electronics

MDPI

Article

Security Aspects of Blockchain Technology Intended for Industrial Applications

Sheikh Mohammad Idrees [1,*], Mariusz Nowostawski [1,*], Roshan Jameel [2] and Ashish Kumar Mourya [3]

[1] Department of Computer Science (IDI), Norwegian University of Science and Technology (NTNU), 2815 Gjøvik, Norway
[2] Department of Computer Science and Engineering, Jamia Hamdard, New Delhi 110062, India; roshanjameel_sch@jamiahamdard.ac.in
[3] Department of Computer Science and Engineering, Gautam Buddha University, Noida 201308, India; ashishmouryaict.gf@gbu.ac.in
* Correspondence: sheikh.m.idrees@ntnu.no (S.M.I.); mariusz.nowostawski@ntnu.no (M.N.)

Abstract: Blockchain technology plays a significant role in the industrial development. Many industries can potentially benefit from the innovations blockchain decentralization technology and privacy protocols offer with regard to securing, data access, auditing and managing transactions within digital platforms. Blockchain is based on distributed and secure decentralized protocols in which there is no single authority, and no single point of control; the data blocks are generated, added, and validated by the nodes of the network themselves. This article provides insights into the current developments within blockchain technology and explores its ability to revolutionize the multiple industrial application areas such as supply chain industry, Internet of Things (IoT), healthcare, governance, finance and manufacturing. It investigates and provides insights into the security issues and threats related to the blockchain implementations by assessing the research through a systematic literature review. This article proposes possible solutions in detail for enhancing the security of the blockchain for industrial applications along with significant directions for future explorations. The study further suggests how in recent years the adoption of blockchain technology by multiple industrial sectors has gained momentum while in the finance sector it is touching new heights day by day.

Keywords: blockchain; decentralized network; distributed ledger; supply chain; security

Citation: Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security Aspects of Blockchain Technology Intended for Industrial Applications. *Electronics* **2021**, *10*, 951. https://kdoi.org/10.3390/electronics10080951

Academic Editor: Juan M. Corchado

Received: 25 February 2021
Accepted: 11 April 2021
Published: 16 April 2021

1. Introduction

Blockchain, a distributed ledger based on cryptographic algorithms [1], was first described by Satoshi Nakamoto [2] in 2008 as a distributed peer-to-peer network for handling the first-ever decentralized digital currency "Bitcoin" that was later rated as the number one currency in terms of user adoption and widespread use [3]. The adoption of blockchain-based networks was held back because of its complex architecture; nevertheless, with time it attracted the attention of numerous industries globally, for example the financial industry, healthcare, logistics, manufacturing, energy, agriculture, and other industries [4]. The blockchain supports a complicated framework that amalgamates other prominent technologies such as peer-to-peer networking, distributed environment, decentralized architecture, cryptography, smart contracts, consensus mechanisms, and others [5]. Fundamentally, the blockchain is used to store time-stamped information during the transactions in data blocks, which are chronologically connected to each other to form a chain. Each block of data has a unique hash value, which is generated using a cryptographic algorithm that assures the integrity of the data. These blocks are connected to each other with these hash values like a linked list. Each block consists of a hash of the previous block along with its own, which helps in connecting the blocks forming the blockchain [6].

Blockchain technology has shown promising vision and has attracted various industries and researchers [7,8]. There are currently over 3000 blockchain-based cryptocurrencies available on the market, and this number continues to grow [9]. Blockchain technology has been applied in several application domains apart from digital currencies including the Internet of Things [10,11], healthcare [12,13], economics [14,15], software [16,17], and education, etc. The sudden spread of the COVID-19 pandemic in the past few months uncovered the constraints in the technology being used and promoted the adoption of blockchain in several domains such as contact tracing [18], patient information sharing [19], supply chain management [20], immigration processes, etc. The implementations of blockchain-based frameworks are now being utilized by almost every type of industry because of its ability to provide historical information of the transactions that is time stamped and immutable. Since the blockchain has no central controlling authority, all the participating nodes within the network have responsibility for maintaining it, for which purpose consensus mechanisms are applied to process and update the data over the blockchain. Furthermore, the smart contracts are used to allow complex rules and conditions within the transactions [21]. Smart contracts were first described back in 1994 [22], as protocol for digitally handling transactions by executing the terms and conditions of the contract, which eliminates the third-party requirement and minimizes the security issues. Basically, the contract acts as an agreement between the untrusted parties by enforcing the rules and regulations. In the blockchain network, these smart contracts are lines of code that run on the distributed network [23].

With the increasing worldwide adoption of blockchain technology, it is expected that its impact is going to be long lasting and the mode of internet behavior is going to change entirely [24,25]. It is being adopted at commercial level by providing breakthroughs to the IT industries for the improved efficiency and streamlined operations of businesses. Furthermore, large market players such as IBM, Google, Amazon, Microsoft, etc. have developed frameworks for providing the blockchain-based architecture as a service to the users to help in developing businesses and perform research on blockchain by themselves [26–29]. The blockchain provides a lot of new opportunities for applications in a decentralized manner with no intermediary, hence serving as a basis for more robust, failure-resistant and often more secure infrastructures. The blockchain has also, on the one hand, reduced fraud and improved financial accountability, on the other hand, introduced new cyberattacks on finances and helped in spreading ransomware [30,31]. Henceforward, it is significant to identify the existing work in this field by systematically analyzing the research done so far. In the past few years, hundreds of papers have been published in the domain of blockchain security. The first systematic review on Bitcoin was presented in [32], which elaborated the problems associated with the anonymity issues and analyzed the techniques for enhancing privacy and security. Subsequent work [33] investigated the existing loopholes in the Bitcoin implementation. In the survey paper [34] the risks associated with popular systems based on blockchain networks are reviewed and the vulnerabilities and attack cases happened so far are analyzed.

The main goal of this article is to emphasizee blockchain technology as a backbone for various applications, its innerworkings, components, security and future adoption aspects. The rest of the paper is organized as follows: a brief overview of blockchain technology and concepts is presented in Section 2. Section 3 outlines the traits related to the security in blockchain-based system. Section 4 reviews the techniques that can be applied to ensure security and privacy on blockchain. The deployment of blockchain-based applications is discussed in Section 5 followed by concluding remarks in Section 6.

2. Blockchain Technology

Nakamoto [2] documented the concepts and details of blockchain technology in 2008, which was then deployed in 2009 as the backbone for the first decentralized cryptocurrency named Bitcoin. Bitcoin allows the exchange of the digital currency over the internet in a decentralized peer-to-peer fashion. In Bitcoin, the blockchain is implemented as a

distributed ledger that is publicly available and hosted by a large number of volunteering hosts, called nodes. The ledger stores and verifies the transactional data over the network. The noteworthy feature provided by the blockchain in Bitcoin is its ability of the prevention of double spending in trades, as the entire network is responsible for the verification of the transactions instead of a central authority like traditional financial frameworks.

Basically, blockchain is a ledger that maintains a list of transactions in an immutable, append-only fashion that is growing with time and expanding the chain in a secure manner; the blocks within the blockchain are protected using cryptographic algorithms that impose the integrity of the transactional details [35]. The blockchain consists of permanent records that cannot be altered or tampered with, thus ensuring the integrity of the data. The data within the blockchain run through the distributed nodes within the network. The feature that makes the blockchain different from other technologies is that it timestamps the data records, providing a total order of blocks. A block consists of the hash value of the data stored in that block, along with the hash value of the previous block, which helps in connecting the chain of blocks. A new block can only be added to the existing blockchain after the successful completion of the consensus mechanism. This consensus mechanism has to control the permissions for entering into the chain, following the protocols for securely verifying the blocks and maintaining the consistency of the records at every node of the network. Hence, in conclusion it can be said that the blockchain is a distributed ledger that stores all the transactional data over a decentralized network in a secure and verifiable fashion. A blockchain-based framework can handle security issues such as unauthorized access of data/transactions, dependency on a third party or central authority and the unreliability of other participants.

2.1. Evolution of Blockchain

Bblockchain technology has developed and drastically evolved, and its evolution can be divided into stages as depicted in Figure 1 below. The first stage of the development is called as Blockchain 1.0, which consists of the public ledger for holding the cryptocurrencies over the distributed network. The next stage is Blockchain 2.0, which includes the trust management feature using smart contracts that manages itself with no involvement of any third parties. The third stage is Blockchain 3.0, which is the present and future of the technology and includes various application areas such as DeFe (decentralised finance), IoT, education, identity management, big data, Artificial Intelligence and healthcare, etc. [36].

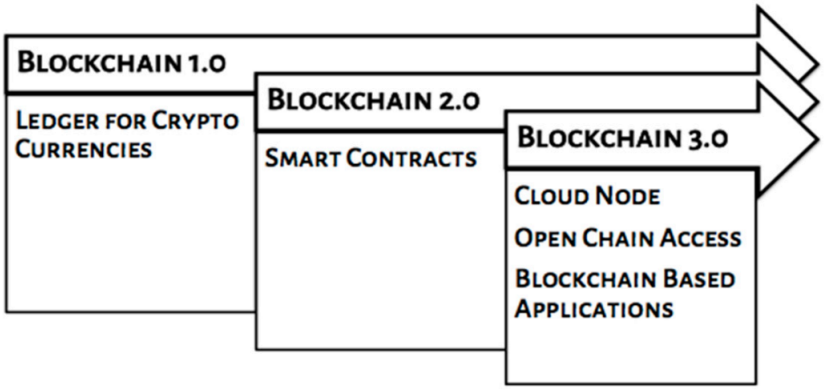

Figure 1. Stages of Blockchain Development.

Blockchain 1.0 began with the first digital currency, Bitcoin, which gave rise to the popularity of blockchain technology. The blockchain framework proposed for handling Bitcoin became famous as it solved various issues related to the data, such as authenticity, security and integrity, using the concepts of cryptography and hash functions [37]. The script used in the original first generation blockchain can be considered limited and purpose-built. It is only possible to express certain contractual agreements using that script. The innovation brought to the blockchain in the second generation is the generalization of

the scripting concept. Instead of offering only limited computational capability, the new generation smart contracts bring the power of a universal computation—that is, the smart contracts can express any algorithm that a universal computer can express. The concept of smart contracts allows the expression of complex contractual agreements, algorithms and workflows. Smart contracts allow the users to digitize any physical asset and map the real world logics to it using an expressive (universal) programming language. This improvement in the blockchain network made the technology more robust and flexible as the users can trace the real-world entities on the network that are secure and traceable. The third stage, Blockchain 3.0, is the current stage of blockchain that is still under development and has good scope for growth. This current generation is going to transform the way of internet based transactions facilitating Blockchain as a service [38–40].

2.2. Classification of Blockchain

While blockchain technology is continuously evolving in terms of its construction, access and verification, several application domains are adopting them. The blockchain can be classified in following three types that users can select from as per the requirements and scenario. These types of blockchain are different from each other but have similar basic characteristics like distributed and decentralized structure, peer-to-peer communication, consensus mechanisms, digital signatures and time stamping.

2.2.1. Public Blockchain

The network in such blockchain is distributed and publically available with no restrictions on reading the data from the network. However, in the context of writing, a public blockchain could be permissioned or permissionless. If it is permissionless then anyone can write into the network but if it is permissioned then only some specific nodes are authorized to have privileges to carry out new transactions (writing into the blockchain), verify the transactions by other nodes along with accessing the existing transactions (reading the blockchain). The proof-of-work consensus makes the public blockchain trustworthy. Such blockchain is considered to be safe because the number of nodes joining the network is usually high (as it is publicly available), and more nodes means a more distributed network. Furthermore, the records ledger is available to all the nodes that make the blockchain transparent. However, there are some flaws in such a blockchain, such as low processing speed because of the larger number of nodes within the network. Scalability and efficiency are also problem areas in such block chains, as proof-of-work consumes large amounts of time and energy in verifying requests. Bitcoin [2], Litecoin [41] and Ethereum [42] are the most common public blockchains available on the market today; a diagrammatic representation of such blockchains is shown in Figure 2 below, in which various types of nodes are connected with one another and share a common distributed network:

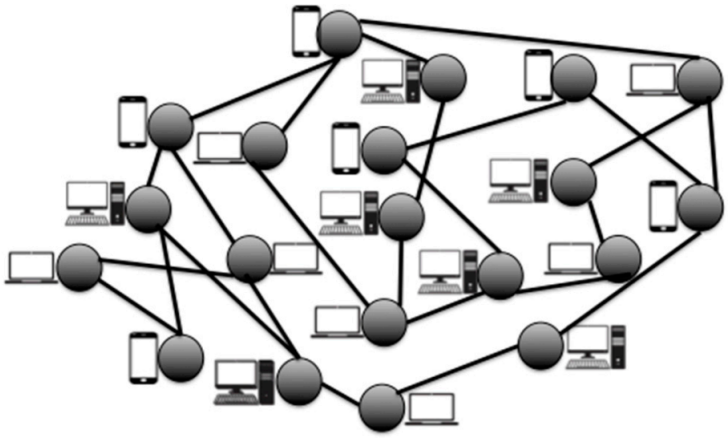

Figure 2. Public Blockchain.

2.2.2. Private Blockchain

The network of such a blockchain has some restrictions and works in a closed manner. Such networks are favored when an organization wants a blockchain with access and participation of some members. Additionally, no person can have the right to access the data or participate in transactions within the blockchain [43]. Such a blockchain is controlled by the organizations themselves and can be used for protecting the assets of customers; managing digital identities supply chains, etc. These blockchain networks could be permissioned or permissionless within the private group of people. Private blockchains are better than public blockchains in terms of computation speed because of the limited number of participating nodes—the consensus works fast—and scalability that allows the adjustment of the number of nodes on the basis of requirement. The shortcoming of such a blockchain is its maintenance, as the organization has to maintain the trust among the participating nodes because confidential information is at stake; also, it is easy to hack a chain with a smaller number of nodes. Therefore, organizations need to be incredibly careful while deciding upon the participating nodes. Some of the examples are Sawtooth [44], Corda [45], Fabric [46], etc. in which only the representative nodes have the right to make changes in the blockchain; a diagrammatic representation of such network is shown in Figure 3 below:

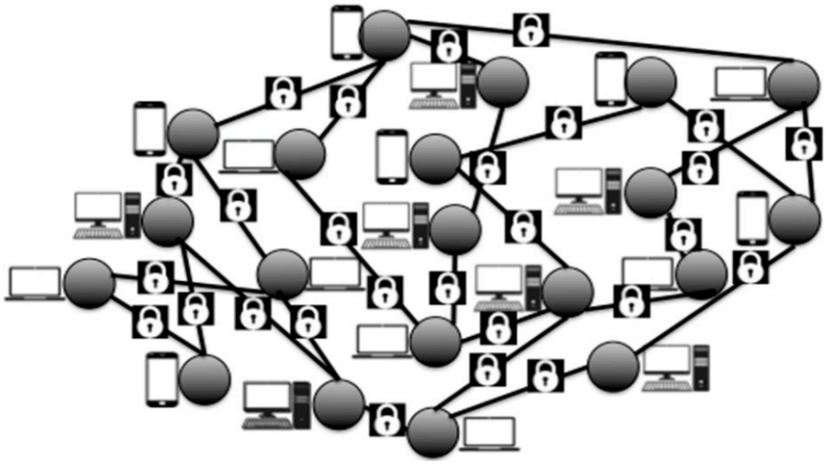

Figure 3. Private Blockchain.

2.2.3. Consortium Blockchain

Some nodes within the network are responsible for management in such a blockchain. Those nodes are the selected representatives of the participating organizations that are responsible for making the decisions within the network. These authoritative nodes control the consensus mechanisms and a few of them are also allowed to participate in the transactions. This blockchain is also called federated blockchain, and can be seen as a permissioned public blockchain in which anyone can read the data from the network but only the representative nodes have the authority to write into the network. The number of nodes in this blockchain is high, like public blockchain, while some restrictions are imposed on the nodes, like the private one. This type of blockchain is usually preferred in government and banking sectors, for example R3, Energy web foundation, etc. A diagrammatic representation of such blockchain is shown in Figure 4 below in which the representatives are depicted using blue nodes:

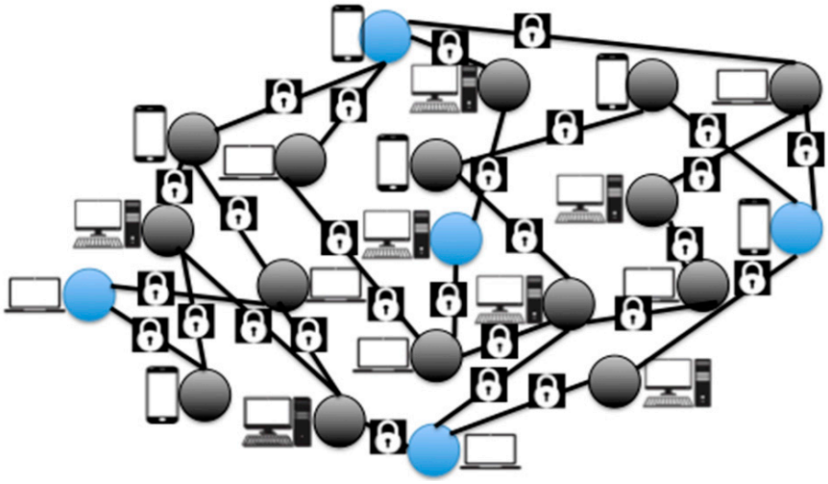

Figure 4. Consortium Blockchain.

2.3. Components and Working of Blockchain

A blockchain is a distributed network that is used to store the transactional data logs in a secure manner. The data within the blockchain is stored in the form of blocks that are chained together as shown in Figure 5 below. A block is generated after a fixed amount of time containing the information regarding the transactions that happened during that interval, which means the greater the number of transactions the larger the size of the blockchain. Whenever a transaction is requested, the mining process starts by broadcasting the request to all the nodes of the network for validation via consensus protocols. The block is added to the chain only after validation by all other nodes.

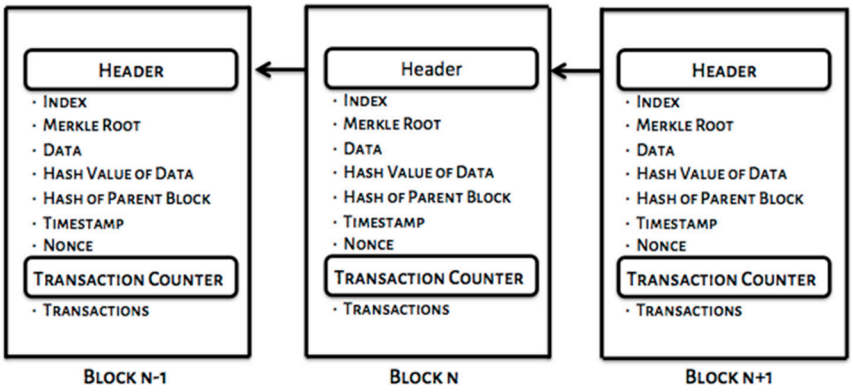

Figure 5. Connected Blocks in a Blockchain.

A blockchain can have several other components, but following are the necessary and basic ones that are required to be understood for getting better insight into the technology.

2.3.1. Block

A blockchain is a chain made of blocks, i.e., a block is the basic data structure of the network. A block can be divided into two parts as shown in Figure 6 below. The first part is the header, which consists of the index number, time stamp, nonce, data, hash values, etc. The blocks are generated by any of the nodes within the network, which is then verified by the entire network to be added to the chain. The first block of the blockchain does not have any value in the previous hash section, because it does not have any previous block, is called 'genesis block'. There are three types of blocks; 'main branch blocks' are the blocks that are added to the longest available blockchain within the network, 'side branch blocks' are the blocks that are not the part of longest chain or have the previous hash in some other chain and 'orphan blocks' whose previous blocks are not known to the present node.

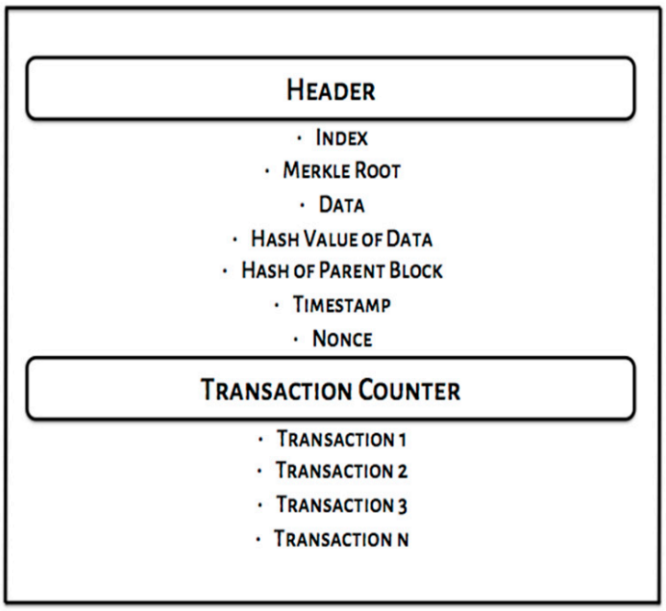

Figure 6. Block Structure.

2.3.2. Hash Pointer

Hash pointer consists of the hash of the data that is stored in the block. This hash is achieved using cryptographic hashing function (e.g., SHA256) and points towards the actual storage location of the data. It can be used to find out the integrity of the data. The hash pointers are responsible for the connectivity of the blocks in the blockchain, as a block is connected to the previous block using this hash value. Each block consists of the hash pointer to its data and data of previous block. The users verify these hashes publicly to assure that the data are tamper-proof. If a data are tampered with, the hash value will change not for that particular block, but for all the previous blocks up to the genesis block, which is not quite practically possible. Therefore, the hash pointer plays a vital role here in blockchain, in assuring the tamper resistance of the network.

2.3.3. Merkle Tree

It is a type of binary search tree with nodes connected to each other via hash pointers of the blocks, used to generate the blockchain. Whenever, more than one node is merged into single node, the Merkle tree creates a parent node for them that contains the hash of the nodes (those are merged) using a tree construction algorithm. The Merkle tree provides the capability of managing the data in a tamper-proof way, as it traverses down from the parent node towards the current node. For instance, if someone tries to alter the data of a node, the hash at the parent level are disturbed and the level above that, etc. up to the root, which makes it impossible for the attacker to change all the hashes at the time, and the tampering can be easily detected within the network.

2.3.4. Digital Signature

It uses cryptographic algorithms (public-private key cryptography, such as RSA or DSA) that can be used to establish the validity of the data within the network. It can also be used to verify the integrity of the data. In order to generate a digital signature, two keys are required a private key that is used by the generator to sign the document which is kept secret and the public key that is announced publicly, that can be used to verify that a certain private key has generated the digital signature. Then, a signing algorithm is required for actually putting a signature on the data using the available private key. Moreover, the signatures are verified using the verification algorithm. The digital signatures algorithms need to make sure that the signatures can be verified and cannot be forged.

2.3.5. Transactions

A block within the blockchain consists of the details of the transactions that happened in a particular time span. A transaction is one of the prominent parts of the block. It consists of the data that is being transmitted over the blockchain network along with the addresses of the sender and receiver. The sender applies the digital signature before sending it. The digital signature is applied on the hash value of the previous block. Next, the requested transaction is announced on the entire network, and the nodes calculate the current status of the node based on the data that they have so as to verify the transaction. The data of these transactions is time stamped—that means any change could be traced. Moreover, nothing can be changed in a blockchain; if a change is required a new transaction is requested instead of altering the existing one.

2.3.6. Consensus Mechanism

A blockchain network is distributed, and peer-to-peer connected, in which the transactional data are available to each and every node. The consensus mechanisms are imposed to ensure the security of the blockchain. Since each and every node owns a copy of the data, it is necessary to update it from time to time, and make sure that the data are consistent. The consensus mechanism is supposed to ensure that every node has an equal right and a new block can only be added to the network after these nodes agree to a consensus with proper participation and co-operation.

2.3.7. Inner Working of a Blockchain-Based System

A blockchain is a chain of blocks containing transactional data, connected using cryptographically generated hash pointers. Each of the blocks within the blockchain consists of data, timestamp of the data, generated hash value of data, hash value of previous block, etc. The blocks consist of information related to the transactions that happened in the given time-period. These transactions are made publicly available and are only carried out when the nodes of the network agree to via consensus mechanism that acts as a trust machine among the unknown parties. The transactions are also permanent, i.e., nobody can alter the data once entered the chain. The blockchain verifies itself on its own that makes it unique and trustworthy. A simple blockchain transaction can be carried out in following manner as shown in Figure 7 below:

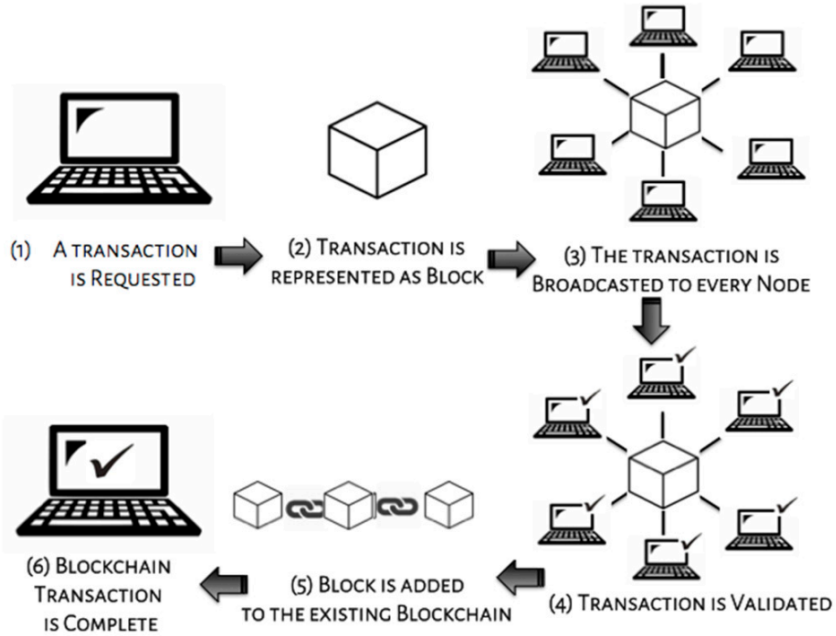

Figure 7. Working of Blockchain.

Blockchain technology supports distributed and decentralized networks, where all the nodes are equally important and have equal rights, and the data are stored in a secure fashion. Whenever a node requests a transaction, it is represented in the form of a block containing all the details regarding the transaction such as data, hash values, time stamp, etc. Then, this transaction is presented to every node of the network, which verifies the genuineness of the transaction by using the consensus mechanism. When the block is verified, it is added to the chain and the node that requested the transaction is notified that the transaction is complete. A blockchain is a huge chain that stores the transactions happening within the network so far in a distributed manner, which is what makes it better than other available platforms at ensuring security and fault tolerance.

3. Security Traits of Blockchain-Based Systems

The blockchain network is implemented in such a way that it assures data consistency and data provenance, tamperproof and auditability, it is pseudonymized, Distributed Denial of Service resistant, resistant to majority attacks, secure, private, and confidential. These properties make the blockchain network unique, transparent, and secure for handling online transactions. These security traits of the blockchain-based systems are described below.

3.1. Consistent Data

The consistency of the data in a blockchain network refers to the concept of ensuring the same copy of the data for every node of the network at every point of time. In the context of Bitcoin, the consistency of data is debatable as it is claimed to be weak as well as strong by different researchers [47,48]. A model for ensuring the data consistency is proposed for distributed networks (the Eventual Consistency Model) that provides a balance between the data's availability and consistency, which updates the data in a lazy manner and provides the readers with the updated values [49]. Eventual consistency does not mean that the data are made consistent straightaway; it only ensures that the data will be consistent eventually, with no restrictions on the time taken. However, such a model can provide stale data if the reader reads the node before the data update. In order to cope up with such situations, a consistency model must assure that no reading can be performed until all the nodes are updated, but the challenge here is cost with respect to availability. Therefore, the blockchain network stores the data transactions in blocks, and when a new request of transaction is received, the miner would add the request and start the proof of work mechanism, after which the block is sent to other nodes within the network to verify the transaction. Then, only that block is added to the blockchain and the other nodes accept it by making its hash the previous hash of their blocks.

3.2. Tamper-Resistant Data

The tamper-resistance of data ensures the ability of the data to resist any type of damage or interference in the data, system, or any product, intentionally or unintentionally. The blockchain is said to be tamper-resistant [50], which means that the information being stored or generated on the blocks of the blockchain can never be modified or tampered with in any case, neither while generating nor after the generation [51]. There could be two cases when the information can be tampered with; first, when the miner tries to modify the data or second, when the opponent tries to tamper it. The tampering can be controlled in a blockchain-based environment, as the transactions are secured using the hash function and digital signatures. Furthermore, the nodes of the network via mining verify the transaction. The first case is handled in such a situation, as when a miner would try to forge the signature or modify the content, it would not be possible, as he would not have the private key of the request generator. The second case when some opponent tries to tamper with the data would be handled the same way using the hash pointer and the cryptography. Were someone to try to change the data, the hashes of the other blocks would be affected, leading to a discrepancy in the hash values. Furthermore, the

blockchain-based distributed network ensures that every node has a copy of the data, and it would not be possible for the attacker to modify the content in each and every copy within the network [52]. Conclusively, it is impossible to tamper with the data within the blockchain network without being noticed.

3.3. Pseudonymized Network

The blockchain network guarantees the pseudonymized identity of the users [53]. The public keys of the users within the network are stored in the form of hashes, which are the addresses of the data [54]. The nodes within the network communicate with the framework using these hashes (public keys) while protecting the actual identities of the users, thus making the addresses of the user nodes as their pseudoidentity. Furthermore, a person can have more than one pseudoidentity. The concept of pseudonymized network in blockchain-based systems makes the system more private and confidential for the users in application domains such as healthcare, finance, insurances, news sharing, etc. [54–56].

3.4. Distributed Denial of Service Attacks-Resistant Network

The distributed denial of service attack on the blockchain-distributed network refers to the unavailability of the resources for the intended users. The attacker floods the host with an overloaded of requests for the resources that results in a shortage of the resources for the legitimate users. In the blockchain, the multiple nodes within the network that are distributed throughout the globe can conduct the DDoS attacks. The attackers take control over some nodes of the network by exploiting the vulnerabilities of the system. It is rather difficult to control such attacks by simply blocking the nodes one at a time. The race in such situations depends on the rate of handling such compromised systems within the network. However, it is still a major concern to handle the availability of the blockchain, as in such a way that the attacker could not knock out the network (partially/wholly). Therefore, decentralized peer-to-peer connections are the solution provided to maintain the blockchain, which ensures that the blockchain network processes the transactions even when a few of the nodes within the network fail. Additionally, for the attacker to totally block the blockchain, more than half of the network nodes would have to be compromised, which is practically not possible [57,58].

3.5. Secure and Confidential Data

The security of the data in the blockchain refers to the authorized access and safe storage, while confidentiality refers to the privacy provided to the sensitive data. The blockchain was first proposed for handling digital currencies; however, its scope is much larger than that. It can be utilized for contract management, copyright handling, and the digitization of several other domains such as healthcare, sales, etc. [59,60]. The confidentiality of the transactions is one of the most critical aspects of the blockchain-based distributed network. In order to keep the nodes secure and confidential, the pseudoidentities are used in the blockchain. The aim of the security within the blockchain is to make sure that there is no malicious or nonmalicious attack on the data [61]. It covers the execution of several tools, policies, and services to ensure that the network is safe. The aim of confidentiality is to make sure that the transactions are being made within the system without making the nodes recognizable, which disables the capability of the adversary to copy the profile of an authentic user. One of the best ways to assure the security of the network is to add the blocks to the chain that is longest (having maximum number of blocks), that makes it difficult for the attacker to hack (majority attack) [62].

4. Security and Privacy Methods Used in Blockchain-Based Systems

Based on literature studies, a thorough discussion of the techniques that can be used to improve the privacy and security of blockchain-based systems is presented in this section.

4.1. Anonymous Digital Signatures

The types of digital signatures that can offer secrecy for the one who uses them are called anonymous digital signatures. Two such signatures are "group signature" [63] and "ring signature" [64], which can be used in blockchain-based systems for enhanced security and privacy. In the group signature technique, a group is formed, and the members have their private keys and a shared public key. Any of the group members can sign by using its private key on behalf of the group in an anonymous way, which can be verified by the other members using a shared public key. The verification can only find out about the membership of the signer to that group and no other personal detail or identity. It also has a group manager who is responsible for handling the disputes (if any occur), revealing the signer's identity, adding, or removing group members, etc. Such an anonymous digital signature schemes can be used in consortium blockchain; as certain nodes in such blockchain are responsible for managing it, those can also be selected as group manager. The ring signature technique is another anonymous digital signature mechanism, which is like a group signature as any member can sign on behalf of the group and can be verified using other members' public key. However, there are two differences; first there is no group manager, thus the identity of the signer can never be revealed, and second the group can be formed by the users themselves, hence, can be applied on public blockchain.

4.2. Mixing

As we know by now that the users within the blockchain uses pseudonyms to hide their real identity, but there is a possibility that the addresses corresponding to these pseudoidentities can be revealed by tracking down the transactions performed. Therefore, in order to prevent such situations, a mixing technique was proposed. In mixing, the assets of the users are mixed with one another, which creates confusion within the network. However, the identities can be concealed with this mechanism, but the theft of digital assets/data cannot be protected. One such technique is called Mixcoin, which was first described in 2014 [65] in which the mixing was performed on cryptocurrencies like Bitcoin and others. In order to guard the digital assets from challengers/attackers, Mixcoin conceals the users by mixing the currency concurrently. Mixcoin delivers anonymity like conventional communication mixing techniques and also utilizes a mechanism for accountability to uncover theft of assets. CoinJoin is another technique that was proposed in 2013 [66] that was based on the concept of a joint payment in which if more than one user wants to make a transaction, they both make it jointly which reduces the chances in which one can trace the user's details. An extension of CoinJoin named CoinShuffle [67] eliminates the need of a third party for mixing of the transactions. It is based on a completely decentralized framework that abolishes the chances of theft and assures anonymity using Dissent [68], which is an anonymous communications protocol for a group. The cryptocurrency Dash [69,70], a fork of original Bitcoin cryptocurrency, has CoinJoin mixing built into the core of the protocol, and calls it PrivateSend. In Dash, users can automatically mix their wallets, increasing the anonymity of their funds and the support for mixing is part of the core protocol [71].

4.3. Homomorphic Encryption Algorithms

Homomorphic encryption is a cryptographic technique that has this special property of allowing the computations to be performed on the cipher text itself [72]. That means that in order to perform some operation on the data, it is not necessary to convert it into plaintext. Furthermore, it also ensures that when the same operation is performed on the same encrypted data after decryption, i.e., reverted to the plaintext, the result generated is the same as the result generated on the cipher text. Homomorphic cryptography can be easily used on the data in the blockchain without any kind of changes in the blockchain features, which assures the privacy of the data in the public blockchain and allows auditing and managing of the data in encrypted form only. Several cryptosystems already use this

technique [73,74]. An Ethereum smart contract also offers the privacy and security of the data on blockchain using Homomorphic encryption technique.

4.4. Secure Multiparty Computation Protocol

This is a model that has a protocol for multiple parties that help in carrying out some joint computations on the private data of those parties, and the output is provided without leaking anything about their data (maintaining the privacy). Initially the protocol was designed for two parties only [75], which was then generalized for multiple parties [76], and it allows sharing in a secretive manner. This generalized version has been used for many MPC mechanisms for applications such as voting, bidding, auction, etc. The MPC has been adopted by blockchain-based systems in the past few years for applications such as "multiparty lottery system" [77] that ensure fairness without any authority. Another such blockchain-based system working on SMPC named "Enigma" [78] offers a scheme for sharing the data secretly using the concept of a hash table in a distributed manner and utilizes the concepts of the blockchain externally for keeping a record of the network in a peer-to-peer decentralized manner. The framework of Enigma is quite like that of Bitcoin, which facilitates autonomous data transactions without any intermediary.

4.5. Attribute Based Encryption Algorithm

The Attribute Based Encryption (ABE) is a cryptographic algorithm that uses the attributes as regulatory factors for the cipher text, which was encrypted using the user's private key [79,80]. The text data can be decrypted only when the attributes of the decoders are matched with the encrypted data. The resistance from the collisions is the default property of this scheme that makes sure that the malicious or nonauthentic user can only access the data which can be decrypted from its private key. It was first proposed with one authority only, which has been extended a few times supporting multiple authoritative parties [81], arbitrary predicates [82], etc. The ABE is an influential technique but has not been applied to many applications because of the lack of knowledge regarding its concepts as well as its implementation details. It can be used for deployment on blockchain; by considering the tokens (privileges issued to the node) as tracking agents by the authorities that are responsible for the distribution of those tokens, these tokens should be considered as nontransferable. The implementation of this concept has still not been done on blockchain and remains an open challenge for researchers and coders.

4.6. Non Interactive Zero-Knowledge Proof System

Non Interactive Zero Knowledge (NIZK) is a powerful technology for cryptography that preserves the privacy of the system using the concept of zero-knowledge proofs [83]. The concept behind it is that a program can be executed with some unknown (private) input data and the output (public), which is generated without disclosing any other detail about the data or users; which means a user can prove about some claim to be true by proving it without revealing the actual data. A variant of NIZK system [84] suggested that a zero-knowledge computational knowledge could be achieved without any type of interactions among the users. The same concept can also be leveraged in a blockchain-based system as the data within the blocks are stored after encrypting—thus, a user can make the transaction by using the NIZK proof without revealing the actual data. An extension called ZoE (Zerocash over Ethereum), which is also available on GitHub, serves as a smart contract for the verification of the transactions while maintaining the privacy of the users [85,86].

5. Blockchain-Based Industrial Applications

Blockchain technology has a vast range of features that can be used for managing transactional records in any type of industry. The way it protects and secures the data with transparency and ensuring its integrity makes it a perfect choice for applications where sensitive data are involved. As the blockchain works on a distributed network platform,

every node within the network holds a copy of the data, which makes it difficult for the attacker to modify or tamper with it. Blockchain is changing the means of information sharing over the internet and is being adopted by several industries globally for conducting business transactions in a secure manner. Some of these applications are discussed in this paper and depicted in Figure 8 below:

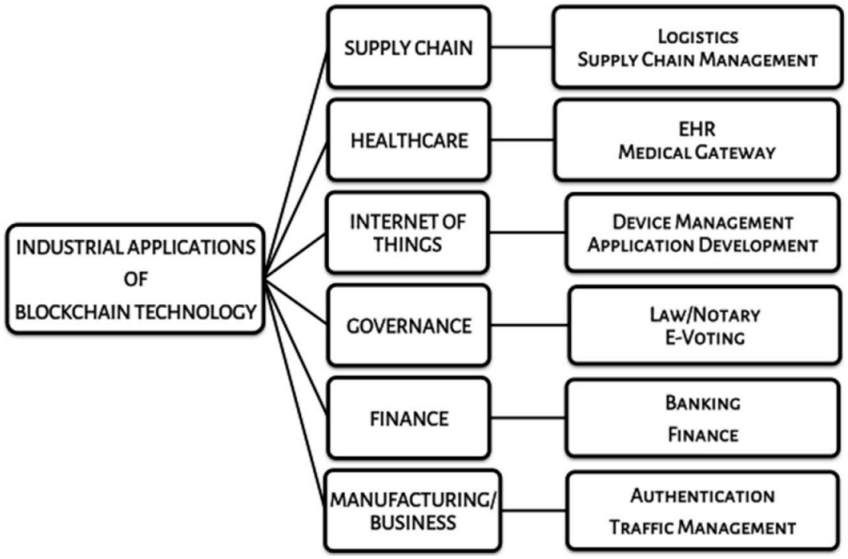

Figure 8. Some of the Industrial Applications of Blockchain Technology.

5.1. Supply Chain

Counterfeit products are one of the biggest issues for every type of industry, as they generate poor customer satisfaction rates, unreliability among stakeholders and downfall in the market economy [87]. The implementation of blockchain-based platforms would minimize the gap between the manufacturers and end users by making the entire process of development and supply chain transparent. Since the entries within the blockchain are tamper-proof and time stamped, it becomes difficult for the intruders to engage in foul play with the products. Currently, the reliance of the quality of the product is based on the documents provided by the manufacturer, but such documents can also be tampered. Implementing blockchain would ensure that the data are secure from any kind of theft, breach, or alteration by providing total traceability of the data along with time stamping. Maintaining the supply chain is an important aspect for every industry, and it is important to keep track of the products throughout the manufacturing and delivery. The traditional supply chains handle the complexities of the system, but they are slow and expensive, and cannot provide real time tracking of the system because of fragmented infrastructure at the customer and manufacturer ends [88].

Due to the limitations in technical knowledge, and the lack of skills and awareness, the implementation of blockchain in the field of supply chains is quite slow. These challenges are hindering the popularity and adoption of the blockchain by the organizations. Although there are several startups that are entirely based on blockchain technology, the field of supply chains is still evolving [89]. Currently IBM provides solutions for managing the supply chain via permissioned blockchain. There are several startups that aims to manage the supply chain via blockchain technology, some of the prominent ones are: Everledger, which tracks the provenance of the diamonds and luxury articles [90]; Openport [91], which helps in connecting carriers and shippers in a cost-effective and optimized manner; Skuchain, which works [92,93] on the concepts of cryptography used in Bitcoin to provide secure and visible management of supply chains at a global level; and Origin Trail, which provides the exchange of data among supply chains that are interconnected to one another. The blockchain can provide solutions to various challenges within the supply chain, as mentioned in Table 1 below:

Table 1. Blockchain for Supply Chain.

Challenges	Possible Solutions
Counterfeit products leading to poor customer satisfaction [37]	Tamper-proof records and transactions [37]
Difficult tracking of products [94]	Time stamping enabled tracking of products [94]
Authentication dependency on documents [95]	Keeping records in immutable ledger [95]
Difficult tracking in real time [96]	Decentralized–Distributed ledger for efficiency [96]

5.2. Healthcare

The healthcare industry is said to be an important industry for any country. Traditionally, healthcare data was stored and managed manually on paper, and then, with the emergence of cloud environments, the records were shifted to a central storage facility where only authentic and authorized users can access the data. The privacy and security of the healthcare data are a concern, as healthcare data consists of personal information that is confidential and vulnerable [97]. Blockchain technology has the ability to provide a transparent and secure platform for storing and analyzing medical data in an efficient manner [98]. The new era of healthcare (called smart healthcare) requires the remote and real time collection of heterogeneous data from a large number of patients via different sensors and wearable devices. These data are generated at high speed and need to be monitored, transmitted and handled in a secure way, as they is shared among different stakeholders like doctors, patients, path labs, chemists, etc. for better decision making to provide intelligent and smart diagnosis and treatment. However, there are some patients who are unwilling to share their personal details to a distributed network and some hospitals are also reluctant to share the exact details of the medications with the insurance companies—thus, the interoperability between the two organizations could become difficult [99]. Researchers have conducted studies on secure healthcare data management [100], healthcare records management [101] and healthcare image sharing [102], etc.

Currently the electronic health records are stored digitally, and the systems are centralized on a small scale. In order to make block chain technology successful, multiple funds providers, healthcare researchers and health ministries will have to work in alliance for the transformation of the healthcare sector, as it is so going to highly benefit the end users. There are several startups that aim to provide healthcare solutions via blockchain technology—some of the them are: Patientory, which manages the patient, healthcare institution and healthcare provider's data and allows the users to track history, insurance, bills, medications, etc.; Nebula Genomics, which is designing a platform based on blockchain that is going to provide the management of genomic data and will allow the buyers to obtain it in a secure manner; Doc.AI, which utilizes the blockchain concepts to obtain insights from the available medical data; and Medical-chain, which stores health records in the blockchain and helps in sharing them among several stakeholders along with supporting telemedicine facility [103,104]. The blockchain can provide solutions to various challenges within the healthcare industry besides diagnosis and treatment, as mentioned in Table 2 below:

Table 2. Blockchain for Healthcare.

Challenges	Possible Solutions
Sharing of Electronic Health Records (EHRs) [105]	Access control mechanisms [105]
Handling voluminous and complex data [106]	Immutable data records [106]
Inconsistency and heterogeneity in data [107]	Linking multiple data files to a single patient [107]
Data confidentiality and security [108]	Actual information is replaced by hash keys that point towards the location of data [108]
Counterfeit drugs [109]	Immutable and Time-Stamped transactions to track dealers and manufacturers [109]

5.3. Internet of Things (IoT)

With the emergence of smart devices and sensors, the IoT has become one of the most widely researched domains within the IT sector in the past few years. The number of IoT devices is continuously increasing and is estimated to reach half a trillion in the coming years. The IoT is not only limited to smart homes or devices but is expanding its implications in other areas and at a larger scale as well. In upcoming times, the internet is going to be denser and tightly connected. Therefore, it is necessary to have a network that is secure and safe, as its failure would cause the loss of confidential information, which is the most precious asset for organizations as well as individuals. The main areas of concern for the IoT domain are the transactions among the devices and servers and with the storages. Additionally, if the sustainable and smart world were to be made, the amalgamation of the blockchain with IoT with distributed network would provide safer data transactions. Moreover, there are no intermediaries in blockchain-based models, which would make the transactions faster and cheaper [110].

There are several types of attacks that can affect the overall performance of the IoT [111]. One such attack is an identity theft attack or impersonation attack, in which the hacker creates a number of fake anonymous identities, which he later attaches to any of the real users' identities, using malicious code during an unprotected data access or data transfer portal. Then, the hacker uses this anonymous identity to replace the real one and executes it as if he is the real end user. Thereby, he uses his tools to unlock the personal and sensitive information of the real user to his own advantage. Another such attack is a manipulation attack, a quite common attack viz. Man in the Middle (MITM), which is is generally used by a hacker with a fake public-key [112]. A similar type of manipulation attack could also be made by the injection of false data into the system of the prey user [113].In the cases of Distributed Denial of Services (DDoS) attack, the connectivity of services or access to a particular service (like sign-in or login) is strategically denied for a particular node or server or computer system on the grid, so that the hacker's objective is achieved by the delay during which DDoS was in execution [114,115]. Therefore, the Blockchain platform must have some stringent security protocols to guard the sensitive and personal information from being accessed by unauthorized users [116,117]. There are several organizations that offer IoT solutions via blockchain technology—some of the them are: Helium, which connects low power IoT devices to the internet through a blockchain network; ArcTouch, which develops software based on blockchain technology for connected IoT devices; NetObjex, which created a platform for IoT devices within the same network to connect and communicate with each other; XAGE, which provides a platform for industries like agriculture, utilities, transportation, etc. to securely access smart devices through blockchain connectivity. Some of the challenges of the IoT that can be addressed by blockchain are stated in Table 3 below:

Table 3. Blockchain for IoT.

Challenges	Possible Solutions
Maintenance of large number of devices [118]	Peer-to-Peer connection [118]
Attacks on central storages [119]	Data distributed among the nodes of the network [119]
Risk of forging [120]	Consensus mechanisms [120]

5.4. Governance

The government of any nation always has access to and control of the information about its citizens and government organizations. A blockchain-based framework could be used for integrating the services and infrastructures in a secure and decentralized manner. The blockchain could be used to provide facilities by the government such as voting, the handling of legal documents, marriage registration, contracts, etc. [121]. Some the projects have already been deployed using blockchain technology; for instance, the World Citizen Project [122], is a blockchain-based framework that handles citizens' data at global level. The internet is taking over lives in every aspect, from healthcare to insurance, from personal identity to professional credentials. Everything is on the internet, thus, making the security and confidentiality of the personal information is a concern for everyone (individuals as well as organizations). Subsequently, blockchain would be a smart choice as it provides the secure integration and transmission of data over the internet. Blockchain can be used to facilitate services such as handling property transactions [123], electronic voting [124], tax management [125] and electronic residents management [126], etc. However, all these facilities are available today but in a centralized framework that could be breached or hacked easily. There are a few organizations that provide digital governance via blockchain technology, some of them are as follows: Exonum [127] provides the online registry of land titles via blockchain network, Blockcerts [128] that allows the secure sharing and storing of academic certificates in the blockchain, Chromaway [129] utilizes blockchain technology for providing transparent property transactions. Conclusively, moving the governance towards the blockchain would assure the security and privacy of the data along with cost effectiveness in implementation, few challenges that can be addressed by blockchain are depicted in Table 4 below:

Table 4. Blockchain for Governance.

Challenges	Possible Solutions
Selling/Renting property [130]	Immutable and Time-Stamped transactions to track and manage assets [130]
Notary/Attestation [131]	Secure automated mechanisms following consensus protocols [131]
Citizen identity data management [132]	Actual information is replaced by hash keys that point towards the location of data [132]

5.5. Finance

The concept of blockchain was first introduced for supporting Bitcoin, which was the first digital currency ever. It is now making its way into every industry including banking and finance. Blockchain has applications such as asset management, stock markets, banking, etc. [133,134]. The banking sector undergoes thousands of transactions per minute that involve dealing with the money or other valuable assets, which makes blockchain a prime choice for this industry. The advantages of blockchain-based frameworks are more storage for data, less energy consumption, more speed and efficiency [135]. Blockchain can facilitate various areas of applications within finance, such as handling payments, managing loans, cryptocurrencies, etc. [136,137]. Blockchain promotes the working of the users on a transparent platform at a low cost of operations. Moreover, there is no need for

any third-party intervention, thus eliminating any vulnerabilities from the system. It can optimize the network by reducing the transactional costs. Furthermore, the blockchain can also be used for providing standard guidelines and regulations to the stakeholders for proper and transparent functioning of the industry. Some of the currently available finance solutions based on blockchain are: We.Trade [138], which provides a trading environment for enterprises and banks; Robinhood, which allows customers to invest their money in the stock market, cryptocurrencies and mutual funds for no cost via the blockchain network; Ripple, which provides the delivery of any currency to any part of the globe in no time; BitPay [139], which aims at increasing the usage of and popularizing cryptocurrencies by accepting payment in Bitcoins. Some of the challenges faced by the finance sector that blockchain can address are mentioned in Table 5 below:

Table 5. Blockchain for Finance.

Challenges	Possible Solutions
Digitization of currencies [140]	Distributed–Decentralized secure network with time-stamped immutable transactions [140]
Handling assets transmission [141]	Immutable and Time-Stamped transactions to track and manage assets [141]
Managing guidelines and regulations [140]	Secure automated mechanisms for implementing consensus protocols [140]

5.6. Manufacturing Business

The procedure of manufacturing something involves several aspects including proper planning, managing operations, managing assets, manufacturing intelligence, interactions between humans and machines, the optimization and monitoring of performance, and visibility. The privacy of data is one of the prominent concerns of the manufacturing and business domains. The systems and frameworks may face data breaches, leaks, theft, eavesdropping, unauthorized access, etc. With blockchain, all these concerns can be addressed as the network stores the records of the data in an immutable chain of blocks that are time stamped, secure, transparent, and managed using consensus mechanisms. The blockchain can be used for handling supply chains, verifying online payments, commercial marketing, etc. [142,143]. Moreover, vending machines can also be handled using blockchain for maintaining the log of availability of the products. Reputation systems can also be implemented using the blockchain network, which are used to rate the products or sites on the basis of customer experiences.

Data management is an important aspect for any type of business, and blockchain can be used for this purpose to handle the data in a decentralized and cost-effective way. Furthermore, bidding and contracts are also an aspect of the business domain that needs to be secured and transparent, which can be implemented using blockchain, which would eliminate third party/human involvement, hence reducing the chances of any discrepancy or unnecessary costs [144,145]. Currently Samsung and Maersk are using a blockchain-based distributed network to trace their international shipments. Moreover, the U.S Air Force and Navy also use blockchain for additive manufacturing and controlling 3D printers, respectively. Table 6 below gives a brief about the current challenges in the business/manufacturing industry and the blockchain-based solutions for the same.

Table 6. Blockchain for Manufacturing Business.

Challenges	Possible Solutions
Data breach, leak, theft, eavesdropping, unauthorized access [146]	Distributed secure network, time-stamped immutable ledger [146]
Human intervention [147]	No third-party involvement [147]
Physical transactions [147]	Integration with automatic verified billing, transparency [147]

6. Concluding Remarks

Blockchain technology that was first proposed as a backbone for implementation of the first digital currency and is now being deployed in various application domains because of its unique properties that assure the secure, transparent and confidential transactions of data in a peer-to-peer manner within a distributed network. The features such as time-stamped data, digital signatures, consensus mechanism, cryptographic hashing, etc. provided by the blockchain make it an extremely secure framework for handling data transactions without any intermediaries. Apart from this, the blockchain offers certain properties such as pseudoidentity, tamper-resistance, data consistency and confidentiality, etc. that assure the security and privacy of the data on the network, thus making the blockchain system more secure. A thorough analysis of blockchain and its contribution is presented in this paper.

This study highlighted the blockchain-based applications in several industrial domains, such as supply chains, where it can efficiently handle the marketing of counterfeit products by keeping track of the entire supply chain mechanism in a time-stamped and tamper-proof manner in real time. We have also discussed how blockchain can also be leveraged in the healthcare domain for securely sharing and confidentially storing Electronic Health Records (EHRs). The blockchain could also provide solutions for the challenges faced by the IoT industry by maintaining large numbers of devices in a distributed and peer-to-peer manner. The governance sector can also benefit from blockchain technology by providing secure mechanisms for the tracking and management of assets and identities. Manufacturing is a domain which consists of several steps such as planning, managing operations and assets, interacting with resources (human and mechanical), monitoring of performances, etc. making data security a big concern. The study suggests that blockchain technology can provide secure solutions to every aspect of the manufacturing process, from the management of supply chains, to verifying online payments, to commercial marketing. However, the sector in which blockchain technology has the most potential includes banking and finance. It is capable of facilitating several applications such as handling payments, managing loans, digitizing currencies, transmitting assets, etc. The smart contract can be employed in future for various processes such as documents' provenance, ownership rights, digital or physical assets or to stop fraud. Likewise, in other industries like the diamond industry, the digital ledger for diamond identification and transaction verification could enable more transparency to be brought into the very opaque diamond market. For the reasons that are discussed in this paper, it is clear that blockchain technology has huge potential to transform almost all industrial sectors. As such, making use of this reliable, trusted technology could contribute to the development of a safer, more secure, and more transparent working environment in all the industrial sectors.

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

Funding: The research received no external funds.

Acknowledgments: This work was carried out during the tenure of ERCIM—Alain Bensoussan Fellowship Program.

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

References

1. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain technologies: The foreseeable impact on society and industry. *Computer* **2017**, *50*, 18–28. [CrossRef]
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2019. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 February 2012).
3. Xie, S.; Zheng, Z.; Chen, W.; Wu, J.; Dai, H.-N.; Imran, M. Blockchain for cloud exchange: A survey. *Comput. Electr. Eng.* **2020**, *81*, 106526. [CrossRef]
4. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
5. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 6–10.
6. Lu, Y. Blockchain and the related issues: A review of current research topics. *J. Manag. Anal.* **2018**, *5*, 231–255. [CrossRef]
7. Kan, L.; Wei, Y.; Muhammad, A.H.; Siyuan, W.; Gao, L.C.; Kai, H. A multiple blockchains Architecture on Inter-Blockchain Communication. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 139–145.
8. Idrees, S.M.; Aijaz, I.; Agarwal, P.; Jameel, R. *Transforming Cybersecurity Solutions using Blockchain*; Blockchain Technologies; Springer: Singapore, 2021; pp. 165–183. [CrossRef]
9. CoinMarketCap. Cryptocurrency Market Capitalizations. 2017. Available online: https://coinmarketcap.com/ (accessed on 12 November 2020).
10. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]
11. Sun, J.; Yan, J.; Zhang, K.Z.K. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innov.* **2016**, *2*, 26. [CrossRef]
12. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A. A Case Study for Block Chain in Healthcare: Medrec Prototype for Electronic Health Records and Medicalresearch Data. 2016. Available online: https://www.media.mit.edu/publications/medrecwhitepaper/ (accessed on 12 November 2020).
13. Idrees, S.M.; Aijaz, I.; Agarwal, P.; Jameel, R. Exploring the Blockchain Technology: Issues, Applications and Research Potential. *Int. J. Online Biomed. Eng.* **2021**, in press.
14. Bylica, P.; Gleń, Ł.; Janiuk, P.; Skrzypczak, A.; Zawłocki, A. A Probabilisticnanopayment Scheme for Golem. 2015. Available online: http://golemproject.net/doc/GolemNanopayments.pdf (accessed on 12 October 2020).
15. Hurich, P. The virtual is real: An argument for characterizing bitcoins as private property. In *Banking & Finance Law Review*; Carswell Publishing: Toronto, ON, Canada, 2016; Volume 31, p. 573.
16. Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A.B.; Chen, S. The blockchain as a software connector. In Proceedings of the 13th Working IEEE/IFIP Conferenceon Software Architecture, Venice, Italy, 5–8 April 2016.
17. Czepluch, J.S.; Lollike, N.Z.; Malone, S.O. *The Use of Block Chain Technology in Different Application Domains*; The IT University of Copenhagen: Copenhagen, Denmark, 2015.
18. Idrees, S.M.; Nowostawski, M.; Jameel, R. Blockchain-based digital contact tracing apps for COVID-19 pandemic management: Issues, challenges, solutions, and future directions. *JMIR Med. Inform.* **2021**, *9*, e25245. [CrossRef]
19. Fusco, A.; Dicuonzo, G.; Dell'Atti, V.; Tatullo, M. Blockchain in healthcare: Insights on COVID-19. *Int. J. Environ. Res. Public Heal.* **2020**, *17*, 7167. [CrossRef]
20. Nandi, S.; Sarkis, J.; Hervani, A.A.; Helms, M.M. Redesigning supply chains using blockchain-enabled circular economy and COVID-19 experiences. *Sustain. Prod. Consum.* **2021**, *27*, 10–22. [CrossRef]
21. Chang, S.E.; Chen, Y.; Lu, M.; Luo, H.L. Development and Evaluation of a Smart Contract–Enabled Blockchain System for Home Care Service Innovation: Mixed Methods Study. *JMIR Med. Inform.* **2020**, *8*, e15472. [CrossRef]
22. Pan, X.; Pan, X.; Song, M.; Ai, B.; Ming, Y. Blockchain technology and enterprise operational capabilities: An empirical test. *Int. J. Inf. Manag.* **2020**, *52*, 101946. [CrossRef]
23. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
24. Peck, M.E. Blockchains: How they work and why they'll change the world. *IEEE Spectr.* **2017**, *54*, 26–35. [CrossRef]
25. Idrees, S.M.; Alam, M.A.; Agarwal, P.; Ansari, L. Effective Predictive Analytics and Modeling Based on Historical Data. In Proceedings of the Advances in Service-Oriented and Cloud Computing, Taormina, Italy, 15–17 September 2015; Springer: Singapore, 2016; pp. 552–564.
26. Available online: https://www.ibm.com/blockchain (accessed on 12 November 2020).
27. Available online: https://azure.microsoft.com/en-in/services/blockchain-service/#:~{}:text=Azure%20Blockchain%20Service%20is%20integrated%20with%20Microsoft%20serverless%20and%20codeless%20development%20tools.&text=Using%20the%20Visual%20Studio%20Code%20extension%2C%20write%2C%20test%2C%20debug,or%20to%20public%20blockchain%20networks (accessed on 12 October 2020).

28. Available online: https://cloud.google.com/customers/blockchain (accessed on 12 October 2020).
29. Available online: https://aws.amazon.com/managed-blockchain/#:~{}:text=Amazon%20Managed%20Blockchain%20is%20a%20fully%20managed%20service%20that%20allows,with%20just%20a%20few%20clicks.&text=Once%20your%20network%20is%20up,and%20maintain%20your%20blockchain%20network (accessed on 12 November 2020).
30. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R. Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence. *IEEE Trans. Emerg. Top. Comput.* **2017**, *8*, 341–351. [CrossRef]
31. Osanaiye, O.; Cai, H.; Choo, K.-K.R.; Dehghantanha, A.; Xu, Z.; Dlodlo, M. Ensemble based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP J. Wirel. Commun. Netw.* **2016**, *2016*, 1–10. [CrossRef]
32. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–20 May 2015; pp. 104–121.
33. Conti, M.; Kumar, E.S.; Lal, C.; Ruj, S. A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3416–3452. [CrossRef]
34. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
35. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.
36. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2084–2123. [CrossRef]
37. Idrees, S.M.; Nowostawski, M. Mobile phone based contact tracing applications for combating Covid-19 pandemic. *Biomed. J. Sci. Tech. Res.* **2020**, *32*, 25194–25197.
38. Samaniego, M.; Deters, R. December. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE International Conference on Inter-net of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 433–436.
39. Zheng, W.; Zheng, Z.; Chen, X.; Dai, K.; Li, P.; Chen, R. NutBaaS: A blockchain-as-a-service platform. *IEEE Access* **2019**, *7*, 134422–134433. [CrossRef]
40. Lu, Q.; Xu, X.; Liu, Y.; Weber, I.; Zhu, L.; Zhang, W. uBaaS: A unified blockchain as a service platform. *Future Gener. Comput. Syst.* **2019**, *101*, 564–575. [CrossRef]
41. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Perform. Eval. Rev.* **2014**, *42*, 34–37. [CrossRef]
42. Wood, G. Ethereum: A secure decent ralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
43. Satybaldy, A.; Nowostawski, M. Review of Techniques for Privacy-Preserving Blockchain Systems. In Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Taipei, Taiwan, 5 October 2020; pp. 1–9.
44. Olson, K.; Bowman, M.; Mitchell, J.; Amundson, S.; Middleton, D.; Montgomery, C. *Sawtooth: An Introduction*; The Linux Foundation: San Francisco, CA, USA, 2018.
45. Brown, R.G.; Carlyle, J.; Grigg, I.; Hearn, M. Corda: An introduction. *R3 CEV* **2016**, *1*, 15.
46. Cachin, C. Architecture of the hyperledger blockchain fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, USA, 25–29 July 2016; IBM Research: Zurich, Switzerland, 2016; Volume 310, pp. 28–32.
47. Vora, J.; Italiya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Hsiao, K.-F. Ensuring Privacy and Security in E- Health Records. In Proceedings of the 2018 International Conference on Computer, Information and Telecommunication Systems (CITS), Colmar, France, 11–13 July 2018; pp. 1–5.
48. Kumar, N.M.; Mallick, P.K. Blockchain technology for security issues and challenges in IoT. *Procedia Comput. Sci.* **2018**, *132*, 1815–1823. [CrossRef]
49. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]
50. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-resistant mobile health using blockchain technology. *JMIR mHealth uHealth* **2017**, *5*, e111. [CrossRef]
51. Nugent, T.; Upton, D.; Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* **2016**, *5*, 2541. [CrossRef]
52. Muzammal, M.; Qu, Q.; Nasrulin, B. Renovating blockchain with distributed databases: An open source system. *Futur. Gener. Comput. Syst.* **2019**, *90*, 105–117. [CrossRef]
53. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
54. Al Omar, A.; Alam Bhuiyan, Z.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Futur. Gener. Comput. Syst.* **2019**, *95*, 511–521. [CrossRef]
55. Islam, A.; Kader, F.; Islam, M.; Shin, S.Y. Newstradcoin: A Blockchain Based Privacy Preserving Secure NEWS Trading Network. In *Fintech with Artificial Intelligence, Big Data, and Blockchain*; Metzler, J.B., Ed.; Springer: Singapore, 2020; pp. 21–32.

56. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
57. Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of blockchain for mitigating the distributed denial of service at-tacks. *Secur. Priv.* **2020**, *3*, e96.
58. Rodrigues, B.; Bocek, T.; Lareida, A.; Hausheer, D.; Rafati, S.; Stiller, B. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. In Proceedings of the IFIP International Conference on Autonomous Infrastructure, Management and Security, Zurich, Switzerland, 10–13 June 2017; Springer: Cham, Switzerland, 2017; pp. 16–29.
59. Srivastava, G.; Crichigno, J.; Dhar, S. A Light and Secure Healthcare Blockchain for IoT Medical Devices. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, Canada, 5–8 May 2019; pp. 1–5.
60. Tapscott, D.; Tapscott, A. How blockchain will change organizations. *MIT Sloan Manag. Rev.* **2017**, *58*, 10–13.
61. Bashir, I. *Mastering Blockchain*; Packt Publishing Ltd.: Birmingham, UK, 2017.
62. Lin, I.C.; Liao, T.C. A survey of blockchain security issues and challenges. *IJ Netw. Secur.* **2017**, *19*, 653–659.
63. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Heal. Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]
64. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the OBD 2016: International Conference on Open and Big Data, Vienna, Austria, 22–24 August 2016; pp. 25–30.
65. Reijers, W.; Wuisman, I.; Mannan, M.; De Filippi, P.; Wray, C.; Rae-Looi, V.; Vélez, A.C.; Orgad, L. Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi* **2018**, 1–11. [CrossRef]
66. Tandon, A.; Dhir, A.; Islam, A.N.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
67. Alam, T. mHealth communication framework using blockchain and IoT technologies. *SSRN Electron. J.* **2020**, *9*. [CrossRef]
68. Wu, H.; Wolter, K.; Jiao, P.; Deng, Y.; Zhao, Y.; Xu, M. EEDTO: An energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing. *IEEE Int. Things J.* **2020**, *8*, 2163–2176. [CrossRef]
69. Mourya, A.K. Performance and Evaluation of Support Vector Machine and Artificial Neural Network over Heterogeneous Data. In Proceedings of the International Conference on Recent Trends in Image Processing and Pattern Recognition, Solapur, India, 21–22 December 2018; Springer: Singapore, 2018; pp. 584–595.
70. Duffield, E.; Diaz, D. Dash: A Privacy-Centric Crypto-Currency. Available online: https://pic.nanjilian.com/20180716/343445b5bc4b5e0cba45893a083b480d.pdf (accessed on 5 March 2021).
71. Amarasinghe, N.; Boyen, X.; McKague, M. A survey of anonymity of cryptocurrencies. In Proceedings of the Australasian Computer Science Week Multiconference, Sydeny, Australia, 29 January–2 February 2019; Association for Computing Machinery: New York, NY, USA, 2019; p. 2.
72. Parmar, P.V.; Padhar, S.B.; Patel, S.N.; Bhatt, N.I.; Jhaveri, R. Survey of various homomorphic encryption algorithms and schemes. *Int. J. Comput. Appl.* **2014**, *91*, 26–32. [CrossRef]
73. Razmjouei, P.; Kavousi-Fard, A.; Dabbaghjamanesh, M.; Jin, T.; Su, W. Ultra-lightweight mutual authentication in the vehicle based on smart contract blockchain: Case of MITM attack. *IEEE Sensors J.* **2020**, 1. [CrossRef]
74. Aijaz, I.; Idrees, S.M. 2020 Performance Evaluation of Multi-protocol Label Switching-Traffic Engineering Schemes. *EAI Endorsed Trans.* **2020**, *1*, 103–112. [CrossRef]
75. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. A distributed framework for detecting DDoS attacks in smart con-tract-based Blockchain-IoT systems by leveraging fog computing. *Trans. Emerg. Telecommun. Technol.* **2020**, e4112. [CrossRef]
76. Chen, M.; Tang, X.; Cheng, J.; Xiong, N.; Li, J.; Fan, D. A DDoS attack defense method based on blockchain for IoTs devices. In Proceedings of the International Conference on Artificial Intelligence and Security, Hohhot, China, 17–20 July 2020; Springer: Singapore, 2020; pp. 685–694.
77. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of block-chain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
78. Swan, M. *Blockchain: Blueprint for A New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
79. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), Oakland, CA, USA, 20–23 May 2007; pp. 321–334.
80. Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 53–70.
81. McMillan, R. Hacker Dreams Up Crypto Passport Using the Tech Behind Bitcoin. 2014. Available online: http://www.wired.com/2014/10/world_passport/ (accessed on 12 October 2020).
82. Daniel, D.; Ifejika Speranza, C. The Role of Blockchain in Documenting Land Users' Rights: The Canonical Case of Farmers in the Vernacular Land Market. *Front. Blockchain* **2020**, *3*, 19. [CrossRef]
83. Pokrovskaia, N. Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation. In Proceedings of the 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, Russia, 24–26 May 2017; pp. 709–712.
84. Shang, Q.; Price, A. A blockchain-based land titling project in the Republic of Georgia: Rebuilding public trust and lessons for future pilot projects. *Innov. Technol. Gov. Glob.* **2019**, *12*, 72–78. [CrossRef]

85. Rondelet, A.; Zajac, M. ZETH: On integrating Zerocash on Ethereum. *arXiv* **2019**, arXiv:1904.00905.
86. Available online: https://github.com/zcash-hackworks/babyzoe (accessed on 12 September 2020).
87. Maldonado, C.; Hume, E.C. Attitudes toward counterfeit products: An ethical perspective. *J. Leg. Ethical Regul. Issues* **2005**, *8*, 105.
88. Goodarzian, F.; Abraham, A.; Fathollahi-Fard, A.M. A biobjective home health care logistics considering the working time and route balancing: A self-adaptive social engineering optimizer. *J. Comput. Des. Eng.* **2021**, *8*, 452–474. [CrossRef]
89. Goodarzian, F.; Shishebori, D.; Nasseri, H.; Dadvar, F. A bi-objective production-distribution problem in a supply chain network under grey flexible conditions. *RAIRO Oper. Res.* **2021**, *55*, 1287. [CrossRef]
90. Everledger. 2017. Available online: https://www.everledger.io/ (accessed on 12 October 2020).
91. Available online: https://openport.com/ (accessed on 15 December 2020).
92. Allison, I. 2016 Skuchain: Here's How Blockchain Will save Global Trade a BillionDollars. Available online: http://www.ibtimes.co.uk/skuchain-heres-how-blockchain-will-save-global-trade-trillion-dollars-1540618 (accessed on 12 November 2020).
93. Tripathi, G.; Abdul Ahad, M.; Paiva, S. SMS: A Secure Healthcare Model for Smart Cities. *Electronics* **2020**, *9*, 1135. [CrossRef]
94. Lu, Y. Industry 4.0: A survey on technologies, applications and open research issues. *J. Ind. Inf. Integr.* **2017**, *6*, 1–10. [CrossRef]
95. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; Association for Computing Machinery: New York, NY, USA; p. 30.
96. Sun, G.; Dai, M.; Sun, J.; Yu, H. Voting-based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain. *IEEE Internet Things* **2020**, *8*, 6257–6272. [CrossRef]
97. Boucher, P. What If Blockchain Technology Revolutionized Voting? Available online: https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf (accessed on 5 March 2021).
98. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. 7 Privacy-Preserving. In *Data Protection and Privacy in Healthcare: Research and Innovations*; CRC Press: Boca Raton, FL, USA, 2021; p. 109.
99. Król, M.; Reñé, S.; Ascigil, O.; Psaras, I. ChainSoft: Collaborative Software Development Using Smart Contracts. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed, Munich, Germany, 7–12 June 2018; pp. 1–6.
100. Cocco, L.; Pinna, A.; Marchesi, M. Banking on blockchain: Costs savings thanks to the blockchain technology. *Futur. Internet* **2017**, *9*, 25. [CrossRef]
101. Cawrey, D. 37 Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet. 2014. Available online: http://www.coindesk.com/37coins-plans-worldwide-bitcoin-access-sms-basedwallet/ (accessed on 5 February 2021).
102. Rizzo, P. How Kipochi Is Taking Bitcoin into Africa. 2014. Available online: http://www.coindesk.com/kipochi-taking-bitcoin-africa/ (accessed on 5 February 2021).
103. Fathollahi-Fard, A.M.; Ahmadi, A.; Goodarzian, F.; Cheikhrouhou, N. A bi-objective home healthcare routing and scheduling problem considering patients' satisfaction in a fuzzy environment. *Appl. Soft Comput.* **2020**, *93*, 106385. [CrossRef]
104. Goodarzian, F.; Hosseini-Nasab, H.; Muñuzuri, J.; Fakhrzad, M.B. A multi-objective pharmaceutical supply chain network based on a robust fuzzy model: A comparison of meta-heuristics. *Appl. Soft Comput.* **2020**, *92*, 106331. [CrossRef]
105. Maslove, D.; Klein, J.; Brohman, K.; Martin, P. Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study. *JMIR Med. Inform.* **2018**, *6*, e11949. [CrossRef]
106. Linn, L.A.; Koo, M.B.; Ivan, D. Moving Toward a Blockchain-Based Method for the Secure Storage of Patient Records. In *Use of Blockchain for Healthcare and Research Workshop*; ONC/NIST: Gaithersburg, ML, USA, 2016.
107. Blough, D.; Ahamad, M.; Liu, L.; Chopra, P. MedVault: Ensuring Security and Privacy for Electronic Medical Records. NSF Cyber Trust Principal Investigators Meeting. 2008. Available online: http://www.cs.yale.edu/cybertrust08/posters/posters/158medvaultposterCT08.pdf (accessed on 20 December 2016).
108. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
109. Mettler, M. Blockchain technology in healthcare: E revolution starts here. In Proceedings of the 18th IEEE International Conference on e-Health Networking, Applications and Services, Ostrava, Czech Republic, 17–20 September 2018; Healthcom: Munich, Germany, 2016.
110. Ying, W.; Jia, S.; Du, W. Digital enablement of blockchain: Evidence from HNA group. *Int. J. Inf. Manag.* **2018**, *39*, 1–4.
111. Sirer, E.G. Bitcoin Guarantees Strong, not Eventual, Consistency. Available online: https://hackingdistributed.com/2016/03/01/bitcoin-guarantees-strong-not-eventual-consistency/ (accessed on 5 March 2021).
112. Wattenhofer, R. *The Science of the Blockchain*, 1st ed.; Inverted Forest Publishing: New York, NY, USA, 2016; ISBN 9781522751830.
113. Riadi, I.; Umar, R.; Busthomi, I. Optimasi Keamanan Autentikasi dari man in the middle attack (MiTM) menggunakan teknologi blockchain. *J. Inform. Eng. Educ. Technol.* **2020**, *2549*, 869X.
114. Vogels, W. Eventually consistent. *Commun. ACM* **2009**, *52*, 40–44. [CrossRef]
115. Ronald, L.; Shamir, R.A.; Tauman, Y. How to Leak a Secret. Advances in Cryptology—ASIACRYPT 2001. In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 December 2001; pp. 552–565.

116. Chaum, D.; van Heyst, E. Group Signatures. In Proceedings of the Advances in Cryptology: EUROCRYPT '91—Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May 1994; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265.
117. Bonneau, J.; Bonneau, J.; Narayanan, A.; Narayanan, A.; Miller, A.; Miller, A.; Clark, J.; Clark, J.; Kroll, J.A.; Kroll, J.A.; et al. Mixcoin: Anonymity for Bitcoin with Accountable Mixes. In Proceedings of the International Conference on Financial Cryptography and Data Security 2014, Christ Church, Barbados, 3–7 March 2014; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2014; pp. 486–504.
118. Stoykov, L.; Zhang, K.; Jacobsen, H.A. VIBES: Fast blockchain simulations for large-scale peer-to-peer networks: Demo. In Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos, Las Vegas, NV, USA, 5–11 December 2017; pp. 19–20.
119. Vora, J.; Nayyar, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J. BHEEM: A blockchain-based framework for securing electronic health records. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
120. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, X. Survey on blockchain for internet of things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
121. Maxwell, G. CoinJoin: Bitcoin Privacy for the Real World 2013. Available online: httpt://www.bitcointalk.org/index (accessed on 5 March 2021).
122. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In Proceedings of the 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 7–11 September 2014; pp. 345–364.
123. Corrigan-Gibbs, H.; Ford, B. Dissent: Accountable Anonymous Group Messaging. In Proceedings of the 17th ACM conference on Computer and Communications Security, New York, NY, USA, 12 October 2010; pp. 340–350.
124. Pichel, F. Blockchain for land administration. *GIM Int.* **2016**, *30*, 38–39.
125. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key Cryptosystems. *Commun. ACM* **2021**, *2*, 120–126.
126. Elgamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *Adv. Cryptol.* **2007**, 10–18. [CrossRef]
127. Yanovich, Y.; Ivashchenko, I.; Ostrovsky, A.; Shevchenko, A.; Sidorov, A. Exonum: Byzantine Fault Tolerant Protocol for Blockchains 2018. Available online: http://www.bitfury.com/ (accessed on 5 March 2021).
128. BlockCerts. The Open Initiative for Blockchain Certificates. Available online: http://www.blockcerts.org/ (accessed on 15 November 2017).
129. Mizrahi, A. A Blockchain-Based Property Ownership Recording System, ChromaWay. 2016. Available online: https://static1.squarespace.com/static/5e26f18cd5824c7138a9118b/t/5e3c1c7d6d5ff061da34da80/1580997757765/A-blockchain-based-property-registry.pdf (accessed on 5 February 2021).
130. Dewan, S.; Singh, L. Use of blockchain in designing smart city. *Smart Sustain. Built Environ.* **2020**, *9*, 695–709. [CrossRef]
131. Sullivan, C.; Burger, E. E-residency and blockchain. *Comput. Law Secur. Rev.* **2017**, *33*, 470–481. [CrossRef]
132. Dunphy, P.; Petitcolas, F.A. A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
133. Mourya, A.K.; Singh, P. Predictive Modeling and Sentiment Classification of Social Media Through Extreme Learning Machine. In *Proceedings of the ICETIT 2019*; Springer: Cham, Switzerland, 2020; pp. 356–363.
134. Yao, A.C. Protocols for Secure Computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Washington, DC, USA, 3–5 November 1982; pp. 160–164.
135. Goldreich, O.; Micali, S.; Wigderson, A. *How to Play Any Mental Game or a Completeness Theorem for Protocols with Honest Majority*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 218–229. ISBN 9781450372664.
136. Andrychowicz, M.; Dziembowski, S.; Malinowski, D.; Mazurek, L. Secure Multiparty Computations on Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; pp. 443–458.
137. Zyskind, G.; Nathan, O.; Pentland, A. Enigma: Decentralized computation platform with guaranteed privacy. *arXiv* **2015**, arXiv:1506.03471.
138. Kim, H.M.; Lee, H.H. Asset specificity and capability of e-Trade performance: Evidence from Korea. *J. Korea Trade* **2016**, *20*, 2–20. [CrossRef]
139. Available online: http://d.ibtimes.co.uk/en/full/1433561/bitcoin-merchants-mainstream-bitpay-cryptocurrency.jpg?w=736 (accessed on 5 March 2021).
140. Nguyen, Q.K. Blockchain_A _nancial technology for future sustainable development. In Proceedings of the 3rd International Conference on Green Technology and Sustainable Development (GTSD), Kaohsiung, Taiwan, 24–25 November 2016; pp. 51–54.
141. Singh, S.; Singh, N. Blockchain: Future of _nancial and cyber security. In Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–17 December 2016; pp. 463–467.

142. Chase, M. *Multi-authority Attribute Based Encryption*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 515–534.
143. Garg, S.; Garg, S.; Gentry, C.; Gentry, C.; Halevi, S.; Halevi, S.; Sahai, A.; Sahai, A.; Waters, B.; Waters, B. Attribute-based encryption for circuits from multilinear maps. *Comput. Vision* **2013**, 479–499.
144. Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proof systems. *SIAM J. Comput.* **1989**, *18*, 186–208. [CrossRef]
145. Blum, M.; Feldman, P.; Micali, S. *Non-Interactive Zero-Knowledge and Its Applications*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 103–112. ISBN 9781450372664.
146. Meeuw, A.; Schopfer, S.; Wortmann, F. Experimental bandwidth benchmarking for P2P markets in blockchain managed microgrids. *Energy Procedia* **2019**, *159*, 370–375. [CrossRef]
147. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]