Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4079781, 14 pages
https://doi.org/10.1155/2022/4079781

Review Article

Adoption of Blockchain Technology for Privacy and Security in the Context of Industry 4.0

Shubham Joshi,[1] **Anil Audumbar Pise**,[2] **Manish Shrivastava**,[3] **C. Revathy**,[4] **Harish Kumar**,[5] **Omar Alsetoohy**,[6] **and Reynah Akwafo**[7]

[1]*Department of Computer Engineering, SVKM'S NMIMS MPSTME Shirpur, Maharashtra, India*
[2]*Computer Science and Applied Mathematics, University of the Witwatersrand, Johannesburg, South Africa*
[3]*Department of Computer Science and Engineering, Chameli Devi Group of Institutions, Indore, India*
[4]*Kamaraj College of Engineering and Technology, Tamil Nadu, India*
[5]*Department of Computer Science, King Khalid University, Abha, Saudi Arabia*
[6]*Faculty of Tourism and Hotels, University of Sadat City, Sadat City, Egypt*
[7]*Electrical and Electronics Engineering, Bolgatanga Technical University, Ghana*

Correspondence should be addressed to Reynah Akwafo; reynah.akwafo@bolgatu.edu.gh

Received 17 January 2022; Revised 29 January 2022; Accepted 5 February 2022; Published 22 February 2022

Academic Editor: Kalidoss Rajakani

Compared to centralized and decentralized models, distributed models have the potential to dramatically expand the scalability of existing IoT and Industry 4.0 solutions while maintaining participant organizations' security and privacy. This is partly because participating firms are not required to rely on or trust other services or third parties to manage the data they gather and transfer, out of concern that these parties could misuse the data or, in the worst-case scenario, share it with mass surveillance programs. However, until blockchain technology (BCT) demonstrates its viability as a means of developing security solutions in decentralized, collaborative, and trustless environments, the vast majority of these use cases will struggle to meet the requirements for integrity, immutability, traceability, and notarization. By utilizing BCT, it is possible to eliminate intermediaries, enabling individuals and devices to manage their data independently of third parties and most significantly to achieve a high level of traceability with information flow harmony. This technology enables transaction, transparency, and traceability by enabling for the interchange of historical data. The fundamentals of blockchain are examined in this research paper, along with an investigation of its operation and a discussion of some of its most fundamental aspects and concepts. A concise overview of smart contracts enables us to completely reimagine how network members create and automate transactions. Finally, several IoT and Industry 4.0 application possibilities that leverage blockchain are investigated, as is the blockchain's future trajectory.

1. Introduction

BCT is one of the upcoming digital technologies that will be utilized during the Fourth Industrial Revolution (Industry 4.0). Security, privacy, and data transparency may all be improved by implementing BCT into the operations of both small and large-scale businesses. Industry 4.0 is a collection of innovative manufacturing techniques that enable enterprises to accomplish their goals more quickly. Additionally, it is referred to as Industry 4.0. Numerous studies on various Industry 4.0 technologies, including artificial intelligence (AI), the Internet of Things (IoT), big data, and blockchain, have been done in recent years to establish whether or not these technologies have the potential to cause substantial disruptions. These technologies provide a slew of possibilities in the manufacturing and supply chain management industries, respectively. BCT has garnered considerable attention and has the ability to significantly improve industrial and supply chain environments. Numerous unique insights into the benefits of BCT in a range of sectors are

Figure 1: Impact of Industry 4.0 on manufacturing with a smart factory [7].

currently available. The fundamental concepts of BCT emerged in the late 1980s and early 1990s. Lamport developed the Paxos protocol in 1989 and published the Part-Time Parliament in ACM Transactions on Computer Systems in 1990; the paper was later reprinted in the journal's 1998 edition [1, 2].

The digital world has grown more and more sophisticated since the 1970s, and we are getting closer to entirely digitizing our society, whether it is through smart home assistants or smart security systems. Industry 4.0 makes use of the IoT to digitally enhance factories, transforming them into smart manufacturing facilities. The establishment of cyber-physical' systems, mechanisms that are monitored by tightly integrated algorithms and software and which copy the physical systems onto a virtual network that makes decentralized decisions, is enabled by this structure, which we call the cyber-physical architecture. As a result of the development of the IoT, cyber-physical systems are now capable of communicating and cooperating with one another, allowing users to interact with systems in real time [3].

In today's context, it is vital to understand BCT and its implications in order to implement Industry 4.0 programs efficiently. Certain industries, such as financial transactions, where blockchains may provide trust, may benefit from BCT in the future. If foreign currency and fiat currency difficulties are ruled out, a controlled supply transaction may take place. The product itself, as well as the identifying element of its assembly, can be connected to other facets of Industry 4.0's BCT [4]. It serves as a reminder of the circumstances in which the ability to recognize defective goods may be beneficial. In this example, blockchain will safeguard all of a product's data, including its subassemblies, parts, and distribution networks. It reduces the cost of retrieval and the risk of service interruption at any stage in the supply chain. Cameras and sensors have gathered new data that might be used to create the blockchain's network. It gives us access to more knowledge than a human being could ever gather in a short amount of time [5, 6]. Figure 1 illustrates the impact of Industry 4.0 on manufacturing through the use of a smart factory.

To ensure that end-user support is not lost, it is necessary for an organization to undergo a similar structural shift as well. BCT has been hailed as one of the most significant technological advancements in a variety of sectors. This technology has advanced significantly in recent years and has a wide range of applications in the manufacturing industry. It is frequently used in conjunction with other buzzwords such as intelligent factories and Industry 4.0. Blockchain is an acronym that refers to a decentralized, encrypted, distributed ledger for filing computers that allows for the creation of tamper-proof, real-time logs [8, 9].

Several parts of Industry 4.0 are currently poorly explained and understood, and this is especially true for the digital transformation. It is hoped that the use of this new technology would result in an increase in the future effects of intelligent manufacturing solutions. A great deal has been gained from the early sales experiences as well as from the current deployments [10]. An inclusive distribution strategy is implemented and incorporates these new technologies that are being pushed and supported as resources in order to achieve broader corporate objectives. Due to the fact that blockchain may make the patent environment more straightforward, transparent, and less intermediate, it may be beneficial to SMEs (small and medium-sized firms) in particular in defending their discoveries. As a result, competition between companies that have a more difficult time gaining entry to the realm of patents would be encouraged. The ability to generate green energy from a freely bargained arrangement will be extended to individuals [11].

1.1. Problem Statement. Numerous studies have been conducted in recent years on the potential for severe disruptions caused by a variety of Industry 4.0 technologies, such as AI, the IoT, big data, and blockchain. As a result of the involvement of Industry 4.0 in the development of new digital technologies, the new technologies are built on the foundation of BCT, which serves as the primary building block. Industry

4.0 is a catch-all term for a collection of cutting-edge industrial technologies that assist businesses in increasing their efficiency. While BCT has the potential to significantly improve data security, privacy, and openness for both small as well as large enterprises, little research has been conducted on the application of BCT to Industry 4.0.

1.2. Motivation and Contribution. An important source of inspiration for this research piece is the fact that new disruptive technologies are being researched for integration into the production environment as a result of the Fourth Industrial Revolution, also known as Industry 4.0, which is currently underway. Bitcoin is one of these technologies, and it is designed to connect different systems while also facilitating commercial transactions along with improving asset monitoring. As a result, this technology assists in the establishment of an optimal supply chain that has the potential to influence the global market.

The following significant contributions are made by this study:

(1) In our study report, we conducted a thorough evaluation of existing blockchain applications in Industry 4.0

(2) We highlight both research work and commercially successful blockchain deployments for each of these critical industries

(3) Furthermore, we investigated the emerging application areas and constraints associated with the use of BCT in Industry 4.0.

The remainder of this paper is organized as follows. In Section 2, a review of different types of blockchain-related articles which are interconnected with Industrial Revolution 4.0 are explored and challenges of recent works are provided. In Section 3, basic concepts about blockchain in IR 4.0 are discussed. In Section 4, applications of BCT in Industry 4.0 are briefly explained. Then, Section 5 presents a proof-of-work (POW) mechanism in blockchain, and in Section 6, key costs impacted by BCT in Industry 4.0 are provided. Challenges to blockchain adoption are explained in Section 7. Blockchain's privacy-preserving approaches are provided in Section 8 while Section 9 provides details about appealing solutions in blockchain. The remaining sections provide blockchain technology's limitations with conclusion and future work.

2. Related Work

In [12], Cardoso et al. discuss the advantages of incorporating a BCT two-factor authentication (2FA) system into a Word-Press website to help safeguard user authentication data. The study employs an exploratory approach, with each analysis based on well-established theoretical reference data on the subject. Concurrent with the installation of the Hydro Raindrop MFA multifactor authentication plugin, a field study was carried out (i.e., MFA, also known as two-factor authentication or 2FA, is a security enhancement that requires a user to present two pieces of evidence or credentials when logging into an account). To improve security, the National Institute of Standards and Technology (NIST) recommends categorizing user credentials into two groups.

This is accomplished through the use of the BCT developed by the Hydrogen Technology Corporation [13] and the Ethereum-based Project Hydro platform [14]. As a result, the goal of their research work was to introduce and explain several of the implemented technologies, emphasizing their importance in information security. The primary findings indicated that using decentralized technology, such as BCT and the Hydro Raindrop plugin, significantly improves user authentication, thereby strengthening the safeguarding of individuals' and organizations' information and assets by inhibiting or reducing the likelihood of successful hacker attacks. Because of its use of modern BCT, this system is on the cutting edge of data security innovation [15]. It has the potential to make a significant contribution to the preservation of critical data and information, which is a core value shared by many Industry 4.0 firms [16].

In the study [17], the authors looked into the advantages of using the Hydro Raindrop multifactor authentication system on a Word-Press page. Also, the authors introduced FabRec, which they defined as a decentralized method of managing manufacturing information by multiple organizations using BCT, a system in which a decentralized network of manufacturing machines and computing nodes automates the transparency of an organization's capability based on historical events, as well as automated mechanisms for facilitating paperless contracts between participants via smart contracts [18]. This solution decentralizes critical manufacturer data and makes it available through a peer-to-peer network of fiduciary nodes, ensuring openness and data provenance via a verifiable audit trail. In [17, 19], the authors described a testbed platform composed of machine and system-on-chip platform computing nodes that can communicate with a consortium of disparate companies via a decentralized network. This prototype testbed demonstrates the benefit of locally stored computer code by dividing it into two independently initiated groups in the actual environment. Many of these issues can be addressed by middleware solutions and BCT functionality, which provide a development and execution environment.

The FabRec smart contract structure is made up of a global register contract (RC) that stores a list of historical event contracts from participants (PHECs). A list of participant relationship contract (PRC) addresses and their current status is included in each PHEC. The blockchain structure is represented by the relationship between the RC and the PHEC. Similarly, each record in the PRC table of the Oracle Database represents a contract between a participant (for example, a user requesting a fabrication service) and the metadata associated with this relationship. Finally, using a cloud MongoDB database can be thought of as a security device that enforces cryptographic verification that the data supplied by the virtual machine node is not altered [20].

There are certain unresolved performance and security challenges with the use of BCT for Industry 4.0. To begin, the security of BCT is contingent on the manner in which

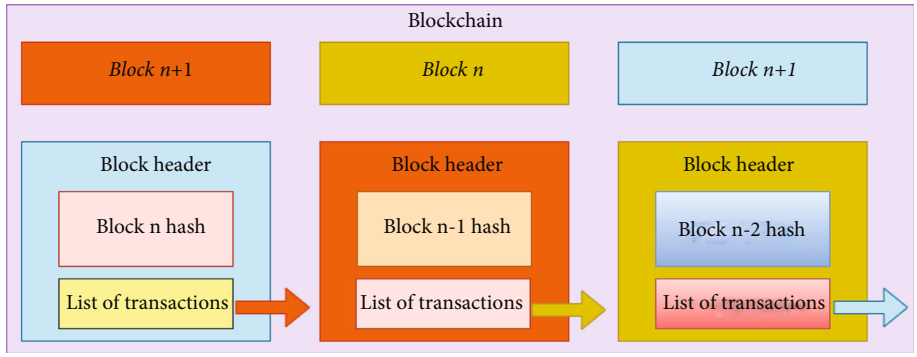

Figure 2: Design structure of blockchain [26].

it is implemented, as well as the software and hardware employed. Due to the fact that all user transactions in BCT are public, it is possible for users' private information to be published [21]. A hacked data user might be regarded as a possible target for both intrusion and denial-of-service attacks. One option is to compel information technology workers operating in an industrial environment to adhere to a policy for protecting confidential data by applying information security standards such as the ISO/IEC 27000 series and NIST recommendations. Second, when the number of miners (i.e., blocks) grows, the BCT grows in size [22]. This increases storage costs while decreasing network speed, resulting in a rise in the number of difficulties such as BCT scalability and availability [23]. For instance, when the number of blocks is increased significantly, the BCT's scalability becomes a concern, potentially resulting in an increase in network latency.

The use of multiple smart applications such as smart farming, smart healthcare, supply chain and logistics, business, tourism and hospitality, and energy management has expanded tremendously over the last several decades due to rising demand for innovative solutions. Security and privacy are key considerations for any applications because the Internet is an open conduit for data transit. Despite the fact that several smart application security solutions and standards have been presented over the years, current solutions are either centralized (with a single point of failure) or have large computational and communication costs. In addition, most current security solutions ignore scalability, robustness, data storage, network latency, auditability, immutability, and traceability [24].

Blockchain technology could be one solution to these problems. In a variety of industries, blockchain technology is on its way to becoming the prioritised standard for addressing concerns like scalability, resilience, data storage, network latency, auditability, immutability, and traceability. This research paper will provide you an overview of a few blockchain-based systems and their uses in Industry 4.0.

3. Blockchain in Industry 4.0

The blockchain is identified by a communication protocol, which is a system based on distributed database logic. Data is stored on many devices that are joined together by nodes in the latter system. Data transactions are separated into pieces and given their own cryptographic keys. The blocks constitute a linear sequence that leads to the establishment of the blockchain, which is its own chain [25]. Figure 2 illustrates the blockchain's design structure.

BCT is a data storage and transfer system that operates on a peer-to-peer (P2P) basis. To study, exchange, and fundamentally safeguard blockchain data, consensus-based mechanisms can be used. Due to the decentralized nature of its execution, no middlemen or trusted third parties are necessary. In layman's terms, blockchain technology is a type of distributed ledger. What exactly does the term "database" imply? A database is a collection of data that is organized. A data structure, in other terms, is a collection of data. As a result, blockchain is essentially a data storage system. As the name implies, there will be a chain of blocks.

These transactions are kept in blocks with cryptographic hashes in their headers that link them together. The fact that once a block is chained, the data stored within it is always available and cannot be modified or altered which ensures immutability. Each block includes a reference to the hash of the previous block. As a result, as shown in Figure 2, a chain of blocks, or blockchain, is generated. Any node with access to this ordered, back-linked list of blocks can read it to find out what the global status of the data being transmitted over the network is right now.

This basic blockchain is made up of a linked list of blocks. The features of each block are given below.

(i) Index

(ii) Timestamp

(iii) Previous Hash

(iv) Hash

(v) Data.

The first block is a one-of-a-kind block referred to as the genesis block. The Genesis block is unique in that it contains no previous blocks or data. The term block refers to a spreadsheet. The term "blockchain" encompasses the whole block family. The term BCT refers to a distributed ledger technology, in which a ledger is spread across network participants (nodes). Each node is responsible for maintaining

a copy of the blockchain. When the number of approved transactions in a block reaches a certain threshold, a new block is created. The blockchain is updated every ten minutes. This is something it does all by itself. The work of the computers is not directed by a central or master computer. It is impossible to update a spreadsheet, ledger, or register once it has been amended. As a result, forging is not a possibility any longer. Only by adding new components can it be enlarged. Across all networked devices, the register is updated in real time.

A node is a device that connects to a blockchain network and provides the infrastructure that allows the technology to operate and grow. Nodes are scattered across a large network and serve a range of functions.

3.1. Types of Blockchain. Private and public blockchains are the two types of blockchains. However, there are many different types of blockchains, such as consortium and hybrid blockchains. Before we go into the details of each blockchain, it is crucial to understand what they all have in common. Each blockchain is made up of nodes connected by a peer-to-peer (P2P) network. Every node in a network has a copy of the shared ledger, which is updated on a regular basis. Each node has the ability to validate transactions, send and receive them, and create blocks. To aid in comprehension, Figure 3 illustrates the various forms of blockchains.

3.1.1. Public Blockchain. A public blockchain is a distributed ledger technology that is permissionless and nonrestrictive. Anyone with access to the internet can join a blockchain platform and become an authorized node, joining the blockchain network. The following are the main characteristics of public blockchains:

(a) On a public blockchain, a node or user can view current and historical data, validate transactions, conduct proof-of-work on incoming blocks, and mine. The primary purpose of public blockchains is to make Bitcoin mining and trading more accessible to the general population. As a result, Bitcoin and Litecoin have become the most widely utilized public blockchains

(b) Public blockchains are frequently secure if users strictly follow security rules and procedures. However, it is only dangerous when players do not strictly follow the security procedures

(c) People from all walks of life can join, transact, mine, and read and write on the blockchain in this category. None of these variables are constrained, and anyone who uses permissionless blockchains is free to conduct transactions, keep a copy of the distributed ledger, and participate in the verification and addition of new blocks to the chain

(d) Furthermore, the blockchain is decentralized and transparent; no preset group of validators exists, and any user can contribute new blocks to the network by solving computationally difficult puzzles or staking their own money. Because each node keeps a full copy of the blockchain, it is secure and immutable

(e) Moreover, because each transaction is associated with a processing fee, this sort of blockchain is resistant to tampering, preventing the public ledger from being hacked because changing its contents would be prohibitively expensive.

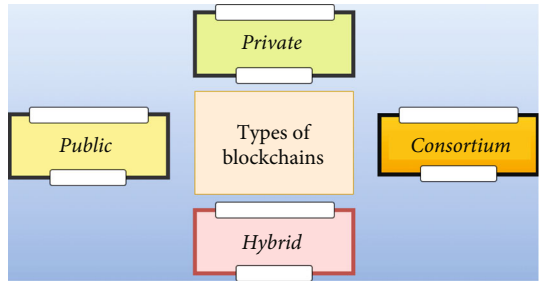

Figure 3: Types of blockchains [27].

3.1.2. Private Blockchain. This type of blockchain is frequently used to enable private data sharing and trade among known members of a specific organization. Because external users cannot access or participate in private blockchains unless they have been granted permission, they are also known as permissioned blockchains. The following are the primary characteristics of private blockchains:

(a) Users' involvement is controlled by a set of rules or an access-controlling network. This has the effect of concentrating the network while weakening the purported key blockchain characteristics of complete decentralization and openness

(b) When nodes join a private blockchain system, they contribute to the network's decentralized operation by keeping a copy of the ledger and working together to establish consensus on updates

(c) However, unlike public blockchains, writes are limited. A private blockchain is a permission-based or restricted blockchain that only exists within a closed network

(d) Private blockchains are widely used within organizations or enterprises because only a few individuals participate in the blockchain network. The amount of security, authorizations, permissions, and accessibility is determined by the controlling organization

(e) As a result, private blockchains operate in a similar manner to public blockchains but with a more limited network. Private blockchain networks are used for a variety of purposes, including voting, supply chain management, digital identity, and asset ownership.

3.1.3. Hybrid Blockchain. A hybrid blockchain combines private and public ledgers into a single digital ledger.

The following are the primary characteristics of hybrid blockchains:

(a) It combines the benefits of both types of blockchains, allowing for both private and public permission-based systems

(b) By utilizing a hybrid network, users can control who has access to which data stored on the blockchain

(c) Only a subset of the data or records on the blockchain may be made public, with the remainder remaining private on the private network

(d) The hybrid BCT is adaptable, allowing users to easily connect a private blockchain to several public blockchains

(e) A transaction on a hybrid blockchain's private network is frequently confirmed within that network. Users can, however, verify it by putting it on the public blockchain

(f) Public blockchains increase the number of nodes involved in the verification process and improve hashing. This improves the blockchain network's security and transparency.

3.1.4. Consortium Blockchain. A consortium blockchain is a type of semidecentralized blockchain in which multiple entities administer the network. A private blockchain, on the other hand, was discovered to be owned by a single company. Several companies may operate as nodes in this type of blockchain, exchanging data and mining. Financial companies, government agencies, and other similar organizations frequently employ consortium blockchains. The following are the main characteristics of consortium blockchains:

(a) This is a partially private and permissioned blockchain in which a preselected collection of nodes controls the consensus process and block validation rather than a single entity

(b) These nodes determine who is allowed to join the network and participate in the consensus process. Due to the control exercised by a few selected validator nodes, it is a fairly centralized system

(c) This type of blockchain, like private blockchains, has no processing fees, and publishing new blocks is computationally simple [28]

(d) While it provides auditability and decreased transaction latency, because the consortium is controlled by a majority of nodes, it does not entirely ensure immutability and irreversibility, which could lead to blockchain manipulation.

Finally, we want you to use your knowledge to determine which blockchain is best for you. If you are part of a public blockchain network, all you have to do now is figure out how it works so you can make informed decisions in the future.

4. Applications of BCT in Industry 4.0

Blockchain enables decentralized transactions and knowledge exchange in Industry 4.0 by performing a series of processing operations within a secure framework that verifies all transactions and timings. Blockchain not only allows businesses to operate more comfortably, but it also confirms their trust. It grew in popularity over time and benefited the environment. While factories are gradually adopting digital transformation, they cannot ignore the benefits of digitalization in terms of efficiency, competitiveness, and agility. We have compiled a list of the most important blockchain applications for Industry 4.0 and illustrated the same in Figure 4.

(1) Transparency and Immutability

Two of the most coveted properties of blockchain are its capacity to maintain open data and its resistance to data change. As a result, it is suitable for supporting Industry 4.0 processes, which require data openness and dependability, as previously indicated.

(2) Tokenomics

Blockchain systems include a mechanism for addressing the economic aspects of Industry 4.0 in the form of crypto tokens. Tokens, for example, can be used by entities outside of a smart factory to execute smart contracts and make other payments to the factory. This could allow for a high level of personalization, which was one of the original goals of the Industry 4.0 strategy.

DLT and tokens, in a broader sense, may form the foundation of a future machine economy, allowing intelligent devices to communicate with and pay for other intelligent machines.

(3) Decentralization

Another of blockchain's distinguishing features that corresponds well to an Industry 4.0 design idea. Blockchain systems are well-known for their independence from central authorities; indeed, the desire of decentralization was probably the fundamental motivation for both the conception of the blockchain and its subsequent development. Consensus methods are used in blockchain networks to ensure that their members adhere to a set of established norms. This technology has the potential to dramatically increase the ability of intelligent devices to act autonomously. This is enhanced by another intriguing feature of BCT.

(4) Programmability

Specific blockchain systems, such as Ethereum and EOS, offer self-executing programs known as smart contracts that can complete actions automatically when certain circumstances are satisfied. This means that the logic underlying various smart factory activities might be encoded in smart contracts, reducing the need for human oversight even further.

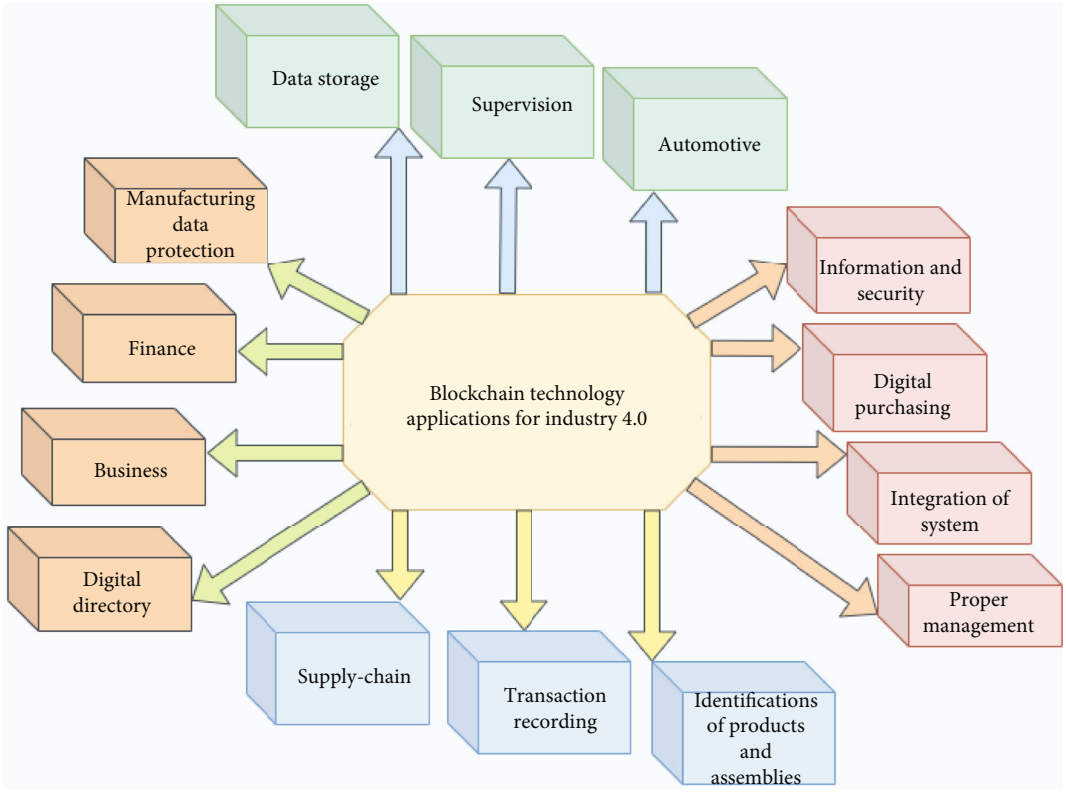

Figure 4: BCT applications for Industry 4.0 [29].

(5) Interoperability

One of the design principles of Industry 4.0 is also at the heart of blockchain's design philosophy. Blockchain-based systems are all about information sharing among interconnected nodes, and the technology can be used to meet the demands of automated manufacturing. A smart factory, for example, could be designed as a peer-to-peer blockchain network, with each machine serving as a node that performs a specific function and freely communicating with other nodes. Another advantage of this approach is that two or more such systems (for example, multiple smart factories) can easily share information as long as they are built on the same blockchain.

BCT could also be applied in a variety of other industries, such as smart metering to optimize energy use or to ensure the management of a building's energy efficiency certificate is secure. Its operating standards are founded on preserving, recording, and permanently establishing them. BCT, as an intelligent network, enables a wealth of possibilities in Industry 4.0. Due to the network flexibility inherent in blockchain transactions, they promise a higher degree of automation, fewer interparty frictions, and consequently cost savings and operational acceleration [30, 31]. It may be implemented in a variety of ways to diverse supply chain systems, resulting in huge benefits for everyone involved. Consumers have a lot of options, and businesses can increase their competitiveness by controlling supply and demand in real time [32]. The effective use of label qualities like immutability, traceability, safety, robustness, and openness illustrates the efficacy of commercial processes.

5. Proof-of-Work (PoW) Mechanism in Blockchain

To construct a viable mining strategy for all nodes, Nakamoto [33] created proof-of-work (PoW) in Bitcoin. To explain this system technically, different protocols and algorithms are used. The Nakamoto protocol employs a noninteractive cryptographic puzzle that must be solved and verified independently by each node. This is a hashcash cryptography algorithm. The goal is to see if there is a value in a hash of inputs that is less than or equal to the target value.

The first and most extensively used consensus mechanism is the blockchain proof-of-work consensus algorithm. Naturally, there are a variety of reasons for its popularity. However, its ability to foster honesty in a decentralized system is its primary explanation for its reputation. While there are various techniques for establishing Byzantine fault tolerance, PoW remains a viable choice (BFT).

Miners assemble all broadcasted transactions into a candidate block and look for valid transactions in it. The solution is to include a secure hash parameter that allows all nodes to verify the block's authenticity. The authorized block is added to the blockchain. The miner who solves the Genesis transaction first will be rewarded. Let us take a

closer look at the math. The SHA-256 algorithm is used by Bitcoin to hash data in the candidate block's head. To see if the hash is smaller, it is initialized and compared to the objective. If that does not work, the nonce value is changed, and it is tried again [22]. 256 bits, or 64 hexadecimal digits, is the ideal length.

$$\text{SHA} - 256(A_1 \| A_2 \| A_3 \| A_4 \| A_5 \| A_6 \| A_7) \leq \text{CT}. \quad (1)$$

In Equation (1) CT means current target.

(1) The previous Block's hash value is A_1

(2) The Merkle root of transactions is A_2

(3) Nonce is A_3.

Here, $0 \leq \text{Nonce} \leq 4{,}294{,}967{,}296$.

(4) Target difficulty is A_4

(5) Timestamp is A_5

(6) Bitcoin protocol version is A_6.

In [33] Nakamoto represented the first target in the Bitcoin genesis block in the pack format of $0 \times 1d00ffff$ in hexadecimal numbers.

A four-byte hexadecimal packed number is the aim. The target's length in bytes is represented by the first byte, H, and the target's value is represented by the next three bytes, R. To put it another way, H stands for the total number of bytes, while R stands for the destination followed by leading zeroes. The difficulty rating represents how difficult it is to find the current target when compared to the genesis block. For instance, the target is $0 \times 192815cc$, where 0×19 represents the H component and $0 \times 2815cc$ represents the R component.

$$\begin{cases} 0 \times 19 = 25 \text{ in decimal} \\ 0 \times 2815cc = 2627020 \text{ in decimal}. \end{cases} \quad (2)$$

The total length of a target is 256 bits, or 64 hexadecimal digits between 0 and F. Because each byte contains two hexadecimal digits, the target length is 50 digits in hexadecimal format, beginning with 0×2815cc0000000000000000 0000000000000000000000 0000000.

And the leading zeroes add out to $64 \times 50 = 14$. Eventually, the target will start with 14 zeros: 0×0000000000 0 0002815cc0000000000000000000 0000000000000000000 0000.

Now, the hash value must be less than or equal to the target value.

As another example, the above-mentioned Genesis block target is $0 \times 1d00ffff$, which means

$$\begin{cases} 0 \times 1d = 29 \text{ in decimal} \\ 0 \times 00ffff = 65535 \text{ in decimal}. \end{cases} \quad (3)$$

The target has $2 \times 29 = 58$ hexadecimal digits beginning with $0 \times 00fff$0000000000000000000000000000000000000000 00 000000000000000.

Finally, the original target is $0 \times 00000000ffff0000000$ 0000000000000000000000 0000000000000000000000000.

This can be obtained by adhering to the formula.

Notable is the fact that $H > = 3$.

$$\text{Target} = R \times 2^{(8 \times (H-3))}, \quad 0 \times 008000 \leq \text{target} \leq 0 \times 00ffff. \quad (4)$$

The average time between blocks was 10 minutes [34, 35], with 144 blocks per day and 2016 blocks every two weeks. The Bitcoin protocol modifies the network's difficulty objective following the creation of the 2016 block. We will need a new target metric to establish the new goal. The situation is as follows:

$$\text{Difficulty} = \frac{\text{Target of Genesis Block}}{\text{Current Target}}. \quad (5)$$

The difficulty of finding the hash target is determined by the ratio. The amended target should be easier to find if the time interval between making 2016 blocks was longer than expected, and harder to find if the time period was less than two weeks. After each 2016 block, the target and difficulty change [36, 37].

$$\text{ND} = \frac{\text{CD} \times \text{Timestamp of building last 2016 blocks}}{\text{20160 Minutes}}. \quad (6)$$

Here, ND means new difficulty.

The acronym CD stands for current difficulty. Validating transactions takes over 10 minutes to discover a block, and proof-of-work uses a lot of electricity. The number of hash values generated by a computer or mining pool per second is known as the hash rate. The hash rate rises in tandem with the amount of miners and equipment. Because proof-of-work is inequitable if a miner can independently compute at least 51% of the hash rate, and if she is dishonest, she can just spend twice.

6. Key Costs Impacted by BCT in Industry 4.0

The impact of BCT on two of the most essential costs, verification and network connectivity, is examined in this section. To ensure that markets remain viable indefinitely, participants must be able to evaluate and audit transaction attributes as quickly as possible, including the parties' qualifications and reputations, the nature of the assets transferred, and external events and information that may have an impact on contractual arrangements.

It is critical to focus on the key cost aspects impacted by BCT in Industry 4.0 in order to improve system efficiency and reduce development and operating costs. BCT has a significant impact on two major cost elements, namely (1) verification and (2) networking.

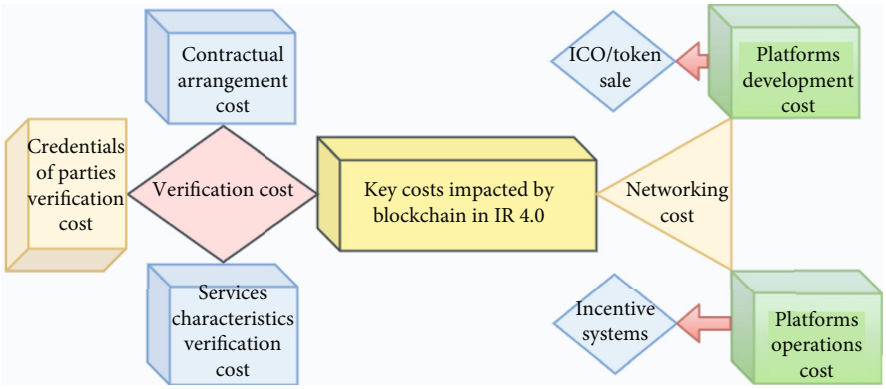

Figure 5: Key costs impacted by BCT in Industry 4.0 [4].

In the event of a problem, BCT, like Bitcoin, alters this flow by providing for the cost-free confirmation of digital information. In a distributed ledger, any market participant, regardless of location, can examine any transaction attribute or information about the agents and objects involved in real time and at a low cost. The cost-effectiveness of blockchain-based platforms is depicted in Figure 5.

The cost of verification in the transaction of goods and services between sellers and customers can be significant in terms of both money and time. Those interested in the transaction should be able to verify and audit its qualities, which should include the credentials of those involved in the market transaction, the features of the goods and services traded between parties, and any other contractual terms and conditions. Blockchain reduces the overall cost of verification by eliminating the need for intermediaries and simplifying the verification of transaction attributes.

In addition, BCT lowers the cost of network infrastructure. When entrepreneurs and developers launch a new platform, they typically use an initial coin offering (ICO) or the sale of native or specialized tokens to fund the network's development costs. The ability of blockchain to lower prices is critical because, historically, intermediaries gained market power by providing customers with intermediary services. In the case of blockchain, on the other hand, market power is distributed across the network's various stakeholders, resulting in long-term societal stability.

7. Challenges to Blockchain Adoption

Depending on where the challenges occur, bottlenecks to BCT adoption are classified as intraorganizational or interorganizational. This section will break down all of the difficulties into subsections.

7.1. Interorganizational Barriers. The behavior and relationships of the parties define the efficiency of BCT as a cross-company supply chain software solution. Effective implementations necessitate not only the connectivity of individual supply chain partners but also the participation of the majority, if not all, of them [38]. The following are the obstacles that exist between organizations:

(1) Reluctance to Divulge Data

Information sharing is usually limited to direct partners and does not extend beyond many levels of the supply chain, making it difficult to set universal standards and exhibiting a reluctance to share data. This could be exacerbated by a power imbalance among supply chain members [31].

(2) Competitive Disadvantages

While the exchange of data and information via blockchain may improve and maintain supply chain traceability [39, 40], transparent data may raise concerns and anxiety about data being accidentally leaked and passed on to other participants. Members of the supply chain, in particular, are concerned that sharing data will disadvantage them competitively [41].

(3) Constraints of Finance and People

Furthermore, the cost of integrating into the supply chain may be an impediment for individual members, leading to aversion to technological change and a lack of collaboration. Financial and human constraints, particularly for small and medium-sized enterprises (SMEs) [42], may result in a lack of network adoption of technological innovation, in addition to prohibitive implementation costs in large supply chains [43]. This is especially true when the added value of the implementation is not immediately apparent.

(4) Role Distribution

Along with issues of cooperation, the blockchain has created a new division of labor among supply chain actors. Businesses must assume new and unexpected responsibilities, which can be discouraging, especially during the supply chain's technology adoption phase [38]. If, on the other hand, a supply chain participant is forced to take on new responsibilities, the reorganization of tasks may result in the formation of the blockchain [44].

7.2. Intraorganizational Barriers

7.2.1. Approval Time. A lengthy approval procedure may also be investigated as a result of a lack of willingness to embrace technology and technological misunderstandings [45]. Adoption of a technology may be rejected if it is not accompanied by structural changes within the organization [46], which limits the scope of the implementation process. As a result, BCT adoption is sluggish [47].

7.2.2. Obstacles in Organizational Culture and Policy. Company cultures and laws can occasionally act as intraorganizational roadblocks. Despite the fact that the advancement of BCT has the potential to influence corporate culture, new organizational norms are required [48]. The application of BCT has caused a shift in the distribution of jobs, responsibilities, and abilities. One such example is innovation policy. In recent years, institutional innovations have become increasingly rare within corporations. Instead, it was distinguished by stable economic models that evolved over time [27]. Technological advancements, on the other hand, have raised the bar for businesses in terms of adaptability and change. Because BCT requires new ways of doing business, changes in corporate culture and regulations must be implemented within the company.

7.2.3. Financial Restrictions. The expenses of purchasing and deploying new technology are high, especially at first [49]. Furthermore, it is costly but necessary to educate personnel on how to adapt to these changes. As a result, incorporating this technology into the organization will necessitate a significant upfront investment. Profits can be made through reducing effort and saving time, but only after the technology has been used successfully for a long time [50].

Initially, implementing BCT within a company may cause financial difficulties. Because integrating blockchain technologies into a business is complicated, BCT adoption is pricey. It does, however, allow for safe and low-cost data exchanges, resulting in a supply chain that is both flexible and cost-effective [51].

7.2.4. Lack of Expertise and Resources. Furthermore, blockchain implementation knowledge and tools are scarce [47]. Businesses are unsure how to successfully manage technology due to a lack of uniform standards [52]. Furthermore, because the long-term viability of BCT is unknown, it is fraught with danger, and its widespread adoption may be hampered. A stable environment, on the other hand, may help to compensate for the lack of information about the long-term viability of the implementation [29].

7.3. External Obstacles. A number of external factors may influence or obstruct the adoption of BCT in the supply chain.

7.3.1. Legal Implications and Applicable Legislation. Furthermore, legal considerations and regulations may present a significant barrier to the use of BCT in the supply chain. Supply chains are internationally networked in an age of globalisation, and the movement of commodities within them is a complicated legal issue due to the proliferation of various parties and regulations [42]. Furthermore, it is vexing that there is no clear legal regulation or legislation governing the use of BCT. As a result, legal uncertainty may serve as an external barrier to implementation [53].

7.3.2. Competition. One such reason could be competition. Blockchain-based technology is being adopted in the context of a technological trend centered on blockchain in order to maintain competitiveness, despite the fact that these conditions are incompatible with the current supply chain and provide no additional value [38].

7.4. Technical Impediments. A lack of access to technology [54] is frequently a major issue in a supply chain. To derive additional value from a digital supply chain, all supply chain participants must have access to the necessary information [55], and all participants must use the same technique or technology. This is not possible, however, due to the disparities in the capabilities of various businesses. For example, not every business can afford the high startup costs [47].

The following are some of the problems that can arise as a result of a lack of technological access:

(1) Lack of Security

Despite the fact that BCT is defined by its immutability, data fraud and fabrication cannot be completely avoided, which could lead to a security breach [56]. Another factor to consider is the human being who, while interacting with BCT, may generate or gather inaccurate data [54]. Consider the user's private key, which is used to verify a person's identity in a blockchain. Because of the decentralized structure of the blockchain, the user is responsible for this. In order to complete a transaction, this key must be imported, and it is possible that it will be stolen during the process. Identification of the culprit is nearly impossible due to the lack of a monitoring party [57].

(2) Developmental Immaturity

In addition, BCT is still in its early stages [58]. Because the supply chain is still in its early stages, problems may arise for which no solutions exist because not all potential barriers have been studied [59].

(3) Adverse Publicity

Another difficulty is raising awareness through negative publicity. Even corrected faults can be seen on the blockchain and across the supply chain [60]. Furthermore, blockchain-related activities may receive negative media attention. These characteristics may influence how organizations and employees view blockchain [61]. Because data security is a primary issue for businesses, this could have a negative influence on other stakeholders in the BCT. In the event of fraud or insecurity, this is not guaranteed. As a result, negative experiences and announcements may have an influence on and drive away potential technology users.

8. Blockchain's Privacy-Preserving Approaches

The implementation of this technology to specific use cases has gotten a lot of attention as interest in it grows. Several significant recommendations linked with the scenarios listed below are discussed in the sections that follow.

8.1. Cryptocurrencies. During the previous few years, the most prominent blockchain-based scenario has been associated with the use of cryptocurrencies. Cryptocurrencies, with a market value of more than $600 billion, represent the future of global payments and remittances, with Bitcoin [33] accounting for more than 90% of the total market capitalisation. In these instances, it is vital to retain the privacy of the parties involved in a transaction (i.e., payer and payee) as well as conceal the amount of coins to be transferred. Recent projects in this approach, such as ZeroCoin [62], CoinJoin [14], Zerocash [63], and Blindcoin [64], will be explored in further detail later in this section and depicted in Figure 6.

8.2. e-Government. Given that individuals' identities are recorded on the blockchain, it is possible to use the SSI model to handle privacy concerns in this brand-new field of application for the first time. It is being employed in this new area of application to deal with privacy concerns that have arisen as a result of the model's implementation. Switzerland (on the basis of uPort [66]), Finland (for immigration services), and Estonia (the first country to experiment with BCT on a national scale and to allow individuals from any country to become e-residents [67]) have all expressed interest in incorporating blockchain technologies into administration services. People's privacy must be protected in this case by establishing minimal disclosure rules while utilizing the aforementioned services, which must be adopted as soon as practicable.

8.3. Smart Cities. As a result of the integration of the Internet of Things (IoT) technology and platform integration, existing towns are being transformed into true smart cities. This can only be done with the help of correct data from a variety of sources, which is difficult to come by. Although privacy concerns must be addressed appropriately [68, 69] BCT's distributed nature, as well as the promise of data immutability and verifiability, may serve as a platform for more secure and trustworthy data-driven applications. Privacy problems, on the other hand, must be addressed properly.

8.4. C-ITS. The evolution of conventional means of transportation into Cooperative Intelligent Transportation Systems is being accelerated by advances in wireless technology (C-ITS). When artificial intelligence techniques are merged into the creation of fully autonomous vehicles, this trend will continue to gain traction in the future years [70]. Vehicle sensors are expected to acquire a huge amount of personal information in order to carry out this strategy, which could pose a privacy risk. As a result, blockchain concepts are important in this scenario since they allow for the establishment of a decentralized infrastructure ledger that can be used to track the activity of such autonomous entities [71].

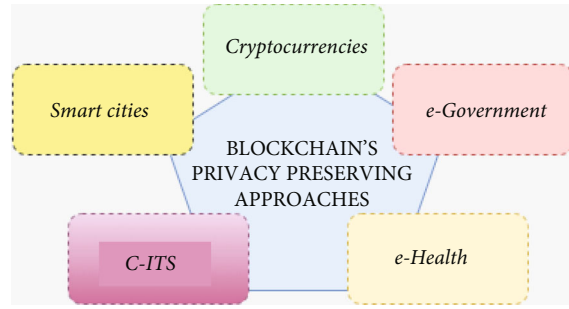

Figure 6: Blockchain's privacy-preserving approaches [65].

8.5. e-Health. The usage of BCT, according to its proponents, will be especially advantageous in the context of e-Health services. Improving personal health record management is particularly crucial in order to provide more effective and personalised healthcare services. Simultaneously, due to the sensitivity of e-Health data, it is vital that it is properly protected to avoid any potential privacy breaches [10]. To take use of the benefits of BCT in terms of decentralization and data immutability, the Estonian government is presently deploying a real-world blockchain-enabled e-Health system [72].

9. Appealing Solutions in Blockchain

In this section, we'll go through the key features and benefits of blockchain that make it a compelling alternative for tackling the concerns raised above in relation to IoT and Industry 4.0 applications.

9.1. Security. Confidentiality, integrity, and availability are the three core components of security. The BCT uses hash functions to link blocks, preserving their integrity and immutability by preventing data within blocks from being changed after they are linked. The conditions for availability are automatically met due to the distributed nature of blockchain, as data is always available. Permissioned blockchain systems keep data private by allowing users to see only the information to which they have been granted access through permissions. Not to mention the fact that transactions must be encrypted before being linked to the current ledger.

9.2. Auditability. Due to the fact that each peer owns a copy of the distributed ledger, they have access to all transaction records that are timestamped. Peers can use this transparency to check and verify transactions involving specific blockchain addresses. Due to the fact that blockchain addresses are not associated with real-world identities, they provide a degree of pseudoanonymity. While the records of a blockchain address cannot be traced back to its owner, individual blockchain addresses can be held accountable and inferences about their transactions drawn.

9.3. Decentralization. BCT is based on the idea of distributed and decentralized processing and storage. A blockchain eliminates the need for a centralized database, allowing users to conduct transactions without relying on a third party to keep track of data exchange or issue authorization. Multiple-to-

one traffic flows and single points of failure are avoided as a result.

9.4. Traceability. In terms of information monitoring and interchange, blockchain achieves a high level of harmony. By allowing for the easy sharing of historical data, this technology ensures transaction transparency and traceability. In IoT applications like smart manufacturing, tracing historical data is crucial. For example, by analyzing data, we may be able to identify crucial characteristics that influence the quality of a product. As a result of the enhancing approaches, the quality will improve. Filtering the data may reveal production faults and other difficulties.

9.5. Immutability. Due to the fact that peers agree on all new additions to the blockchain decentralized, the blockchain is impenetrable to censorship and nearly impossible to tamper with. Similarly, all previous entries on the blockchain are immutable, and an attacker would need to compromise a majority of the network's nodes to alter any historical data. Otherwise, any changes to the blockchain's contents are easily apparent.

10. BCT's Limitations

Blockchain technology holds enormous promise for the development of trustless, decentralized apps. It is not, however, without flaws. Blockchain technology is unsuitable for widespread adoption due to a number of impediments. The following list exemplifies the limitations of blockchain technology.

10.1. Consensus Mechanism. We know that a block on the blockchain can be created every ten minutes. This is due to the fact that each transaction is necessary to ensure that all blocks in the blockchain network reach a shared consensus. The back-and-forth interactions required to obtain consensus in a blockchain can consume significant time and resources, depending on the network's scale and the number of blocks or nodes involved.

10.2. Scalability. As with Bitcoin, blockchain technology is based on consensus mechanisms that need the transaction to be validated by each participating node. It places a cap on the amount of transactions that a blockchain network may process. As a result, Bitcoin was never intended to support the amount of transactions required by many other organizations. At the moment, Bitcoin has a transaction rate of seven per second.

10.3. Key Management. As previously stated, blockchain is built on cryptography, which requires the existence of distinct keys, such as public and private keys. Working with a private key raises the possibility of losing access to it. This happened a lot in Bitcoin's early days, when it was not worth much. Individuals would simply accumulate a large amount of Bitcoin and then misplace the key, which could be worth millions of dollars today.

10.4. Immutable. We are unable to make any changes to the immutable records. It is especially important if you want to keep a record's integrity and ensure that no one tampers with it. Immutability, on the other hand, has a disadvantage. If you want to make changes or revert to a previous configuration, we completely understand. For example, you may have completed a payment and now need to change it.

10.5. Limited Availability of Technical Talent and Lack of Awareness. Today, there are numerous developers that are capable of performing a wide variety of tasks in virtually any industry. However, the number of blockchain developers with specific expertise in blockchain technology is not quite as large. As a result, the scarcity of coders makes it difficult to create anything on the blockchain. While much has been said about blockchain, many people are ignorant of its inherent usefulness or how it may be applied in a variety of contexts.

11. Conclusion

We have explored the essential notions of IoT and Industry 4.0 ecosystems throughout this research paper, as well as the key issues and concerns related with their rise, most notably security and trust requirements. At the time, we underlined the importance of decentralizing such systems through the use of blockchains.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University, for funding this work through a general research group program under grant number G.R.P/326/42.

References

[1] L. Lamport, "The part-time parliament," *Concurrency: the-Works of Leslie Lamport*, pp. 277–317, 2019.

[2] R. Nair, S. Gupta, M. Soni, P. Kumar Shukla, and G. Dhiman, "An approach to minimize the energy consumption during blockchain transaction," *Materials Today: Proceedings*, 2020.

[3] M. K. Sahu, M. Ahirwar, and P. K. Shukla, "Improved malware detection technique using ensemble based classifier and graph theory," in *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, pp. 150–154, Ghaziabad, India, 2015.

[4] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services - the overview, challenges and recommendations from expert interviewees," *Technological Forecasting and Social Change*, vol. 158, p. 120166, 2020.

[5] C. S. Tang and L. P. Veelenturf, "The strategic role of logistics in the Industry 4.0 era," *Transportation Research Part E: Logistics and Transportation Review*, vol. 129, pp. 1–11, 2019.

[6] P. K. Shukla, S. Goyal, W. Rajesh, M. A. Rizvi, P. Sharma, and N. Tantubay, "Finding robust assailant using optimization functions (FiRAO-PG) in wireless sensor network," *Mathematical Problems in Engineering*, vol. 2015, 7 pages, 2015.

[7] G. Buchi, M. Cugno, and R. Castagnoli, "Smart factory performance and Industry 4.0," *Technological Forecasting and Social Change*, vol. 150, article 119790, 2020.

[8] S. Trinks and C. Felden, "Edge computing architecture to support real time analytic applications: a state-of-the-art within the application area of smart factory and Industry 4.0," in *2018 IEEE International Conference on Big Data (Big Data)*, pp. 2930–2939, Seattle, WA, USA, 2018.

[9] A. S. Rajawat, B. Pradeep, S. B. Goyal et al., "Securing 5G-IoT device connectivity and coverage using Boltzmann machine keys generation," *Mathematical Problems in Engineering*, vol. 2021, 10 pages, 2021.

[10] A. A. Pise, H. Vadapalli, and I. Sanders, "Relational reasoning using neural networks: a survey," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 29, pp. 237–258, 2021.

[11] C. Fuhrhop, J. Lyle, and S. Faily, "The webinos project," *21st international conference on World Wide Web*, pp. 259–262, 2012.

[12] J. A. Cardoso, F. T. Ishizu, J. T. de Lima, and J. de Souza Pinto, "Blockchain based mfa solution: the use of hydro raindrop mfa for information security on wordpress websites," *Brazilian journal of operations and production management*, vol. 16, no. 2, pp. 281–293, 2019.

[13] P. A. Audumbar and G. Hitesh, *High security optical watermark based on digital printing*, 2013.

[14] L. Peng, W. Feng, Y. Zheng, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: a survey," *Digital Communications and Networks*, vol. 7, no. 3, pp. 295–307, 2021.

[15] P. Sethi and S. R. Sarangi, "Internet of Things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, 25 pages, 2017.

[16] H. He, C. Maple, T. Watson et al., "The security challenges in the iot enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," in *2016 IEEE congress on evolutionary computation (CEC)*, pp. 1015–1021, Vancouver, BC, Canada, 2016.

[17] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for blockchain in manufacturing: "FabRec": a prototype for peer- to-peer network of manufacturing nodes," *Procedia Manufacturing*, vol. 26, pp. 1180–1192, 2018.

[18] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: a survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[19] A. A. P. H. Vadapalli and I. Sanders, "Estimation of learning affects experienced by learners: an approach using relational reasoning and adaptive mapping," *Wireless Communications and Mobile Computing*, vol. 2022, 14 pages, 2022.

[20] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[21] T. M. Fernandez-Carames and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cyber-secure Industry 4.0 smart factories," *Ieee Access*, vol. 7, pp. 45201–45218, 2019.

[22] B. Nour, K. Sharif, F. Li, and W. Yu, "Security and privacy challenges in information-centric wireless internet of things networks," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 35–45, 2020.

[23] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: techniques, applications, and challenges," in *2018 27th international conference on computer communication and networks (ICCCN)*, pp. 1–11, Hangzhou, China, 2018.

[24] M. Ammar, A. Haleem, M. Javaid, R. Walia, and S. Bahl, "Improving material quality management and manufacturing organizations system through Industry 4.0 technologies," *Materials Today: Proceedings*, vol. 45, pp. 5089–5096, 2021.

[25] D. Miller, "Blockchain and the internet of things in the industrial sector," *IT professional*, vol. 20, no. 3, pp. 15–18, 2018.

[26] J. A. Jaoude and R. G. Saade, "Blockchain applications–usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.

[27] D. W. E. Allen and C. Berg, "Blockchain governance: what we can learn from the economics of corporate governance," *Allen, DWE and Berg, C (Forthcoming)'Blockchain Governance: What can we Learn from the Economics of Corporate Governance*, 2020.

[28] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[29] G. Baruffaldi and H. Sternberg, *Chains in chains-logic and challenges of blockchains in supply chains*, 2018.

[30] S. Khan, R. Singh, and Kirti, "Critical factors for blockchain technology implementation: a supply chain perspective," *Journal of Industrial Integration and Management*, no. article 2150011, 2021.

[31] A. Pise, H. Vadapalli, and I. Sanders, "Facial emotion recognition using temporal relational network: an application to e-learning," *Multimedia Tools and Applications*, pp. 1–21, 2020.

[32] P. Pinheiro, R. Santos, and R. Barbosa, "Industry 4.0 multi-agent system based knowledge representation through blockchain," in *International Symposium on Ambient Intelligence*, pp. 331–337, Springer, 2018.

[33] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, no. article 21260, 2008.

[34] M. Swan, *Blockchain: Blueprint for a new economy*, O'Reilly Media, Inc, 2015.

[35] P. K. Shukla, P. K. Shukla, M. Bhatele et al., "A novel machine learning model to predict the staying time of international migrants," *International Journal on Artificial Intelligence Tools*, vol. 30, no. 2, article 2150002, 2021.

[36] S. Nakamoto, *Bitcoin: a peer-to-peer electronic cash system bitcoin: a peer-to-peer electronic cash system*, 2009, https://bitcoin.org/en/bitcoin-paper.

[37] P. K. Mannepalli, V. Richhariya, S. K. Gupta, P. K. Shukla, and P. K. Dutta, *Block Chain Based Robust Image Watermarking Using Edge Detection and Wavelet Transform*, 2021.

[38] S. Seebacher and R. Schuritz, *Blockchain–Just Another It Implementation? A Comparison of Blockchain and Interorganizational Information Systems*, 2019.

[39] R. van Hoek, "Unblocking the chain–findings from an executive workshop on blockchain in the supply chain," *Supply*

Chain Management: An International Journal, vol. 25, no. 2, pp. 255–261, 2019.

[40] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Management: An International Journal*, vol. 24, no. 1, pp. 62–84, 2019.

[41] A. Imeri, N. Agoulmine, C. Feltus, and D. Khadraoui, "Blockchain: analysis of the new technological components as opportunity to solve the trust issues in supply chain management," in *Intelligent Computing-Proceedings of the Computing Conference*, pp. 474–493, Cham, 2019.

[42] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchainenabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[43] R. van Hoek, "Exploring blockchain implementation in the supply chain," *International Journal of Operations & Production Management*, vol. 39, no. 6/7/8, pp. 829–859, 2019.

[44] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.

[45] F. Poszler, A.-C. Ritter, and I. Welpe, "Blockchain startups in the logistics industry: the technology´ s potential to disrupt business models and supply chains," in *Logistik im Wandel der Zeit–Von der Produktionssteuerung zu vernetzten Supply Chains*, pp. 567–584, Springer, 2019.

[46] D. J. Ghode, V. Yadav, R. Jain, and G. Soni, "Blockchain adoption in the supply chain: an appraisal on challenges," *Journal of Manufacturing Technology Management*, vol. 32, 2021.

[47] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proceedings of the 50th Hawaii international conference on system sciences*, Big Island, Hawaii, 2017.

[48] J. Mendling, I. Weber, W. V. Aalst et al., "Blockchains for business process management-challenges and opportunities," *ACM Transactions on Management Information Systems (TMIS)*, vol. 9, no. 1, pp. 1–16, 2018.

[49] L. Heilig, E. Lalla-Ruiz, and S. Vos, "Port-io: an integrative mobile cloud platform for real-time inter-terminal truck routing optimization," *Flexible Services and Manufacturing Journal*, vol. 29, no. 3, pp. 504–534, 2017.

[50] P. M. Block and S. K. Marcussen, *Blockchain technology and the implementation in the supply chain: occuring barriers: a multiple case study*, 2020.

[51] O. Gallay, K. Korpela, N. Tapio, and J. K. Nurminen, "A peer-to-peer platform for decentralized logistics," in *Proceedings of the Hamburg International Conference of Logistics (HICL)*, pp. 19–34, Berlin, 2017.

[52] G. Fridgen, S. Radszuwill, N. Urbach, and L. Utz, "Cross-organizational workflow management using blockchain technology: towards applicability, auditability, and automation," in *51st Annual Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 2018.

[53] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," 2018, https://arxiv.org/abs/1809.02702.

[54] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[55] S. Apte and N. Petrovsky, "Will blockchain technology revolutionize excipient supply chain management?," *Journal of Excipients and Food Chemicals*, vol. 7, no. 3, p. 910, 2016.

[56] D. C. de Leon, A. Q. Stalick, A. A. Jillepalli, M. A. Haney, and F. T. Sheldon, "Blockchain: properties and misconceptions," *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, 2017.

[57] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[58] M. Jović, E. Tijan, D. Žgaljić, and S. Aksentijević, "Improving maritime transport sustainability using blockchain-based information exchange," *Sustainability*, vol. 12, no. 21, article 8866, 2020.

[59] M. Henry, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[60] K. Francisco and D. Swanson, "The supply chain has no clothes: technology adoption of blockchain for supply chain transparency," *Logistics*, vol. 2, no. 1, p. 2, 2018.

[61] Y. Y. Hsieh, J. P. Vergne, and S. Wang, "The internal and external governance of blockchain-based organizations: evidence from cryptocurrencies," in *Bitcoin and beyond*, pp. 48–68, Routledge, 2017.

[62] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: anonymous distributed e-cash from bitcoin," in *2013 IEEE Symposium on Security and Privacy*, pp. 397–411, Berkeley, CA, USA, 2013.

[63] E. B. Sasson, A. Chiesa, C. Garman et al., "Zerocash: decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, pp. 459–474, Berkeley, CA, USA, 2014.

[64] L. Valenta and B. Rowan, "Blindcoin: blinded, accountable mixes for bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 112–126, Berlin, Heidelberg, 2015.

[65] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, pp. 87–91, Tiruchirappalli, India, 2019.

[66] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, *Uport: a platform for self-sovereign identity*, 2017, https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf.

[67] T. Kotka, C. Vargas, and K. Korjus, "Estonian e-residency: redefining the nation-state in the digital era," *University of Oxford Cyber Studies Programme working paper*, vol. 3, 2015.

[68] M. A. Khan and K. Salah, "Iot security: review, blockchain solutions, and open challenges," *Future generation computer systems*, vol. 82, pp. 395–411, 2018.

[69] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[70] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice*, vol. 77, pp. 167–181, 2015.

[71] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," 2018, https://arxiv.org/abs/1802.05050.

[72] T. Kalvet and A. Aaviksoo, *The development of eservices in an enlarged eu: egovernment and ehealth in estonia*, 2008.