress). doi:10.1109/bigdatacongress.2017.85.

[34] Singh, S., Assaf Mansour, H., Kumar, A., & Agrawal, N. (2017). Speaker Recognition System for Limited Speech Data Using High-Level Speaker Specific Features and Support Vector Machines. International Journal of Applied Engineering Research, 12(19), 8026-8033.

[35] Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. IEEE Access, 8, 62478–62494. doi:10.1109/ACCESS.2020.2983601.

[36] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. IEEE Access, 5, 14757–14767. doi:10.1109/ACCESS.2017.2730843.

[37] Vukolić, M. (2012). Quorum Systems: With Applications to Storage and Consensus. Synthesis Lectures on Distributed Computing Theory, Springer, Cham, Switzerland. doi:10.2200/s00402ed1v01y201202dct009.

[38] Azimy, H., Ghorbani, A. A., & Bagheri, E. (2022). Preventing proof-of-work mining attacks. Information Sciences, 608, 1503-1523. doi:10.1016/j.ins.2022.07.035.

[39] Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. Review of Financial Studies, 34(3), 1156–1190. doi:10.1093/rfs/hhaa075.

[40] Sun, Y., Yan, B., Yao, Y., & Yu, J. (2021). DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. Procedia Computer Science, 187, 371–376. doi:10.1016/j.procs.2021.04.113.

[41] Wang, X., WeiLi, J., & Chai, J. (2018). The Research on the Incentive Method of Consortium Blockchain Based on Practical Byzantine Fault Tolerant. 2018 11th International Symposium on Computational Intelligence and Design (ISCID). doi:10.1109/iscid.2018.10136.

[42] Cachin, C., Schubert, S., & Vukolić, M. (2016). Non-determinism in byzantine fault-tolerant replication. arXiv preprint, arXiv:1603.07351. doi:10.48550/arXiv.1603.07351.

[43] Kwon J. and Buchman E. (2018). A network of distributed ledgers, pp. 1-41. Available online: https://v1.cosmos.network/resources/whitepaper (accessed on February 2023).

[44] Singh, S., Assaf, M. H., Das, S. R., Biswas, S. N., Petriu, E. M., & Groza, V. (2016). Short duration voice data speaker recognition system using novel fuzzy vector quantization algorithm. 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings. doi:10.1109/i2mtc.2016.7520363.

[45] Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. Open Problems in Network Security. iNetSec 2015, Lecture Notes in Computer Science, 9591. Springer, Cham, Switzerland. doi:10.1007/978-3-319-39028-4_9.

[46] Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain access privacy: Challenges and directions. IEEE Security and Privacy, 16(4), 38–45. doi:10.1109/MSP.2018.3111245.

[47] Smith, S. M., & Khovratovich, D. (2016). Identity system essentials. Evernym, 29 March 2016. Available online: https://www.evernym.com/wp-content/uploads/2017/02/Identity-System-Essentials.pdf (accessed on March 2023).

[48] Biryukov, A., & Pustogarov, I. (2015). Security and Privacy (SP). 2015 IEEE Symposium on Security and Privacy. doi:10.1109/SP.2015.15.

[49] O'Dwyer, K. J., & Malone, D. (2014). Bitcoin Mining and its Energy Footprint. 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014). doi:10.1049/cp.2014.0699.

[50] Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current Opinion in Environmental Sustainability, 28, 1–9. doi:10.1016/j.cosust.2017.04.011.

[51] Göbel, J., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 104, 23–41. doi:10.1016/j.peva.2016.07.001.

[52] Eyal, I., & Sirer, E. G. (2018). Majority Is Not Enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95–102. doi:10.1145/3212998.

[53] Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin, London, United Kingdom.

[54] Yeoh, P. (2017). Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance, 25(2), 196–208. doi:10.1108/JFRC-08-2016-0068.

[55] Schulte, F., & Fry, E. (2019). Death by 1,000 clicks: Where electronic health records went wrong. Kaiser Health News, 18.

[56] Mikulic, M. (2022). Counterfeit incidents concerning pharmaceuticals worldwide in 2021, by Region. United States.

[57] Lasseter, R. H., & Paigi, P. (2004). Microgrid: a conceptual solution. 2004 IEEE 35th Annual Power Electronics Specialists Conference (IEEE Cat. No.04CH37551). doi:10.1109/pesc.2004.1354758.

[58] Aitzhan, N. Z., & Svetinovic, D. (2018). Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840–852. doi:10.1109/TDSC.2016.2616861.

[59] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. IEEE Transactions on Industrial Informatics, 14(8), 3690–3700. doi:10.1109/TII.2017.2786307.

[60] Lee, L. (2015). New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market. SSRN Electronic Journal. doi:10.2139/ssrn.2656501.

[61] Paul Michelman, "How Blockchain Will Change Organizations. What the Digital Future Holds: 20 Groundbreaking Essays on How Technology is Reshaping the Practice of Management, MIT Press, Cambridge, United States.

[62] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17). doi:10.3390/s21175874.

[63] Shetty, A., Shetty, A. D., Pai, R. Y., Rao, R. R., Bhandary, R., Shetty, J., Nayak, S., Keerthi Dinesh, T., & Dsouza, K. J. (2022). Block Chain Application in Insurance Services: A Systematic Review of the Evidence. SAGE Open, 12(1), 1-15. doi:10.1177/21582440221079877.

[64] Anik, F. I., Sakib, N., Shahriar, H., Xie, Y., Nahiyan, H. A., & Ahamed, S. I. (2023). Unraveling a blockchain-based framework towards patient empowerment: A scoping review envisioning future smart health technologies. Smart Health, 29. doi:10.1016/j.smhl.2023.100401.

[65] Zhao, S., Li, S., & Yao, Y. (2019). Blockchain Enabled Industrial Internet of Things Technology. IEEE Transactions on Computational Social Systems, 6(6), 1442–1453. doi:10.1109/tcss.2019.2924054.

[66] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger fabric. Proceedings of the Thirteenth EuroSys Conference. doi:10.1145/3190508.3190538.

[67] J.-Y. Nie, (2017). Institute of Electrical and Electronics Engineers, and IEEE Computer Society, 2017 IEEE International Conference on Big Data : Proceedings : Dec 11- 14, 2017, Boston, MA, USA.

[68] Lade, P., Ghosh, R., & Srinivasan, S. (2017). Manufacturing analytics and industrial Internet of Things. IEEE Intelligent Systems, 32(3), 74–79. doi:10.1109/MIS.2017.49.

[69] Florea, B. C. (2018). Blockchain and Internet of Things data provider for smart applications. 2018 7th Mediterranean Conference on Embedded Computing (MECO). doi:10.1109/meco.2018.8406041.

[70] Sciancalepore, S., Piro, G., Caldarola, D., Boggia, G., & Bianchi, G. (2017). OAuth-IoT: An access control framework for the Internet of Things based on open standards. In 2017 IEEE symposium on computers and communications (ISCC), 676-681. doi:10.1109/ISCC.2017.8024606.

[71] Li, J. Q., Yu, F. R., Deng, G., Luo, C., Ming, Z., & Yan, Q. (2017). Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges. IEEE Communications Surveys and Tutorials, 19(3), 1504–1526. doi:10.1109/COMST.2017.2691349.

[72] Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges. IEEE Access, 8, 24746–24772. doi:10.1109/ACCESS.2020.2970576.

[73] Sodhro, A. H., Pirbhulal, S., & De Albuquerque, V. H. C. (2019). Artificial Intelligence-Driven Mechanism for Edge Computing-Based Industrial Applications. IEEE Transactions on Industrial Informatics, 15(7), 4235–4243. doi:10.1109/TII.2019.2902878.

[74] Kasten, J. E. (2020). Engineering and Manufacturing on the Blockchain: A Systematic Review. IEEE Engineering Management Review, 48(1), 31–47. doi:10.1109/EMR.2020.2964224.

[75] Wu, X., Duan, B., Yan, Y., & Zhong, Y. (2017). M2M Blockchain: The Case of Demand Side Management of Smart Grid. 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS). doi:10.1109/icpads.2017.00113.

[76] Meng, Z., Wu, Z., Muvianto, C., & Gray, J. (2017). A Data-Oriented M2M Messaging Mechanism for Industrial IoT Applications. IEEE Internet of Things Journal, 4(1), 236–246. doi:10.1109/JIOT.2016.2646375.

[77] Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. IEEE Access, 6, 115–124. doi:10.1109/ACCESS.2017.2757955.