applied sciences

Review

Distributed Ledger Technologies and Their Applications: A Review

Reza Soltani [1], Marzia Zaman [2], Rohit Joshi [3] and Srinivas Sampalli [1,*]

[1] Faculty of Computer Science, Dalhousie University, Halifax, NS B3H 1W5, Canada
[2] TeleAI Corporation, Ottawa, ON K2E 7V7, Canada
[3] Cistel Technology, Ottawa, ON K23 7V7, Canada
* Correspondence: srini@cs.dal.ca

Abstract: With the success of Bitcoin and the introduction of different uses of Blockchain, such as smart contracts in Ethereum, many researchers and industries have turned their attention to applications that use this technology. In response to the advantages and disadvantages of Blockchain, similar technologies have emerged with alterations to the original structure. Distributed ledger technology (DLT) is a generalized distributed technology encompassing these new variants. Several studies have examined the challenges and applications of Blockchain technology. This article explores the possibilities of using different DLTs to solve traditional distributed computing problems based on their advantages and disadvantages. In this paper, we provide an overview and comparison of different DLTs, such as Hashgraph, Tangle, Blockchains, Side Chain and Holochain. The main objective of the article is to examine whether distributed ledger technologies can replace traditional computational methods in other areas instead of traditional methods. Based on the primary keywords, we conducted a systematic review of more than 200 articles. Based on the data extracted from articles related to the use of DLT, we conclude that that DLTs can complement other methods, but cannot completely replace them. Furthermore, several DLTs such as Sidechain, Holochain and Hashgraph are still in their infancy, and we foresee much research work in this area in the coming years.

Keywords: blockchain technology; distributed ledger technology (DLT); applications of DLT

Citation: Soltani, R.; Zaman, M.; Joshi, R.; Sampalli, S. Distributed Ledger Technologies and Their Applications: A Review. *Appl. Sci.* **2022**, *12*, 7898. https://doi.org/10.3390/app12157898

Academic Editors: Hossein Hassani and Nadejda Komendantova

Received: 11 July 2022
Accepted: 2 August 2022
Published: 6 August 2022

1. Introduction

A whole new field of research was created with Satoshi Nakamoto's introduction of Blockchain technology in 2009 [1]. The use of Blockchain technology has been proposed in numerous areas by researchers [2]. This technology has created a new space for various applications by providing a distributed platform along with encryption algorithms. In the early days, this type of technology was used to create a platform for financial transactions, and its main goal was to create a system that could solve the problem of double spending. In addition to solving problems traditionally solved with distributed methods, this system was gradually used for other applications due to its high security on a distributed platform. This technology can be used in several ways, such as improving the way elections are conducted [3], storage and security of medical records [4–7] and supply chain management [8,9]. In systems that used to rely on third-party solutions, this technology allows for increased transparency, traceability and immutability of records in a trusted distributed manner [10]. Blockchain technology is still in its infancy and is not yet mature enough to replace traditional solutions in areas such as supply chain management, healthcare and insurance. Furthermore, Blockchain technology has several advantages and disadvantages that have resulted in the evolution of new trusted distributed technologies with different structures that can be encapsulated into a general technology called distributed ledger technology (DLT).

Many researchers have proposed new ideas and solutions by exploring the use of this technology in other fields [10]. In addition, there are numerous articles that have collected information about different methods of using this technology in various fields [10–37]. In some of these articles, the technical issues of this technology have been discussed, along with its advantages and disadvantages. Others examine how to use these technologies in a specific field, including the DLT solutions applicable to that field.

A critical analysis of the differences between the different technologies, as well as the efficiency of this technology, is necessary due to the rapid growth of this technology and the interest of industries and researchers in investigating and better utilizing this technology in solving problems that were traditionally solved by other distributed methods.

Each new idea presented in the area should be analyzed according to its unique characteristics, so that a large portion of the required information can be comprehensively presented in a paper. To determine the importance of a particular technology, it is necessary to examine its most important features according to the specific characteristics of the field and to determine its advantages over traditional methods according to the characteristics of the problem. For example, issues such as voting require high accuracy and security, and issues such as financial processing require high scalability in addition to high security. Whether these technologies can be applied in real-world scenarios is a question that needs to be answered. It appears that most of the previous articles only discuss the technical aspects of these technologies or only one specific application area. In this article, we have attempted to collect all of them in an up-to-date manner and to analyze the differences, technical characteristics and potential of each in different fields.

This paper provides an overview and comparison between different DLTs and their applications. Current survey papers on DLTs are mostly Blockchain-specific, with a focus on their applications and challenges. Table 1 shows a comparison of our survey paper with others.

Table 1. Comparison of current survey papers in DLT research.

Research Area	Applications	Focus	Articles
Blockchain	Partially focused	Mostly on Blockchain only	[11–16]
Application of Blockchain	Focused on Blockchain tech	Partially focused	[17–23]
Tangle	IoT Networks	Only on IOTA	[24]
Hashgraph	Financial	Proposed method only	[25]
Sidechain	Event-oriented application	Proposed method only	[26,27]
Survey paper on DLT	Partially covers some applications	Includes several technologies	[28–38]
This Paper	Covers well-known applications	Covers several challenges and technical details	

Many articles have investigated only one aspect of this technology [10–37] or have addressed its applications only in one field. In this article, we have compared the technologies according to the requirements of different environments, their advantages, disadvantages and differences from the traditional methods that were used.

After analyzing the various features of these technologies and examining the applications in various scenarios, such as voting, healthcare, IoT networks, etc., it has been concluded that this technology cannot fully replace traditional methods. In general, these technologies, except Tangle, which works specifically with IoT devices, are in the early stages of development, and the problems of these technologies still need to be addressed. We can mention the use of combined methods with traditional methods to solve these problems or presenting new ideas to change the current technology. As this technology grows extremely fast and gains attention from the scientific and industrial communities, it is necessary to update the reviews on progress of this technology.

1.1. Methodology

The first step was to determine the research questions from the article's objective, which is to provide an overview of the latest distributed ledger technologies, their applications, and how they can be applied to problems traditionally addressed with other methodologies. Table 2 presents the research questions that were formulated.

Table 2. Research questions.

Question	Description
RQ1: What technologies are included in DLT?	DLT is a general term that has been used for technologies with difference in structure, namely, their topology, consensus algorithm, but similar in two features, namely, distributed nature and linked based recording data.
RQ2: What are the advantages and disadvantages of each subcategory of DLT?	Technical details on each technology and their comparison.
RQ3: What is the application of each DLT?	Discovering the main applications of each DLT by review of their literature.
RQ4 Can DLT technologies replace traditional methods in different areas?	One of the main purposes of this paper is to investigate the feasibility of DLTs in replacing traditional solutions in various areas.

Comparisons between their subcategories must be updated as DLTs grows rapidly. This article evaluates five different categories of this technology based on review of articles found in reputable scientific databases such as IEEE, Elsevier, and ACM.

We first identified and reviewed 27 primary survey papers by searching keywords as shown in Table 3.

Table 3. Keywords for review papers.

Keywords	Combination of This Keyword
Blockchain	Blockchain Technology, Blockchain survey, Blockchain review, Application of Blockchain, Application of Blockchain review
Distributed ledger technologies (DLT)	DLT, DLT review, DLT survey, Distributed ledger technologies review, Distributed ledger technologies survey, application of DLT, application of Distributed ledger technologies.

After reviewing other survey papers, we identified all the subsets of this technology by searching for keywords in Table 4.

Table 4. Keywords for DLT related technologies.

Keywords	Combination of This Keyword
Blockchain	Blockchain Technology, Blockchain, Application of Blockchain, Blockchain Related Technologies, Future of Blockchain, Blockchain Alternatives, Blockchain issues, advantages of Blockchain, Scalability Blockchain, Security Blockchain
Distributed ledger technologies (DLT)	DLT, Distributed ledger technologies, application of DLT, application of Distributed ledger technologies, DLT scalability, DLT security, Transactions DLT.
Consensus algorithm	Consensus Algorithm DLT, Proof of Work, Proof of Stake, Proof of Burn, Delegated Proof of Stake, Byzantine Fault Tolerance, Practical Byzantine Fault Tolerance, SIEVE,
Smart contract	Smart contract, DLT Smart contract, Application Smart Contract
Novel	Novel DLT,

By utilizing keywords such as Sidechain, Holochain, Blockchain, Ethereum, Bitcoin, IOTA, Tangle and Hashgraph while searching for recent articles on social networks such as Twitter, and websites, and checking in scientific databases such as IEEE, Elsevier, ACM and finally with the help of the Google Scholar search engine for finding most of the subcategories in DLT we added keywords related to the desired application environment, such as healthcare, voting, etc., to the current keywords. A total of 214 papers have been reviewed, and 85 selected primary papers have been added after reviewing abstracts, introductions, methodologies and conclusions.

1.2. Organization of the Paper

Section 2 presents a review of distributed ledger technology with a focus on their advantages and disadvantages. Section 3 discusses the applications of these technologies in different areas Section 4 presents concluding remarks.

2. Distributed Ledger Technology

DLT is a general protocol and structure for recording data in a distributed and secure fashion. It emphasizes the presence of a system that is controlled by a distributed network and has no central control. DLT secures data through cryptography and distributes them across the network for storage. This technology is designed to establish trust between parties that do not trust each other. Multiple copies of each record are kept and are linked together by a cryptographic algorithm, and all copies of data must be compromised for the intrusion to be successful [39].

This technology is divided into different subcategories according to the structure created to keep the data record. Each of these subcategories includes a wide range of technologies that have their own advantages and disadvantages.

This article discusses five sub-technologies under the distributed ledger technology: Blockchain, Tangle, Hashgraph, Side-chains and Holochain. Each of these technologies distributes trust between users and records information, but the manner in which they retain data and the consensus algorithm they use to ensure the accuracy of procedures are different. In summary, consensus algorithms can be used to make all the nodes in the network agree on the records they are storing [40]. Due to the differences between consensus algorithms, each technology has unique features as well as advantages and disadvantages.

2.1. Blockchain

Blockchain technology was first used to solve the problem of double spending [1]. Cryptographic algorithms and distributed ledgers form the basis of this technology. It consists of a chain of blocks linked to each other, with each block containing numbers of transactions merged to the previous block and linked to previous transactions. As a general rule, an initial block is formed, and then new transactions result in a new block that is linked by keeping the previous block's hash data. Moreover, these blocks are widely distributed within a distributed network without central management, making it difficult to easily add a fake block or question a block's existence. With these features, transactions are immutable; therefore, data can be recorded on a Blockchain network without any changes or the ability to track the record history [41]. In addition, each Blockchain has a unique consensus algorithm for agreeing on a new block to prevent attacks such as Sybil attacks [14]. The selection of a trusted entity to make a new block in Blockchain can be based on algorithms such as proof of work [42], proof of burn [43] and proof of stake [44].

Distributed databases and cryptographic algorithms are combined in Blockchain technology to reliably store transactions [45]. Data integrity can be guaranteed by this technology without a centralized entity managing or controlling it. All transactions made with Blockchain technology are placed into a block and verified by all the nodes. Additionally, a hash of the transaction will be recorded in the block, and a hash from the previous block will be recorded to provide a link [46]. Therefore, if one transaction in a block changes, the newly calculated hash will differ from the hash already registered, and the block will become invalid [46].

The structure of the Blockchain is multiple blocks chained together in a timestamped chronological manner. Blocks generally consist of three parts: data, hash for the current block, and hash for the previous block that is included in the new block to determine the order of the blocks. The genesis block will be the first block created, and the next block will keep the hash of the genesis block with its own data and hash. A hash is a mathematical function that changes data into a short, arbitrary size, array of data [47]. The hash function produces results that cannot be decrypted and should be unique so that every dataset has its own fingerprint. By changing data on a block, the hash will no longer be the same, and if the hash has also been altered, the chain of the subsequent block cannot be linked due to the difference between the hash recorded in the next block and the current block. Therefore, the following chain will be considered invalid [46]. Figure 1 illustrates the Blockchain and the block, which consists of data, their current hash and the previous block hash. Any tampering with a block will result in the invalidity of the block and the following chain of blocks.

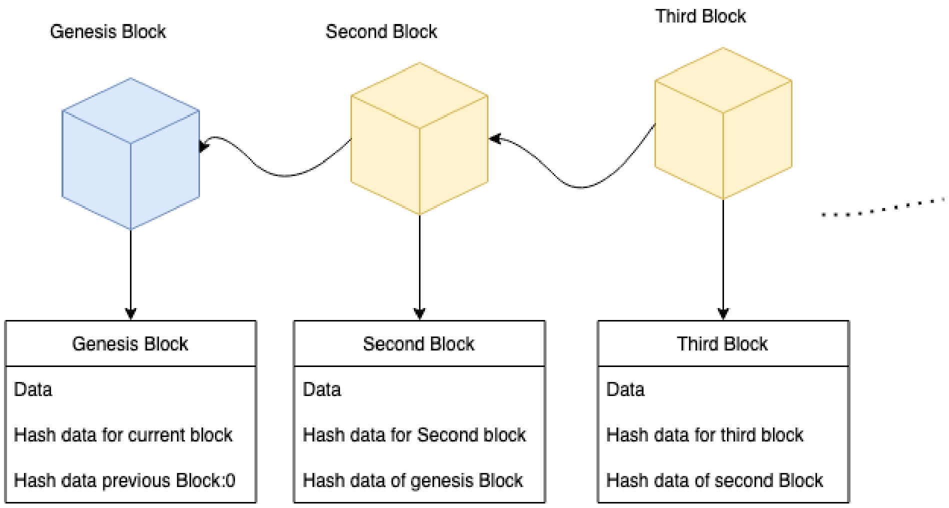
Genesis Block
Second Block
Third Block
Genesis Block
Data
Hash data for current block
Hash data previous Block:0
Second Block
Data
Hash data for Second block
Hash data of genesis Block
Third Block
Data
Hash data for third block
Hash data of second Block

Figure 1. Blockchain layer architecture.

In Blockchain, a hash function acts as a fingerprint [48], whereas in central systems changing the hash data is easy due to the single-failure node issue. Therefore, to prevent the data from being altered in a distributed network, a copy of the Blockchain will be shared among all participants. Whenever a node joins the network, they will receive a copy of all Blockchain records, so in the event of an attack, the attacker will need to gain the support of more than 50 percent of the network to change the data that exist in the Blockchain. Furthermore, every participant on the Blockchain should verify and agree on the new block before it is added to the Blockchain. It is here that consensus algorithms play a vital role. As a result of the consensus algorithm, one of the participants wins the ability to declare and share the new block with the network. The other participants are required to verify the block to ensure that the data and hashes on the block are valid. In the example of Bitcoin, a group of transactions will be chosen from a pool of transactions, and a proof of work algorithm will require a mathematically difficult puzzle to be solved, and each participant who solves the puzzle will create data consisting of the transactions chosen from the pool and send the new block for verification to other participants. Other participants will verify the data and the validity of the transaction, such as by verifying the sender and recipient's address and the Bitcoin that is going to be transferred, before approving the new block [49].

With this technology, cryptocurrencies were born. Bitcoin's market and demand have grown so rapidly that, at the time of writing this paper, the price for each Bitcoin is around USD 47,000. Since the introduction of Bitcoin and Blockchain, this technology has been studied by many researchers and has been used in many other applications in addition to payment processing. As a result, many other Blockchain technologies have been introduced to the world, but all of them have the same key features of transparency, immutability and decentralization [50].

- Transparency

Blockchain transactions can be tracked, as it is necessary to verify new transactions against old ones. All the nodes in the Blockchain network hold a copy of the Blockchain, and by checking the last block, the previous block can be found from the hash data [51].

- Immutability

Blockchain data are recorded in different copies, which are encrypted and linked to previous data. Additionally, they have a robust consensus algorithm for making new blocks, such as proof of work, making it difficult to change recorded data or introduce fake data into the network [52].

- Decentralization

All Blockchain technologies aim for decentralization, but some do have some central management. In some cases, private Blockchain networks are not completely decentralized [53,54].

The application of Blockchain to real-world problems has gained increased attention in recent years because of the above key features. Bitcoin and other cryptocurrencies were first used as financial and payment systems, and many industries have adopted them as a payment method [55–58]. Financial services that employ cryptocurrencies can be seen in tourism [59], the trading of digital assets [60] and black markets [61]. While cryptocurrencies are mostly used to make payments, this technology has also opened up many other opportunities. The second generation of Blockchain technologies such as Ethereum and the addition of smart contracts into this technology have evolved.

Ethereum was introduced by Vitalik Buterin in 2014 [62]. The Ethereum protocol has a built-in programmability feature that implements Nick Szabo's definition of smart contracts [63]. The introduction of smart contracts opened up the possibility of Defi Applications (decentralized finance), which allowed finance applications to run on the Ethereum network without the need for central validation. In Szabo's definition of smart contracts, a computer program can replace paper contracts and automate the process of implementing contract terms and conditions [63,64]. Smart contracts have shown a wide range of applications in areas such as secure voting [65], insurance policies [66], healthcare record data security [67,68] and digital asset trading, among others. Blockchain-based smart contracts have advantages over paper contracts due to their transparency, prevention of errors and fraud, and low cost.

Blockchain technology has also shown the potential to compete with and replace other digital solutions. A Blockchain can, for instance, be used to secure a system through its own public-private key authentication. There have been many studies on using Blockchain technology and solving issues in other areas such as supply chain management without involving a third party with greater transparency and immutability. However, this technology has its own limitations in its ability to replace older technologies.

In addition to having some similar features such as transparency or being decentralized to govern the network, Blockchain technology also has some differences such as its scalability, access, programmability, and open-source nature that make it useful in certain areas while useless in others. While there are many benefits and advantages of Blockchains, their disadvantages should also be considered. The most common issue is scalability [69]. The Bitcoin network can handle up to 10 transactions per second, so it is difficult to use Bitcoin to replace a payment system such as Visa, which has the ability to handle millions of transactions per second. Furthermore, a Blockchain such as Bitcoin has limited storage for each block (1 MB) and a proof of work algorithm that ensures the creation of new blocks every 10 min. As a result, the validation of one transaction is expensive compared to traditional systems such as the Visa or Mastercard networks.

2.1.1. Blockchain Life Cycle

The transaction is built by a node and signed by its private key, which can be accessed by its own public key. A gossip protocol is used to send this transaction to the network [70]. The next peer-named miners select some number of transactions for validation and verification. The miners create a block based on those verified transactions and attempt to get that block approved by the network. In this step, consensus algorithms play an important role in determining which miner is eligible to create the next block [71]. For instance, the Bitcoin network uses proof of work to ask miners to solve a difficult math puzzle in order to be eligible to add a new block. This algorithm requires the miner to pay a high price for securing the validation of transactions. In Bitcoin, a reward is given for making a block, and some Bitcoin is given to the miner who solves the puzzle and adds the new block to the network. To keep track of all transactions in recent blocks, the new block will be linked to the chain by hash algorithms. To show the order of blocks in the chain, each block stores a hash of its previous block. Additionally, they include the number of transactions based on their size, which varies depending on the technology. Because all ledgers and peers in the Blockchain network have copies of the blocks, they can be tracked. Figure 2 illustrates the lifetime of a transaction and the addition of a new block to Blockchain.

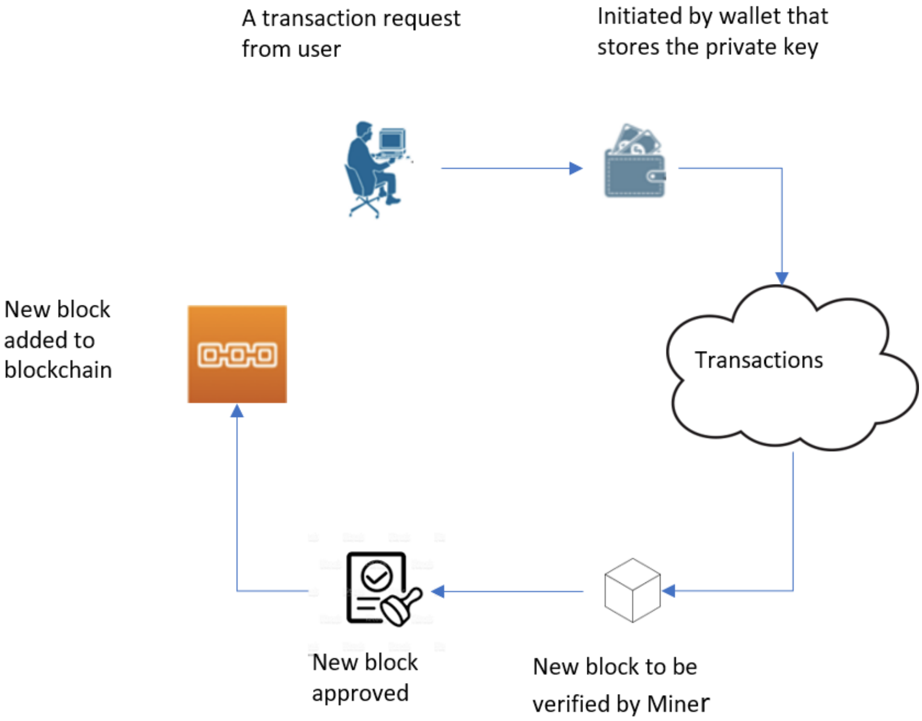
A transaction request from user
Initiated by wallet that stores the private key
Transactions
New block to be verified by Miner
New block approved
New block added to blockchain

Figure 2. Blockchain life cycle.

Blockchain technology can be classified from many perspectives. Depending on how a node joins the Blockchain network, it can be classified as public or private. The Bitcoin Blockchain, which is the quintessential example of a public Blockchain, is entry/exit free. In private Blockchain networks, only known nodes can enter the network [72]. Cryptocurrencies can be divided into two categories based on the way they are generated and distributed.

The first category includes cryptocurrencies created by the first transaction on the genesis node, which is then distributed among stakeholders. The second category includes cryptocurrencies that are generated over time and distributed. There are different methods for the generation process, depending on the type of cryptocurrency. With proof of work, miners are rewarded with cryptocurrencies for solving difficult problems, e.g., Hashcash [73] in Bitcoin. As an alternative to the proof of work, the proof of stake is another approach [44]. Proof of stake enables a miner who possesses more cryptocurrency to have a higher chance of placing blocks in the Blockchain and earning coins. However, in proof of work, the power of the miner's processors determines their ability to create a new block and acquire coins as a reward. Further, there are other approaches, such as proof of burn, which is used in cryptocurrencies such as Slimcoin, where miners earn Slimcoin in exchange for destroying another cryptocurrency such as Bitcoin [73].

Although Blockchain technology has many benefits, it also has many disadvantages. The disadvantages of Blockchain technology are outlined below.

2.1.2. Scalability

In order to have a trustless robust system, Blockchain needs to propagate data amongst all the nodes as there is no trust amongst the networks. To do that, it needs to make limited storage available for each block; for example, in Bitcoin only 1 MB is available, which can hold only a limited number of transactions. Further, the consensus algorithm is another bottleneck in this process that makes it difficult to constantly build new blocks. As a result, in the Bitcoin network the limitation for transactions per second is 10, and in Ethereum it is around 13 to 17 transactions. Table 5 shows a comparison between different Blockchain technologies.

Table 5. Comparison between different Blockchains.

Name	Permission	Consensus Algorithm	Scalability	Transactions per Second	Smart Contract	Applications	References
Bitcoin	Public	PoW	Low	5	No	Financial	[1]
Ethereum	Public	PoW/PoS	Low	15	Yes	Industries, Financial, Insurance, Voting, etc.	[74]
Litecoin	Public	Scrypt hash algorithm	Medium	55	Yes, OmniLite	Financial	[75]
Bitcoin Cash	Public	PoW	Medium	300	Through side chains such as smartBCS [76]	Financial	[77]

2.1.3. Security

Blockchain technology has many security issues, most of which are related to the amount of power miners possess. As such, a 51 percent attack is one in which a malicious side gains more than 50 percent of the power in the network. This allows them to commit double spending and produce fraudulent blocks, which leads to the loss of trust in that network [78]. To prevent such an issue, any new Blockchain technology needs to make sure it avoids giving such power and starts growing quickly among different stakeholders to make it more difficult for this to occur. In addition, there are other types of attacks such as Sybil attacks [79], fishing on wallets holding private keys [80], and selfish mining attacks [81] that make the Blockchain more vulnerable. Any good Blockchain technology must be immune to these attacks.

2.2. Tangle

Despite all the benefits of Blockchain technology, this technology can only be used for high-power systems. Specifically, using Blockchain in Internet of Things (IoT) networks poses a number of problems. To solve these problems, Tangle was proposed specifically for IoT devices [82]. Tangle technology is a decentralized encrypted network for recording data in a scalable and secure manner. To track history and validate the network, Tangle uses a non-cyclical directional graph to link transactions together [83]. Tangle's first technology is IOTA, which is built for IoT networks. Key features of IOTA are scalability, zero-fee transactions and its lightweight proof of work based on the Hashcash algorithm, which fits IoT devices with limited resources.

Each user who wants to perform transactions also needs to validate other transactions, so the key difference between ITA and Blockchain technology is there is no incentive system for miners to validate other transactions; therefore, to perform a transaction a user only needs to validate two other transactions. Further, if these two transactions are deemed invalid, the new transaction will also be considered invalid. This results in requiring no fees for performing thousands of transactions between IoT devices. Having more users on the network will also result in higher scalability on the network since the validating job is distributed among all users in the network [82–84]. Figure 3 illustrates the validation of transactions in IOTA.

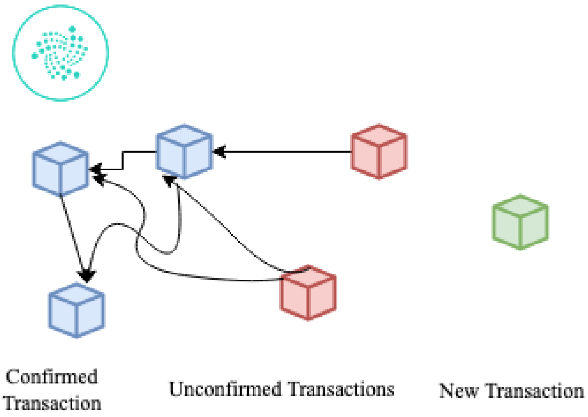

Figure 3. New transactions choose two unconfirmed transactions for validation.

2.2.1. Tangle Life Cycle

The genesis transaction was the first transaction in the IOTA tangle that created all IOTA coins and distributed them to the initial investors [85]. For Blockchain, the issue was the size of the block and the energy required to validate the block, which is a bottleneck for Blockchain technologies; therefore, in IOTA there are no blocks, and transactions are recorded instead. Once the genesis node is recorded, other transactions verify the genesis transaction, become unconfirmed transactions, and remain in a pool of transactions. When a transaction needs to occur, the provider of that transaction will choose two unconfirmed transactions from the pool with a tip selection algorithm and validate them and check double spending on both, linking their transaction to those unconfirmed transactions. The graph will be cut if any transactions deemed invalid are linked to those invalid transactions [82]. Transactions will be confirmed when they reach a cumulative score of approvals from new transactions. In IOTA, there are entities called coordinators that provide security and scalability. IOTA foundation controls coordinators, which confirm the network and find invalid transactions. The problem with coordinators is their centrality over the network and their vulnerability to single failure node attacks [86].

2.2.2. Advantage of Tangle

The Tangle network has higher scalability than traditional Blockchains since all users validate transactions to request a transaction, and as the network grows the number of validators also increases. The other advantage of IOTA Tangle is that there is no fee for any transaction, and the nature of IoT devices requires a high number of micro transactions that would cost too much on a Blockchain network, but not on IOTA [87]. Moreover, IoTA is built for devices with low computing power capability since the consensus algorithm is much lighter than the ones that use PoW in Blockchain.

2.2.3. Disadvantages

IOTA has many advantages over Blockchain, but it also has weaknesses. One of its major weaknesses is the lack of distribution and the existence of a central coordinator. Distributed technologies are designed to create trust between network communities by removing any central power, the presence of which reduces trust. Additionally, targeting them can cause disruptions in the network. A second disadvantage of the IOTA network is its wallet security, which is a weakness of the WOTZ algorithm that generates addresses and signs messages in the network. Using the same address continuously causes security breaches in IOTA wallets [88]. Finally, the disadvantage of IOTA is that it is only used for performing micropayments between IoT devices and no smart contracts are provided, although this style has many other features such as the MAM protocol which can be used to communicate between IOTA nodes in a secure environment [89].

2.2.4. Scalability

IOTA addresses two main issues associated with blockchain, which are scalability and miners. In IOTA, each node must confirm transactions that have not yet been confirmed in addition to issuing a transaction. It begins by selecting two unconfirmed transactions, named tips, and then verifies there are no conflicts between them and adds its transaction to the network using a light Proof-of-Work algorithm. This technique makes IOTA's Tangle incredibly scalable. For every transaction that is added to the Tangle, two others are being confirmed. This means that the network doesn't slow down when there are several new transactions. The IOTA network becomes faster when more transactions happen. This means that IOTA can handle almost an unlimited number of transactions per seconds while traditional blockchain can only handle a few transactions per second. However, there is also another aspect to scalability which everybody tends to forget, which is storage. In Blockchain, users need a full copy of the chain before they can start adding new transactions, IOTA's Tangle is much more light weight. Users do not need a full copy of the Tangle to add transactions. They only need a small part of the Tangle to create and verify transactions. This makes it much more future proof and, crucially, IOTA has no miners. The concept of mining does not exist on the IOTA network [87].

2.2.5. Security

The security in issuing transactions in IOTA is based on Winternitz One Time Signature Scheme [88]. In IoTA each node has a seed that will be added to a random index and hashed with the kerl function. After steps of fragmentation and hashing over and over a private key will be produced. The concern with this algorithm is reusing the same address over and over which may cause security breaches [88]. In the coming Chrysalis update IOTA will switch to a well-trusted digital signature scheme called the Edwards-Curve digital signature algorithm which Bitcoin and Ethereum have relied upon for years. It allows users to use static reusable addresses, which will help to improve user as well as developer experiences [90].

2.3. Hashgraph

The Swirlds Hashgraph consensus algorithm was introduced by Baird in 2016 to solve the fairness and scalability issues associated with Blockchain technology [25]. Hashgraphs are based on vertical time series of events by each user. Using the gossip protocol, each user will request an event or transaction in a time series, and it will be shared with other users for voting. This is fair since the choice of event is based on the date the event was created, and it is scalable since there is no need for a history of transactions because the transaction will be deleted after it has been validated. In comparison with Blockchain technology, this provides fairness for transactions, as Blockchain relies on the miners to validate transactions, and they choose transactions that benefit them [25]. Both technologies are resistant to attacks such as distributed denial of service (DDoS) and Sybil attacks. Hashgraph technology is a private network managed by the founder. Its code is not opensource, which makes trusting this network difficult. In addition, since the network requires permission to enter, it is difficult to establish trust between the community of Hashgraph. Furthermore, while transactions in Blockchain technology can be tracked as transparent, this is not possible in Hashgraph since they are deleted after some time, making storage for the nodes much more limited than in other Blockchains. Figure 4 shows the structure of Hashgraph. In Hashgraph, each entity has a timeline that requests events. These events will be validated according to the date they were published.

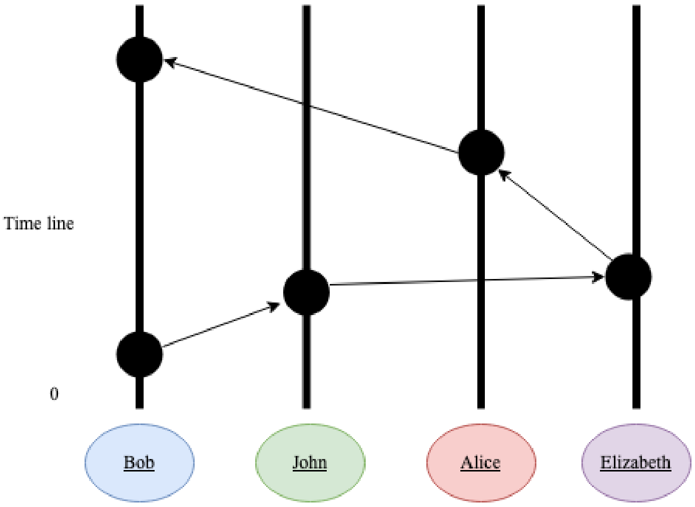

Figure 4. Events will be created by nodes, and they will be voted on and distributed by gossip protocol and virtual voting. The fairness is based on the time when an event is created.

Hashgraph has advantages and disadvantages compared to blockchain technology, which are listed below.

2.3.1. Energy Efficient

After a period, transactions in the hashgraph are deleted. Additionally, this results in less energy being wasted when checking the network and maintaining payments, even though this issue has a disadvantage for uses that require a complete history of the network [25].

2.3.2. Security

Hashgraph uses Byzantine Fault Tolerance (BFT) for securing the network, which stops intruders from tampering with the data or entering the network. Despite failures or malicious nodes, BFT provides a situation for Hashgraph to continue functioning [25].

2.3.3. Scalability

Hashgraph propagates events through gossip control, which prevents overcrowding the network with messages and enables transactions to be approved more quickly [25].

2.3.4. Disadvantages

The most important drawback of Hashgraph technology can be pointed out in the fact that this technology is closed and patented, which makes fewer people trust it, and this network is not fully distributed [25].

2.4. Side Chain

Side chain is a consortium of subnets with different features as separated Blockchain networks. The novelty of side chain is the sharding that connects different subchains of networks. Each subchain performs its own verification and validation, and only some data are locked into the main chain or master chain. Side chain attempts to solve the scalability problem in Blockchain technology by sharding the network into parallel systems so that each group can validate its own transactions and record a fragment of the data into the master chain. Each subchain can maintain its own asset that trades in the subchain, and the last state of the transaction is maintained on the master chain. It is a permission-based network, which brings more privacy into the network because each group can create a subchain to trade with the others and only share fragments of the data in the main chain. Further, it is scalable due to the fact that transactions happen in parallel with small or no fees [91,92].

Advantages and Disadvantages

The goal of Side Chain is to create a common ecosystem to communicate between different DLTs. Taking into account their relationship, this technology is actually shared between other technologies, preserving all their capabilities and independency. Sidechains can be divided into independent sub-networks to divide transactions, each of which has its own unique capabilities. This makes the DLT technology ecosystem integrated and increases the speed of the processes in a more efficient way. However, this technology is still in its infancy and the usage of this technology is more about trading ecosystems.

2.5. Holochain

Holochain is an agent-centric distributed application platform. A major difference between Holochain and other DLTs is that it is based on agents. Each agent holds a Blockchain for itself with access to the main Holochain with a private key that allows it to record data. Using the application-driven agents, Holochain performs transactions and stores the data. In contrast to Blockchain, it is more of a distributed application that can be used for asset trading in a scalable and energy-efficient manner [86]. Table 6 shows a comparison between DLTs based on scalability, cost, fairness, security, permission, and open-source status.

Table 6. General comparison between DLTs.

Technology	Scalability	Cost	Fairness	Security	Permission	Open Source
Blockchain	Low	High	Low	High	Public/Private	Many of them are opensource
IOTA Tangle	High	No cost	Due to high scalability, it is not important	High	Public	Yes
Hashgraph	High	Low	Good	High	Private	No
Side Chain	High	Low	Depends on subchains	Good	Both Private and public	Depends on Subchains
Holochain	Medium	Medium	It is not addressed	Depends on Agents	Both Private and Public	Depends on Agents

In comparison, these five technologies differ mostly in their architectures although they all share two important characteristics in common, namely, their distribution and the use of a consensus algorithm to provide data immutability. These technologies have various uses depending on their structure. IOTA technology, for instance, is designed exclusively for IoT networks and IoT devices, because other technologies require computationally intensive operations that cannot be handled by small IoT devices.

They also differ in the scalability of their systems, which has been solved by changing the consensus algorithm in other technologies such as Tangle, Hashgraph, Sidechain and Holochain. The other difference between them, which stems from the differing consensus algorithms and structures, is the cost of transactions in each, which has made it harder to use them in various cases due to the high cost of proof-of-work algorithms in technologies such as Bitcoin. The creation of new methods has led to a reduction in the costs associated with these networks.

The discussion of fairness in the execution of transactions is also important, as it can lead to long-term delays in the execution of a transaction, and in technologies such as Blockchain, due to the existence of transaction costs and incentives, this position becomes important to investigate. This problem in technologies such as Hashgraph has been solved by prioritization of the time that each event has been created. In addition, this problem is not seen in other technologies with a high number of transactions per second.

Furthermore, the security of these networks depends on the consensus algorithm, which should protect against intrusions such as the Sybil Attack. As another point of comparison between these technologies, it may be worth highlighting the openness of the network to new users, whether it is a public network or a private one that needs permission to access. In general, private networks have better access control and higher transaction speeds, but due to the existence of a supervisory body, they cannot be fully monitored in a distributed fashion, and this conflicts with the main purpose of these technologies.

In the end, the availability of the source codes is vital for drawing attention to these technologies and building trust in them, which can be an issue with a technology such as Hashgraph, since this technology is not open source.

The different characteristics of these technologies showed their potential utility in a variety of areas that require these features. Comparing these technologies with each other and with traditional approaches is necessary. Thus, in the next section a comparison of their application with regard to their features has been given.

3. Applications of DLT

The lack of centralized computing in DLT has paved the way for different applications. One is the use of Blockchain for actions where the need for trusted third parties is inevitable. Researchers have defined concepts such as smart contracts in this area.

3.1. DLT in Energy Trading

Energy trading is one of many fields in which smart contracts have been used [93]. As a result of the high demand for energy, different home-based methods for generating electricity have emerged. With this power generation, consumers and service providers can establish a two-way energy exchange network. Therefore, smart grids have been developed to trade energy via central systems in traditional solutions [94]. These systems have the drawback of lacking the trust of customers and privacy [95]. Furthermore, single-point failures can cause damage to central systems. The Blockchain, with its distributed platform and smart contracts, provides the opportunity to trade energy between consumers in a secure way.

This article discusses energy trading using Blockchain. In this method, energy is traded among peers, and only information is exchanged via the Blockchain network, which is a low-cost way to make private and secure transactions. Blockchains enable transactions to be carried out securely and safely, which eliminates the need to exchange energy and costs with third parties. This makes energy management and energy trading easier and more secure. By using smart contracts and transparency feature of them, a Blockchain network can also improve security and ease the execution of transactions compared to non-Blockchain systems. When a seller of energy sends a smart contract to the Blockchain network and requests a price, the smart contract provides transparency to the buyer.

Mengelkamp et al. [96] developed a private Blockchain and smart contracts for energy trading markets in response to the need to manage renewable energy sales. As part of this Blockchain, smart contracts are used due to the need to manage the distributed sales market for renewable energies [91]. Furthermore, Abdella et al. provided a survey with useful details on smart grids and smart contracts [97]. Keke Gai et al. implemented a Consortium Blockchain-based technique to solve issue of privacy and data leakages in smart grids, which can lead to leakage of the location of each customer [98]. Wang et al. also used Blockchain for authentication problems in smart grids to develop a solution for attacks such as DDoS [99]. Bera et al. introduced the DBACP-IoTSG method and a new consensus algorithm for Blockchain-based access control for smart grids. The communication in their method is based on peer-to-peer communication with leaders in networks [100]. Table 7 shows a comparison between DLT-based approaches and traditional methods for running a network of smart grids.

Table 7. Comparison of DLT-based approaches and traditional approaches in smart grids.

Method	Cost	Security	Privacy
Smart Grid with DLT	Lower	High	Secure Access Control and Authentication
Central Method	High	Single Failure Node, DDoS attack	Leakage of Data is Highly Possible

3.2. DLT in Insurance

DLT can also be used in the insurance industry. Insurance processes are often done manually or on paper, which is time-consuming and costly. In traditional insurance, contracts were made at a high cost on paper, which is harmful to the environment and can endanger people's private data. Many of the problems of traditional insurance systems can be solved using smart contracts by employing features such as trust, privacy and transparency. The use of smart contracts for micropayments and insurance claims was suggested in [101]. Furthermore, Bader et al. suggested a new method called CAYPAY to limit the need for car inspections by using smart contracts and tamper-resistant sensors. The method did not completely replace the traditional process, but it resulted in a reduction in cost and time [66]. Additionally, Ciocarlie et al. introduced BlockCIS for a continuous loop feedback system between customers and insurance companies based on Blockchain and tested with Hyperledger Composer [102]. Blockchain can also be used for recording medical data in insurance companies due to its tamper-resistant nature. MIStore is an example of the use of Blockchain to record and keep medical insurance data [103]. In general, Blockchain can be integrated in any step of the insurance process and offers advantages such as cost efficiency, trust and transparency. However, it also has some limitations, such as in fraud management and approving claims evidence; therefore, Blockchain is not mature enough to replace insurance companies' traditional approaches, but it can help reduce costs and time. Table 8 summarizes the advantages and disadvantages of DLT in the insurance industry.

Table 8. Advantages and disadvantages of Blockchain technology in the insurance industry.

Method	Advantages	Disadvantages
Traditional approaches	Human inspection of evidence	High in cost and time
DLT approach	Time and cost efficient, environment friendly, tamper-resistant recoding data, transparent functionality	Not mature enough to fully replace traditional approaches

3.3. DLT in Voting

DLT's trust feature makes its use in voting a viable option. A centralized system cannot be trusted in voting because it cannot be given full liability and is prone to single-point failure issues. A traditional voting system can be paper-based or electronic, as long as it is managed by a central system. A central system cannot be fully trusted to prevent votes from being tampered with [72], so a DLT can play a critical role due to its distribution, transparency, and immutability abilities [104].

A system utilizing e-voting can save energy and be cost efficient by allowing voters to cast their ballot from anywhere by clicking just a few buttons. However, there are also disadvantages such as cyber-attacks that may cause large-scale issues with fewer resources than a traditional system such as paper-based voting. E-voting systems can also have other disadvantages, such as being more complex to use.

McCorry et al. introduced the use of Blockchain for voting in a boardroom scenario. This was the first time Blockchain technology and smart contracts were used to vote in small networks by giving voters options. Voters' privacy was preserved, and the system was run on the Ethereum network [65]. To cast your vote, you can also use Blockchain-based methods, such as Bitcoin, to send transactions to candidates' addresses, which is considered a vote for that candidate [105,106]. Table 9 shows a comparison between traditional and DLT-based methods for voting.

Table 9. Advantages and disadvantages of DLT in voting systems.

Method	Advantages	Disadvantages
Traditional approaches	Everyone knows how to vote	Centralized management such as governments cannot be trusted for fully transparent voting
DLT approach	Transparent, privacy reservation	Expensive for voters, needs knowledge, hard to control by governments

3.4. DLT in Healthcare

Smart contracts and blockchain technology provide a safe and secure method for storing data, which helps resolve issues related to unreliable medical data and the manipulation of data since they are recorded in a distributed network. Blockchain technology is also useful for managing electronic health records (EHRs). There are also privacy concerns with traditional systems, and DLT-based systems can be used for managing EHRs and preserving the privacy of individuals. As a result of a system such as this, which has no central administration, the security of personal information can be guaranteed by multiple nodes within the Blockchain [107]. Table 10 shows a comparison between traditional and DLT-based methods for storing healthcare records.

Table 10. Advantages and disadvantages of DLTs in healthcare.

Method	Advantages	Disadvantages
Traditional approaches	Mature systems, widely used	Lack of standardization in EHR formats, not fully trusted, does not fully keep privacy
DLT approach	Transparent, privacy reservation, integration between different formats, having a method for access control by the owner of the record	Expensive to record healthcare records, in the infancy level

3.5. Other Applications of DLT

As DLT is integrated with supply chain management systems, the supply chain of a product can be traced from the beginning. Tian presented the use of a Blockchain system in the food industry to track the supply chain by recording and tracking history in a chain of blocks [108]. Furthermore, smart contracts and Blockchain can be used for trading, such as for making payouts in industries [109] or selling lemons in Denmark [110].

DLT technology also has some drawbacks that need to be addressed. As transparent networks, Blockchain networks should not store private information. Furthermore, smart contracts need to be bug-free to be fully trusted [111]. Finally, the lack of legal support for Blockchain-based applications is hindering the development of applications in DLT [112].

IOTA Tangle technology is designed for IoT networks, and its application can be found in the security of vehicular applications [113], improving IoT network security [114], increasing privacy in healthcare [115], securing WSN networks [116], P2P energy trading [117] and any IoT-related area that needs a lightweight distributed ledger payment system with high scalability. In comparison to the usage of Blockchain, the high scalability and lack of fees gives IOTA high potential in applications related to IoT devices.

Additionally, Hashgraph technology can be used for private DLT networks to build a secure, highly scalable, DLT for transactions. Compared to Blockchain technology, it has the advantage of high scalability on recording transactions, but it also has the disadvantage of not being an open-source environment for a community to grow.

Side chain technology is a highly scalable technology compared to Blockchain and has the ability of having customized Blockchain technology as a subchain on the network. There is great potential in this area to replace Blockchain technology, and there are some efforts, for example the TON network, to use this technology to provide a fast scalable network with different ways of customization to build specific Blockchain technology for specific applications such as recording data or trading assets.

The Holochain network, which is an application and agent-driven DLT network, can benefit distributed applications running in separated Blockchain with no cost on the network in a more secure and scalable manner; however, this technology and its application is still in its infancy.

Table 11 shows a comparison of the different capabilities and applications of DLTs.

Table 11. Comparison between DLTs in their applications.

Technology	Scalability	Smart Contract	Common Application	Effectiveness
Blockchain	Low	Yes	Financial, Smart contracts	Infancy level
Tangle	High	No	Managing the IoT network and its payments	Toward mature
Hashgraph	High	No	Event-based applications	Infancy
Side Chain	Medium	Yes	Multi-Blockchain structure	Infancy Level
Holochain	High	Yes	DApp-driven network	Infancy Level

4. Conclusions

This paper discusses the advantages and disadvantages of five different DLTs. A classification of DLT as well as the most commonly used applications of DLT are discussed. A comparison based on the advantages and disadvantages of each DLT is also provided. While there are many uses for DLT, the aim of this paper is to compare the effectiveness of DLT in solving problems, so the most common used and discussed applications are selected. Due to its nature of trustworthiness, transparency, built-in security features and immunity of records, DLT has the potential to replace some traditional approaches. Once the technology matures further, it is expected that more applications will use DLT based solution to address the issues present in traditional systems such as single point of failure, lack of data security, privacy and transparency.

Due to its unique capabilities and its design focus for IoT networks, Tangle is close to maturity among the reviewed technologies. A variety of new applications can be developed using Tangle. Furthermore, some areas such as e-Voting can benefit from DLTs since the most important features that voting needs are immutability and transparency which DLT can provide them. There is a lot of potential in DLTs for voting, and a lot of their current problems can be solved by changing laws or training people to use this technology. These technologies can provide many advantages in combination with traditional methods in fields such as insurance, but they are still in the early stages of completely replacing traditional methods, so they should be able to focus on the unique characteristics of each field. As a final observation, this technology is advancing rapidly, and it is necessary to conduct updated studies on their application, since this technology is predicted to become of the most influential ones that will change the world.

Author Contributions: R.S.: Conceptualization, Investigation, Writing the first draft.; M.Z.: Project Administration, Supervision, Writing Review; R.J.: Supervision, Conceptualization, Writing Review; S.S. Supervision, funding acquisition, writing review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by a Collaborative Research and Development Grant by the Natural Sciences Engineering Research Council (NSERC), Canada.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: There are no conflict of interest.

References

1. Nakamoto, S. Bitcoin P2P e-cash paper. In *The Cryptography Mailing List*; Nakamoto Institute: Austin, TX, USA, 2008.
2. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
3. Cooley, R.; Wolf, S.; Borowczak, M. Blockchain-based election infrastructures. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; pp. 1–4.
4. Rghioui, A. Managing Patient Medical Record using Blockchain in Developing Countries: Challenges and Security Issues. In Proceedings of the 2nd IEEE International Conference of Moroccan Geomatics (MORGEO 2020), Casablanca, Morocco, 11–13 May 2020; pp. 1–6.
5. Zhao, Y.; Cui, M.; Zheng, L.; Zhang, R.; Meng, L.; Gao, D.; Zhang, Y. Research on electronic medical record access control based on blockchain. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719889330. [CrossRef]
6. De Oliveira, M.T.; Reis, L.H.A.; Carrano, R.C.; Seixas, F.L.; Saade, D.C.M.; Albuquerque, C.V.; Fernandes, N.C.; Olabarriaga, S.D.; Medeiros, D.S.V.; Mattos, D.M.F. Towards a blockchain-based secure electronic medical record for healthcare applications. In Proceedings of the ICC 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
7. Vazirani, A.A.; O'Donoghue, O.; Brindley, D.; Meinert, E. Blockchain vehicles for efficient medical record management. *NPJ Digit. Med.* **2020**, *3*, 1–5. [CrossRef] [PubMed]
8. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
9. Trollman, H.; Garcia-Garcia, G.; Jagtap, S.; Trollman, F. Blockchain for Ecologically Embedded Coffee Supply Chains. *Logistics.* **2022**, *6*, 43. [CrossRef]
10. Sayyad, S.F.; Pawar, M.; Patil, A.; Pathare, V.; Poduval, P.; Sayyad, S.; Pawar, M.; Patil, A.; Pathare, V.; Poduval, P. Features of blockchain voting: A survey. *Int. J.* **2019**, *5*, 12–14.
11. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
12. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **2019**, *3*, 1–17. [CrossRef]
13. Nguyen, G.-T.; Kim, K. A survey about consensus algorithms used in blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128.
14. Kaushik, A.; Choudhary, A.; Ektare, C.; Thomas, D.; Akram, S. Blockchain—literature survey. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), New York, NY, USA, 19–20 May 2017; pp. 2145–2148.
15. Lin, I.-C.; Liao, T.-C. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659.
16. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **2017**, *107*, 841–853. [CrossRef]
17. Xu, Y.; Li, X.; Zeng, X.; Cao, J.; Jiang, W. Application of blockchain technology in food safety control: Current trends and future prospects. *Crit. Rev. Food Sci. Nutr.* **2020**, *62*, 2800–2819. [CrossRef] [PubMed]
18. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef] [PubMed]
19. Belu, M.G. Application of blockchain in international trade: An overview. *Rom. Econ. J.* **2019**, *71*, 2–16.
20. Monrat, A.A.; Schelen, O.; Andersson, K. A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
21. Bhaskar, P.; Tiwari, C.K.; Joshi, A. Blockchain in education management: Present and future applications. *Interact. Technol. Smart Educ.* 2020; *ahead-of-print*. [CrossRef]
22. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. *Financ. Innov.* **2016**, *2*, 24. [CrossRef]
23. Wu, J.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
24. Conti, M.; Kumar, G.; Nerurkar, P.; Saha, R.; Vigneri, L. A survey on security challenges and solutions in the IOTA. *J. Netw. Comput. Appl.* **2022**, *203*, 103383. [CrossRef]
25. Baird, L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance; Swirlds Tech Reports SWIRLDS-TR-2016-01. 31 May 2016. Available online: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf (accessed on 11 June 2022).
26. Singh, A.; Click, K.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Choo, K.-K.R. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J. Netw. Comput. Appl.* **2019**, *149*, 102471. [CrossRef]
27. What Is Polygen. Available online: https://www.coinbase.com/learn/crypto-basics/what-is-polygon (accessed on 6 June 2022).
28. Fox, M.B.; Glosten, L.R.; Greene, E.F.; Guan, S.S. Distributed Ledger Technology and the Securities Markets of the Future: A Stakeholder Survey. *Colum. Bus. Law Rev.* **2021**, *2*, 651.
29. Li, J.; Kassem, M. Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction. *Autom. Constr.* **2021**, *132*, 103955. [CrossRef]
30. Kadam, S. Review of distributed ledgers: The technological advances behind cryptocurrency. In Proceedings of the International Conference Advances in Computer Technology and Management (ICACTM), Pune, India, 23–24 February 2018.

31. Río, D.; César, A. Use of distributed ledger technology by central banks: A review. *Enfoque Ute* **2017**, *8*, 1–13.
32. Nurgazina, J.; Pakdeetrakulwong, U.; Moser, T.; Reiner, G. Distributed Ledger Technology Applications in Food Supply Chains: A Review of Challenges and Future Research Directions. *Sustainability* **2021**, *13*, 4206. [CrossRef]
33. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. *Sensors* **2020**, *20*, 483. [CrossRef]
34. Asante, M.; Epiphaniou, G.; Maple, C.; Al-Khateeb, H.; Bottarelli, M.; Ghafoor, K.Z. Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey. *IEEE Trans. Eng. Manag.* **2021**, 1–27. [CrossRef]
35. Zhu, Q.; Loke, S.W.; Trujillo-Rasua, R.; Jiang, F.; Xiang, Y. Applications of distributed ledger technologies to the internet of things: A survey. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34. [CrossRef]
36. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed ledger technology review and decentralized applications development guidelines. *Future Internet* **2021**, *13*, 62. [CrossRef]
37. Siano, P.; de Marco, G.; Rolan, A.; Loia, V. A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets. *IEEE Syst. J.* **2019**, *13*, 3454–3466. [CrossRef]
38. El Ioini, N.; Pahl, C. A review of distributed ledger technologies. In Proceedings of the OTM Confederated International Conferences on the Move to Meaningful Internet Systems, Valletta, Malta, 22–26 October 2018; pp. 277–288.
39. Sunyaev, A. Distributed ledger technology. In *Internet Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 265–299.
40. Bhardwaj, R.; Datta, D. Consensus algorithm. In *Decentralised Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 91–107.
41. Niranjanamurthy, M.; Nithya, B.N.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Clust. Comput.* **2019**, *22*, 14743–14757. [CrossRef]
42. Jakobsson, M.; Juels, A. Proofs of Work and Bread Pudding Protocols (Extended Abstract). In *Secure Information Networks*; Springer: Boston, MA, USA, 1999; pp. 258–272.
43. Karantias, K.; Kiayias, A.; Zindros, D. Proof-of-burn. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kinabalu, Malaysia, 10–14 February 2020; pp. 523–540.
44. Saleh, F. Blockchain without waste: Proof-of-stake. *Rev. Financ. Stud.* **2021**, *34*, 1156–1190. [CrossRef]
45. Glaser, F. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. In Proceedings of the HICSS 2017, Waikoloa Village, HI, USA, 4–7 January 2017; pp. 1543–1552.
46. Golosova, J.; Romanovs, A. The Advantages and Disadvantages of the Blockchain Technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2016; pp. 1–6.
47. Merkle, R.C. A fast software one-way hash function. *J. Cryptol.* **1990**, *3*, 43–58. [CrossRef]
48. Le Nguyen, T. Blockchain in healthcare: A new technology benefit for both patients and doctors. In Proceedings of the 2018 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, USA, 19–23 August 2018; pp. 1–6.
49. Segendorf, B. What is bitcoin. *Sveri Gesriksbankecon.* **2014**, *2014*, 2–71.
50. Rajasekaran, A.S.; Azees, M.; Al-Turjman, F. A comprehensive survey on blockchain technology. *Sustain. Energy Technol. Assess.* **2022**, *52*, 102039. [CrossRef]
51. Rizal Batubara, F.; Ubacht, J.; Janssen, M. Unraveling transparency and accountability in blockchain. In Proceedings of the 20th Annual International Conference on Digital Government Research, Dubai, United Arab Emirates, 18–20 June 2019; pp. 204–213.
52. Hofmann, F.; Wurster, S.; Ron, E.; Bohmecke-Schwafert, M. The immutability concept of blockchains and benefits of early standardization. In Proceedings of the 2017 ITU Kaleidoscope Academic Conference: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017.
53. Khan, A.G.; Zahid, A.H.; Hussain, M.; Farooq, M.; Riaz, U.; Alam, T.M. A journey of WEB and Blockchain towards the Industry 4.0: An Overview. In Proceedings of the 2019 International Conference on Innovative Computing (ICIC), Seoul, Korea, 26–29 August 2019; pp. 1–7.
54. Guegan, D. *Public Blockchain Versus Private Blockhain*; HAL: Lyon, France, 2017.
55. Lin, C.; He, D.; Huang, X.; Khan, M.K.; Choo, K.-K.R. DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2440–2452. [CrossRef]
56. Wang, H.; Qin, H.; Zhao, M.; Wei, X.; Shen, H.; Susilo, W. Blockchain-based fair payment smart contract for public cloud storage auditing. *Inf. Sci.* **2020**, *519*, 348–362. [CrossRef]
57. Yu, R.; Xue, G.; Kilari, V.T.; Yang, D.; Tang, J. CoinExpress: A Fast Payment Routing Mechanism in Blockchain-Based Payment Channel Networks. In Proceedings of the 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–9.
58. Nguyen, Q.K. Blockchain-a financial technology for future sustainable development. In Proceedings of the 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), Kaohsiung, Taiwan, 24–25 November 2016; pp. 51–54.
59. Bodkhe, U.; Bhattacharya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S. BloHosT: Blockchain enabled smart tourism and hospitality management. In Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Beijing, China, 28–31 August 2019; pp. 1–5.

60. Zhu, X.; Wang, D. Application of Blockchain in Document Certification, Asset Trading and Payment Reconciliation. *J. Phys. Conf. Ser.* **2019**, *1187*, 052080. [CrossRef]
61. Afzal, A.; Asif, A. Cryptocurrencies, blockchain and regulation: A review. *Lahore J. Econ.* **2019**, *24*, 103–130. [CrossRef]
62. Buterin, V.; Wiederhold, B.K.; Riva, G.; Graffigna, G. A next-generation smart contract and decentralized application platform. *Etherum* **2013**, *11*, 7. [CrossRef]
63. Szabo, N. The Idea of Smart Contracts. Available online: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (accessed on 8 June 2022).
64. O'Shields, R. Smart contracts: Legal agreements for the Blockchain. *NC Bank. Inst.* **2017**, *21*, 177.
65. McCorry, P.; Shahandashti, S.F.; Hao, F. A smart contract for boardroom voting with maximum voter privacy. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017; pp. 357–375.
66. Bader, L.; Bürger, J.C.; Matzutt, R.; Wehrle, K. Smart contract-based car insurance policies. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7.
67. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [CrossRef]
68. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med Syst.* **2018**, *42*, 130. [CrossRef]
69. Chauhan, A.; Malviya, O.; Verma, M.; Mor, T.S. Blockchain and scalability. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 122–128.
70. Saldamli, G.; Upadhyay, C.; Jadhav, D.; Shrishrimal, R.; Patil, B.; Tawalbeh, L. Improved gossip protocol for blockchain applications. *Clust. Comput.* **2022**, *25*, 1915–1926. [CrossRef]
71. Calvão, F. Crypto-miners: Digital labor and the power of blockchain technology. *Econ. Anthr.* **2018**, *6*, 123–134. [CrossRef]
72. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2018**, *36*, 55–81. [CrossRef]
73. Back, A Hashcash—A Denial of Service Counter-Measure. 2002. Available online: http://www.cypherspace.org/hashcash/ (accessed on 6 June 2022).
74. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
75. Litecoin. Available online: https://litecoin.org/ (accessed on 10 June 2022).
76. Smart BCH. Available online: https://smartbch.org/ (accessed on 10 June 2022).
77. Bitcoin Cash. Available online: https://bitcoincash.org/ (accessed on 10 June 2022).
78. Gupta, K.D.; Rahman, A.; Poudyal, S.; Huda, M.N.; Mahmud, M.P. A hybrid POW-POS implementation against 51 percent attack in cryptocurrency system. In Proceedings of the 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Sydney, Australia, 10–13 December 2019; pp. 396–403.
79. Swathi, P.; Modi, C.; Patel, D. Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 August 2019; pp. 1–6.
80. Saminathan, K.; Kondaveeti, H.K.; Karunanithi, S. Structure security attacks and countermeasures in the blockchain network. In *Convergence of Blockchain Technology and E-Business*; CRC Press: Boca Raton, FL, USA, 2021; pp. 61–84.
81. Bai, Q.; Zhou, X.; Wang, X.; Xu, Y.; Wang, X.; Kong, Q. A deep dive into blockchain selfish mining. In Proceedings of the ICC 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
82. Popov, S. The Tangle. 2018. Available online: https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf (accessed on 12 June 2022).
83. Bhandary, M.; Parmar, M.; Ambawade, D. A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; pp. 827–832.
84. Salimitari, M.; Chatterjee, M.; Fallah, Y.P. A survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet Things* **2020**, *11*, 100212. [CrossRef]
85. Pervez, H.; Muneeb, M.; Irfan, M.U.; Haq, I.U. A comparative analysis of DAG-based blockchain architectures. In Proceedings of the 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 19–21 December 2018; pp. 27–34.
86. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Futur. Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
87. Schueffel, P. Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph—A High-Level Overview and Comparison. 2017. Available online: https://ssrn.com/abstract=3144241 (accessed on 10 June 2022).
88. Shafeeq, S.; Zeadally, S.; Alam, M.; Khan, A. Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1244–1255. [CrossRef]
89. Lindvall, M. How Is Authenthicity and Confidentiality Maintained for MAM Channels on the IOTA Tangle? *Varden Development*. 2019. Available online: https://varden.info/doc.php?id=7 (accessed on 10 July 2022).
90. A Year of Transformation. Available online: https://blog.iota.org/a-year-of-transformation/ (accessed on 12 June 2022).
91. Gaži, P.; Kiayias, A.; Zindros, D. Proof-of-stake sidechains. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–22 May 2019; pp. 139–156.

92. Qasse, I.A.; Abu Talib, M.; Nasir, Q. Inter blockchain communication: A survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track, Rabat, Morocco, 7–9 March 2019; pp. 1–6.
93. Wang, N.; Zhou, X.; Lu, X.; Guan, Z.; Wu, L.; Du, X.; Guizani, M. When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art. *Appl. Sci.* **2019**, *9*, 1561. [CrossRef]
94. Bayram, I.S.; Shakir, M.Z.; Abdallah, M.; Qaraqe, K. A survey on energy trading in smart grid. In Proceedings of the 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Ottawa, ON, Canada, 11–14 November 2014; pp. 258–262.
95. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
96. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput. Sci. Res. Dev.* **2017**, *33*, 207–214. [CrossRef]
97. Abdella, J.; Shuaib, K. Peer to Peer Distributed Energy Trading in Smart Grids: A Survey. *Energies* **2018**, *11*, 1560. [CrossRef]
98. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
99. Wang, W.; Huang, H.; Zhang, L.; Su, C. Secure and efficient mutual authentication protocol for smart grid under blockchain. *Peer-Peer Netw. Appl.* **2020**, *14*, 2681–2693. [CrossRef]
100. Bera, B.; Saha, S.; Das, A.K.; Vasilakos, A.V. Designing blockchain-based access control protocol in iot-enabled smart-grid system. *IEEE Internet Things J.* **2020**, *8*, 5744–5761. [CrossRef]
101. Lamberti, F.; Gatteschi, V.; Demartini, C.; Pelissier, M.; Gómez, A.; Victor, S. On-demand Blockchain-based car insurance using smart contracts and sensors. *IEEE Consum. Electron. Mag.* **2017**, *7*, 72–81. [CrossRef]
102. Lepoint, T.; Ciocarlie, G.; Eldefrawy, K. Blockcis—A blockchain-based cyber insurance system. In Proceedings of the 2018 IEEE International Conference on Cloud Engineering (IC2E), Orlando, FL, USA, 17–20 April 2018; pp. 378–384.
103. Zhou, L.; Wang, L.; Sun, Y. MIStore: A Blockchain-Based Medical Insurance Storage System. *J. Med. Syst.* **2018**, *42*, 149. [CrossRef]
104. Moura, T.; Gomes, A. Blockchain voting and its effects on election transparency and voter confidence. In Proceedings of the 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, 7–9 June 2017; pp. 574–575.
105. Bistarelli, S.; Mantilacci, M.; Santancini, P.; Santini, F. An end-to-end voting-system based on bitcoin. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 4–6 April 2017; pp. 1836–1841.
106. Lee, K.; James, J.I.; Ejeta, T.G.; Kim, H.J. Electronic voting service using block-chain. *J. Digit. Forensics Secur. Law* **2016**, *11*, 8. [CrossRef]
107. Nawari, N.O.; Ravindran, S. Blockchain technology and BIM process: Review and potential applications. *J. Inf. Technol. Constr.* **2019**, *24*, 209–238.
108. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016.
109. Cardeira, H. Smart contracts and their applications in the construction industry. In Proceedings of the New Perspectives in Construction Law Conference, Bucharest, Romania, 19–21 March 2015.
110. Cholewa, J.B.; Shanmugam, A.P. Trading real-world assets on blockchain-an application of trust-free transaction systems in the market for lemons. *Bus. Inf. Syst. Eng.* **2017**, *59*, 425–440.
111. Tsankov, P.; Dan, A.; Drachsler-Cohen, D.; Gervais, A.; Buenzli, F.; Vechev, M. Securify: Practical security analysis of smart contracts. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 67–82.
112. Raskin, M. The law and legality of smart contracts. *Geo. Law Tech. Rev.* **2016**, *1*, 305.
113. Bartolomeu, P.C.; Vieira, E.; Ferreira, J. IOTA feasibility and perspectives for enabling vehicular applications. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7.
114. Shabandri, B.; Maheshwari, P. Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 1069–1075.
115. Abdullah, S.; Arshad, J.; Khan, M.M.; Alazab, M.; Salah, K. PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle. *Complex Intell. Syst.* **2022**, 1–19. [CrossRef]
116. Lin, I.-C.; Chang, C.-C.; Chang, Y.-S. Data Security and Preservation Mechanisms for Industrial Control Network Using IOTA. *Symmetry* **2022**, *14*, 237. [CrossRef]
117. Park, J.; Chitchyan, R.; Angelopoulou, A.; Murkin, J. A Block-Free Distributed Ledger for P2P Energy Trading: Case with IOTA? In Proceedings of the International Conference on Advanced Information Systems Engineering, Rome, Italy, 3–7 June 2019; pp. 111–125.