Review

Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain—A Survey

Zainab Iftikhar [1], Yasir Javed [2,*], Syed Yawar Abbas Zaidi [1], Munam Ali Shah [1], Zafar Iqbal Khan [2], Shafaq Mussadiq [3] and Kamran Abbasi [4]

[1] Department of Computer Science, COMSATS University, Islamabad 45550, Pakistan; zainab_iftikhar13@yahoo.com (Z.I.); yawar.abbas3636@gmail.com (S.Y.A.Z.); mshah@comsats.edu.pk (M.A.S.)
[2] Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia; zkhan@psu.edu.sa
[3] Institute of Information Technology, Kohat University of Science and Technology, Kohat 26000, Pakistan; dr.shafaq@kust.edu.pk
[4] Department of Distance Continuing and Computer Education, University of Sindh, Hyderabad 76080, Pakistan; abbasikamran@usindh.edu.pk
* Correspondence: yjaved@psu.edu.sa

Abstract: With opportunities brought by Internet of Things (IoT), it is quite a challenge to assure privacy preservation when a huge number of resource-constrained distributed devices is involved. Blockchain has become popular for its benefits, including decentralization, persistence, immutability, auditability and consensus. With the implementation of blockchain in IoT, the benefits provided by blockchain can be derived in order to make IoT more efficient and maintain trust. In this paper, we discuss some applications of IoT in different fields and privacy-related issues faced by IoT in resource-constrained devices. We discuss some applications of blockchain in vast majority of areas, and the opportunities it brings to resolve IoT privacy limitations. We, then, survey different researches based on the implementation of blockchain in IoT. The goal of this paper is to survey recent researches based on the implementation of blockchain in IoT for privacy preservation. After analyzing the recent solutions, we see that the blockchain is an optimal way for preventing identity disclosure, monitoring, and providing tracking in IoT.

Keywords: blockchain; consensus; IoT; smart contracts; bitcoin

check for updates

Citation: Iftikhar, Z.; Javed, Y.; Zaidi, S.Y.A.; Shah, M.A.; Iqbal Khan, Z.; Mussadiq, S.; Abbasi, K. Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain—A Survey. *Electronics* **2021**, *10*, 1732. https://doi.org/10.3390/electronics10141732

Academic Editors: Sang-Soo Yeo and Damien Sauveron

Received: 8 June 2021
Accepted: 11 July 2021
Published: 19 July 2021

1. Introduction

With the recent advancements in the field of Information Technology, a complex system called IoT evolved. It consists of several computing devices connected with each other through Internet and able to process and transfer data among each other with minimal human interaction needed. This system grew rapidly as the devices kept increasing and number of links increased automatically. Cisco Inc. predicted 50 billion devices by 2020, and it is still growing. IoT applications are increasing the level of convenience and efficiency in everyday life at low costs. For example, home automation and healthcare systems. An overview of IoT is given in Section 2.

However, with huge growth in the number of devices in IoT, the challenges also keep increasing. IoT devices can be as small as a watch; apart from processing, storage and networking limitations faced by such IoT devices, security is a serious concern of researchers and technicians. The growing number of devices makes attack surface broader. These security and privacy issues make IoT less trustworthy for organizations that have sensitive data and maintaining customer's privacy and data security are their top priorities. Also it becomes hard to manage a large number of devices and to have an consensus between them.

IoT's privacy and security with interconnected devices causes security challenges in the area of network computing. It means at any moment from anywhere, an attack can be launched on these devices that includes threats like denial of service, fabrication of identity, physical threats, communication channel targeting and many more. One of the biggest challenges in this research field is consumption of power resources and computational overheads on IoT devices. Many solutions have been proposed by the researchers in which strategies based on blockchain, homomorphic encryption, and attribute-based encryption are provided.

The exchange of data among physically connected devices related to their infrastructure and behaviors in the form of groups is known as IoT. From the Gartner report shown in Table 1, it was expected that almost 5.8 Billion interconnected devices would be having a vast share in market of $3 trillion in 2020 [1], while the forecasts of international data co-operation report that the expected market value of IoT devices is $1.1 trillion for 2023—the market of full stack systems, like RIOT [2] and Contiki [3] that enabled IoT devices functionality, is also expected to expand.

Table 1. IoT endpoint market by segment, 2018–2020, worldwide (in billions) [1].

Segment	2018	2019	2020
Utilities	0.98	1.17	1.37
Govt	0.40	0.53	0.70
Building automation	0.23	0.31	0.44
Physical security	0.83	0.95	1.09
Manufacturing and natural resources	0.33	0.40	0.49
Automotive	0.27	0.36	0.47
Healthcare providers	0.21	0.28	0.36
Retail and wholesale trade	0.29	0.36	0.44
Information	0.37	0.37	0.37
Transportation	0.06	0.07	0.08
Total	3.96	4.81	5.81

IoT brings improvement in quality of life in various domains. IoT devices play a huge role in different aspects of life, for example security, energy, safety, healthcare, smart grid, VANETs, industry and entertainment, but in terms of battery power, network protocol, complex computation and infrequent connectivity, these devices are fundamentally constrained in resources.

IoT bears the risk of not having a standard security scheme implementation, which results in security concerns like data misuse [2,3]. IoT devices collect personal information of a user such as his identity, contact number, energy consumed, and location. These devices also reveal a user's behavior, by collecting information about his lifestyle and daily activities—including watching movies, playing games, home activities, gatherings, etc. Therefore, the exposure of the user's personal data to non-trusted private and public servers can pose serious privacy-related issues, and the data gathered by these devices can be misused against the user. These threats make it crucial to focus on the security and privacy designs of IoT devices.

Since the application of blockchain in bitcoin cryptocurrency [4], it has become quite popular. Blockchain is being deployed in a large number of fields, such as education, healthcare, banking, agriculture, etc., for the opportunities that it brings.

One of the most important features of blockchain is decentralization. It is also used as a consensus mechanism to enable trust between all parties involved in decentralized networks, one example is cryptocurrency—for example, Bitcoin and Ethereum. IoT devices are decentralized and hence can be benefited by the blockchain.

There are many survey papers recently published that cover various aspects of blockchain in different environments [5–9]. Bitcoin overview was presented in [6] by Sankar et al. [7], in which challenges related to blockchain research are presented. Recently, in [10], an overview of blockchain-based IoT applications is presented. In [11], a comprehensive discussion about blockchain applications and framework implementations has been presented by Gao et al. The authors in [12] provide smart contract-based blockchain-dependent banking ledgers transactions overview. In many smart applications implementing blockchain, a systematic survey was provided in [13]. An overview of blockchain security services like confidentiality, privacy, access control and authentication has been given by Salman et al. in [14].

Many surveys on IoT security and Privacy-related issues and their solutions have been published. An analysis of privacy issues in IoT is given by Ziegeldorf et al. in [15]. The focus of this survey is on classification of privacy and security challenges in IoT devices. The challenges faced by industrial IoT devices are introduced by Sadeghi et al. in [16]. In [17], security-related challenges and their solutions are discussed. The authors have categorized security-related issues in mobile devices based on authenticity, confidentiality, trust, security, and access control. The ongoing research challenges and their status is discussed by Suo et al. [18]. Privacy preservation mechanisms based on encryption have also been discussed and some mechanisms are developed for private communication.

Many solutions have been proposed by the researchers recently for integration of blockchain in different IoT applications. The integration of blockchain with IoT and the pros and cons of this integration are examined by Christidis and Devetsikiotis in [19], and Atzori et al. in [20], whereas a comprehensive survey on IoT applications is presented in [21] by Conoscenti et al. For IoT decentralization, certain challenges and solutions are provided by the authors. In [22], blockchain-based IoT research opportunities, challenges and different architectures are discussed by Reyna et al. In [23], blockchain-based IoT with edge centric technology solutions have been discuss by Yeow et al. For security and privacy in blockchain-based IoT, a survey is presented in [10] by Fernendaz et al. A research done by Panarello et al. involves smart grid and smart cities in [24].

Recently, a survey on publicly deployed blockchain on different network principals has been provided by Neudecker and Hartenstein, in which design trade-offs of public blockchain and potential attacks are also presented [25]. The privacy issues in blockchain and their solutions are presented in [26,27]. The authors provided literature review comprehensively on privacy aspects of blockchain with their solution strategies and presented a zero knowledge proof, signature and cryptographic approaches analysis in [26]. Whereas in [27], Feng et al. presented privacy issues insights in a detailed manner, technical details summary and different defence mechanism were analyzed.

In this paper, we survey the deployment of blockchain in constrained IoT devices in order to achieve privacy and security.

In Section 2, we present an overview of IoT, its applications and privacy-related challenges. We present an overview of blockchain technology in Section 3, and we highlight some applications and strengths of blockchain. In the same section, We highlight different consensus mechanisms used by blockchain, and smart contracts that come with it. A review of applications of blockchain in IoT is presented in Section 4. At different layers of IoT, privacy mechanisms and issues are analyzed. Future challenges and their solutions are provided in Section 6. The conclusion of our paper is provided in Section 5. Future directions are given in Section 6.

All the researches highlighted above have mainly discussed strengths and limitations of either blockchain or IoT. Many researches are based on the integration of blockchain in IoT to achieve consensus, decentralization, or smart contracts. While there are a huge number of surveys that discuss the security parameters, such as integrity, non-repudiation, transparency and immutability, provided by blockchain to IoT, this survey focuses mainly on privacy preservation in resource-constrained IoT devices using blockchain. In this survey, we present state-of-the-art literature on privacy preservation assurance in IoT using blockchain. Contributions of this survey, as compared to other surveys, are as follows.

- We highlight some applications of IoT in different fields and see how much it impacts our lives and how crucial it is to preserve user privacy in IoT.
- We highlight privacy-related issues faced by IoT. We discuss the literature on techniques used for privacy preservation in IoT using blockchain.

- We discuss some of the most important applications of blockchain to show how it is being used in different industries. We highlight the strengths of blockchain that IoT can benefit from.
- We provide an analysis on the integration of blockchain in IoT systems. We mainly focus on blockchain's potential to preserve data privacy in IoT scenario.
- We provide future directions on privacy preservation in IoT.

2. Internet of Things

2.1. Overview

IoT is a system formed by the connection of multiple uniquely identified devices, such as computers, smartphones, sensors, software, cars, vending machines, thermostats, etc., to process and share data without the need of a human interaction. It relies on the Internet for communication purposes among these devices [28] to keep the data synchronized. The devices can be controlled remotely to perform desired actions.

Kevin Ashton used the term "Internet for things" for the first time in 1999. Originally it was called "Internet for things" and then it became "Internet of things". Since then, this framework became popular for the convenience it brought into everyday life. Today there are billions of IoT devices operating in a large number of fields (Figure 1). Although it is not feasible to discuss all applications of IoT, but Figure 1 shows some fields, including military [29,30], industry [31], smart cities [32], consumer [33], security [34] and home automation [35], and respective IoT applications. With time, IoT has become more human-friendly by processing large amounts of data with minimal human efforts put. Today IoT is not just limited to the personal use, but it is being used to detect weather, monitor surgeries, manage energy, monitor environment and manage transportation.

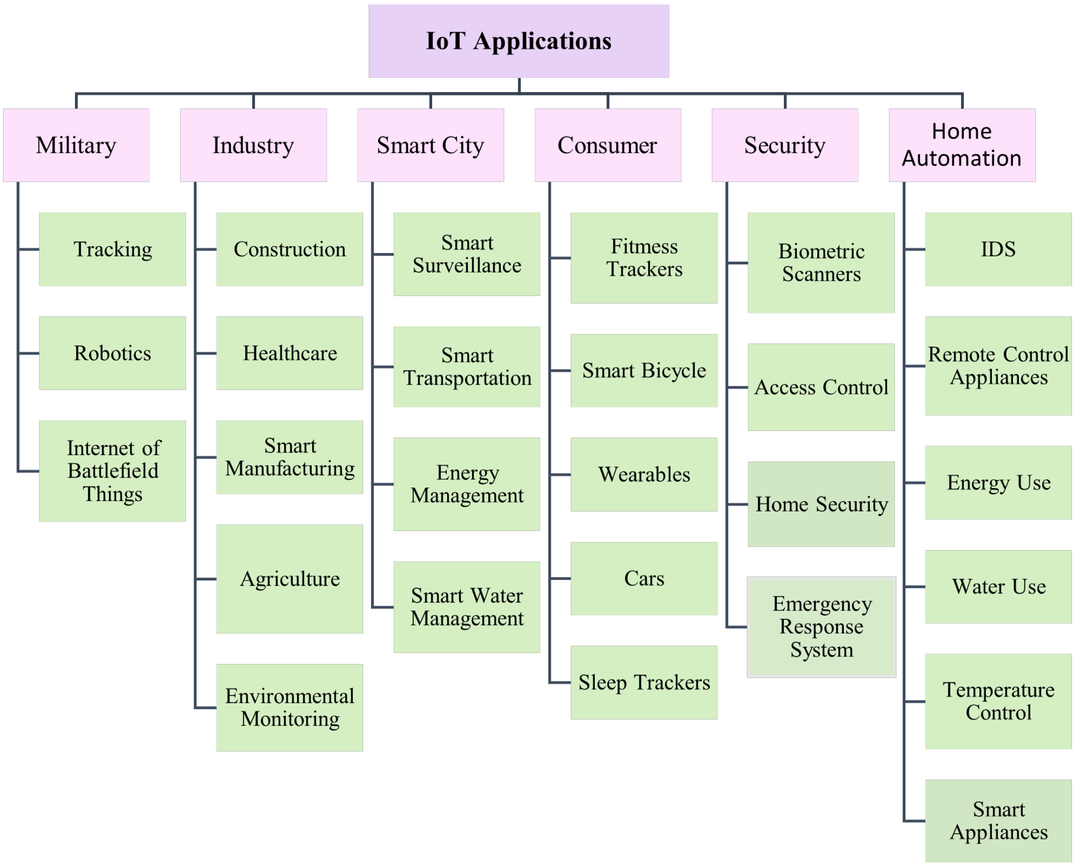

Figure 1. Applications of IoT.

2.2. Characteristics of IoT

- Intelligence: A lot of IoT devices are set to perform some specific actions when need arises, such as generating an alarm when a wearable sensor senses a high blood pressure for a patient. The decisions taken by a certain device depend on the sensitivity. Artificial intelligence and machine learning are making IoT devices smarter.
- Complexity: There is a huge number of devices, links, and actors in IoT, that keep increasing on a rapid rate.
- Heterogeneity: The devices are different from each other on the basis of hardware, software and networks.
- Connectivity: The devices in IoT are connected with each other through Internet to share data. For example, the sensors used to collect patient data on regular intervals need to transmit this data to the concerned medical personnel [36]. The state of data and devices keep changing. Therefore, it is important to keep the devices synchronized.
- Interoperability: The IoT devices are different from each other in nature but yet compatible when it comes to performing the tasks that involve the use of multiple devices at the same time.
- Decentralization: IoT comprises of billions of devices connected with each other using the Internet throughout the globe. No one "owns" IoT. The elements such as access, control and ownership are spread across the actors/nodes that make up IoT.

2.3. Privacy-Related Issues in IoT

The environment saturation with smart objects to perform daily tasks is provided by IoT. Sensors, micro controllers and transmitters that exchange and transmit data refer to nonstandard networking devices, which enable decision making support and smart interactions. For the collection and exchange of surroundings' data in industrial and consumer's devices, IoT is planted. IoT is remotely controlled via Internet or directly, which causes physical environmental changes. The safeguard protection techniques and collection of data in IoT are much lower than the momentum at which the devices are developed for customer use.

2.3.1. IoT Device Limitations

Resource constrained devices have a certain capability of weight, size and network connection, which directly impacts the complexity of IoT devices in data rates, unreliable links, packet sizes and power consumption. Many challenges in IoT environment are pointed out by various scholars.

The main challenge is preserving user privacy and their employed status with other connected smart objects. The smart objects that IoT uses are continuously producing data, it becomes more complex as these objects become anonymous. The objects' interaction with each other is one the most important aspects of IoT security.

A privacy preservation approach in a multiple IoT scheme has been proposed by the Serena et al. in [37], which prevents feature disclosure. The approach is based on t-closeness and k-anonymity notions from the database theory. These two notions derive group's robustness from privacy expectations. It prevents feature disclosure as well as information disclosure. Their scheme also protects from disruptive effects that occur from the malicious objects analysis. The key point in this paper is multi-network representation which depends on the correspondence on network of every identified group. In terms of node, every object can be modeled. Same group relationships between objects inside the present communication network are known as inner arcs, while in different group relationships they are known as cross arcs.

Some statistics of compromised IoT are given in Table 2. Shodan [38], Zoomeye and Censys are popular search engines for IoT devices vulnerabilities. The observations made by authors regarding IoTs include host-based approaches being more vulnerable than network-based in IoT platform, and traditional security measures for IoT devices are not properly secure. The main challenge is that the devices are resource constrained. Other than blockchain, many solutions have also been proposed for privacy preservation in IoT, including holochain [39,40], machine learning [41,42], IOTA [43,44], and intrusion detection system [45].

Table 2. Statistics of broken IoT [38].

	Top Countries	Count
1	United States	21,258
2	China	8655
3	Germany	5647
4	Russian Federation	3869
5	France	3660
6	Korea	3407
7	Italy	2858
8	Taiwan	2639
9	Japan	2368
10	United Kingdom	2176

2.3.2. Complex Heterogeneity Impact on IoT

In the design of IoT protocols, heterogeneity plays a vital role. Interaction of resource-constrained IoT devices such as cloudlets, web servers and blockchain either involve gateways or direct communication. The lightweight security mechanisms need to be implemented for secure end-to-end communication, as access policy and data summarization related mechanisms that enable transparency are controlling our lives silently. Figure 2 shows heterogeneous structure of IoT. It includes four layers; sensors, networks, cloud servers and consumer applications.

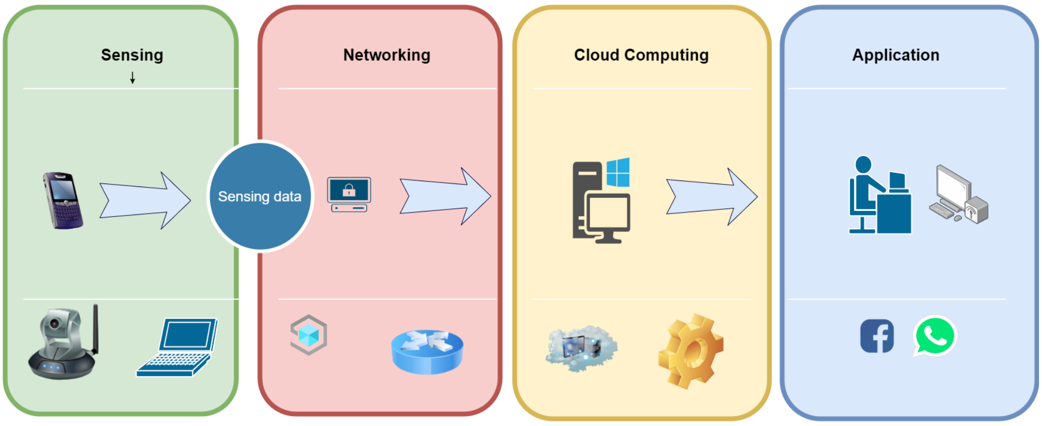

Figure 2. Heterogeneous IoT structure.

- Sensing: In this layer, the architecture of IoT provides sensing information for cloud computing to make appropriate decisions by recording and monitoring user data with the help of different kind of sensors e.g. color, camera, motion, flame, etc. Node location leakage is one vulnerability in such kind of heterogeneous IoT which can be address by smart sensor nodes.
- Networking: For forwarding data from source to destination, network layer is responsible in heterogeneous IoT. Due to which, higher transmission rates are provided by the network models like hybrid, star, mesh, and tree networks. The transmission of data through super nodes and relay units to cloud servers is done by network models. They also manage efficient construction mechanisms. Data throughput, energy consumption and malicious attacks are the limitations of network models.
- Cloud Computing: Heterogeneous IoT is accurately handling the large amounts of data with cloud computing. Its main function is to receive and transmit data to and from other architecture layers [46]. Strong analytical computing, storage of data,

emergency response strategies and efficient decision making are the advantages of cloud computing.

2.4. Applications

The applications of IoT range from healthcare to smart homes. The rapidly growing number of IoT applications makes it a technology that changes the way things work.

Authors in [47] discuss key technologies of industry 14.0, including IIoT. The structure of IIoT technology is shown, including four layers; sensing layer, network layer, service layer and interface layer. Authors show that IIoT requires real-time data availability and high reliability, unlike IoT, to increase product efficiency.

2.5. IoT's Security Mechanism Deployment

To preserve Confidentiality, infrastructure, data integrity, security and privacy, strong security mitigation mechanisms are required. Figure 3 shows trends of methods used by researchers for countermeasures and mitigation of attacks in IoT. Figure 3 shows that authentication is most popular security technique which is used by 49%, almost half of other techniques altogether, trust management is second most popular technique due to detection and prevention abilities while blockchain is the last.

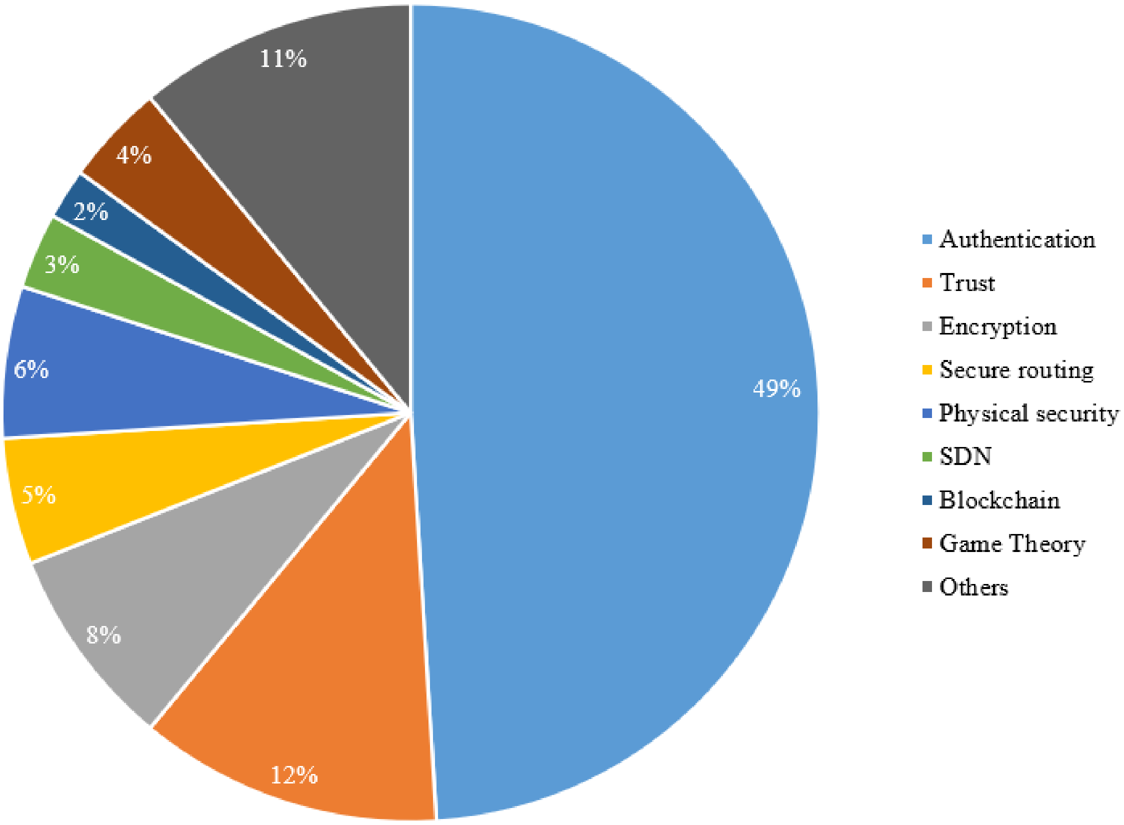

Figure 3. IoT security publications (2016–June 2018) in Elsevier, IEEE, Hindawi and Springer [48].

3. Blockchain

3.1. Overview

In recent years, we have seen that the IoT's potential of delivering services is increasing in several sectors by using different kinds of domains. The data transfer among a huge number of IoT devices is a major challenge. Recently blockchain [5,49,50] has been covering all the major areas of IoT with trustful and anonymous transactions in decentralized environment. Table 3 points to other survey papers addressed in this survey.

Table 3. Content discussed in different surveys based on Blockchain (x is for not covered, * is for partially covered).

References	Survey Based on Blockchain	Addressed in Our Survey
[5,49,50]	Decentralized consensus with blockchain taxonomy	*
[10,51–53]	Blockchain applications	Yes
[22]	Blockchain-based trust model	*
[14,17,54,55]	Blockchain-based security services	*
[47,56–58]	IoT/IIoT security and its integration with blockchain	Yes
[26,58]	Privacy issues in blockchain	x
[59,60]	Smart Contract	x
[61]	Sidechain technology	x
[10,18,22–25,62]	Ongoing research challenges	Yes
[63,64]	Blockchain security	*
[65,66]	Blockchain in industry	x
[27,67,68]	Privacy protection	*

IoT with blockchain integration benefits the users with decentralized nature of resources, low operational cost and robust behavior. Blockchain, a technology based on distributed ledger, initially developed for cryptocurrencies like Bitcoin, provides integrity, immutability, decentralization, transparency and pseudonymity. Satoshi Nakamato [4] in 2008 introduced the bitcoin technology using blockchain. Since then, blockchain gained attention for decentralized nature of data sharing and distributed network of computing. Through adoption of cryptographic technology with decentralized control and storage of data in the system, controlling attacks can be avoided.

Due to uniqueness and advanced features like immutability, integrity, transparency, authorization, auditability and transactional privacy, blockchain has been used in different sectors before cryptocurrencies. Identity management[69], mobile crowd sensing [70], Internet of energy [11,71–73], agriculture [74], supply chain management and industry 4.0 [75,76] are some areas of it.

Figure 4 shows the structure of blockchain, which is a combination of different blocks linking together in a linear fashion. In a peer-to-peer network of blockchain nodes, digital signed transactions are maintained in a public ledger. Two types of keys are used in blockchain, public key is used for encryption of data while the corresponding private key is used to decrypt the ciphertext. A user also uses private key for signing and public key for unique addressing. Transaction broadcasting and signing are done at the initial stage. When transaction is received by the peers, validation of transaction and its dissemination over the network takes place. To achieve consensus, validation of the newly issued transactions is done by all the nodes present in the network. Miners act like special nodes in a distributed consensus that participate in transaction issuance. The block, once generated, is broadcast by the miners in the network. In this way, every node in the network has a copy of the transaction and can verify it. Verification only involves computing a hash, which is not computationally expensive as opposed to transaction generation, this is why any node in the network can verify a transaction.

Blockchain is divided into three categories, public blockchain, which is permissionless, private blockchain, which is permissioned and consortium blockchain, which is a combination of both. All types provide immunity against malicious and faulty ledger users. Table 4 shows properties of all four types of blockchain. Their detailed example is presented in [10] by T. M. Fernández et al. Strengths of blockchain include accuracy, cost reduction, decentralization, efficiency, immutability, transparency and privacy.

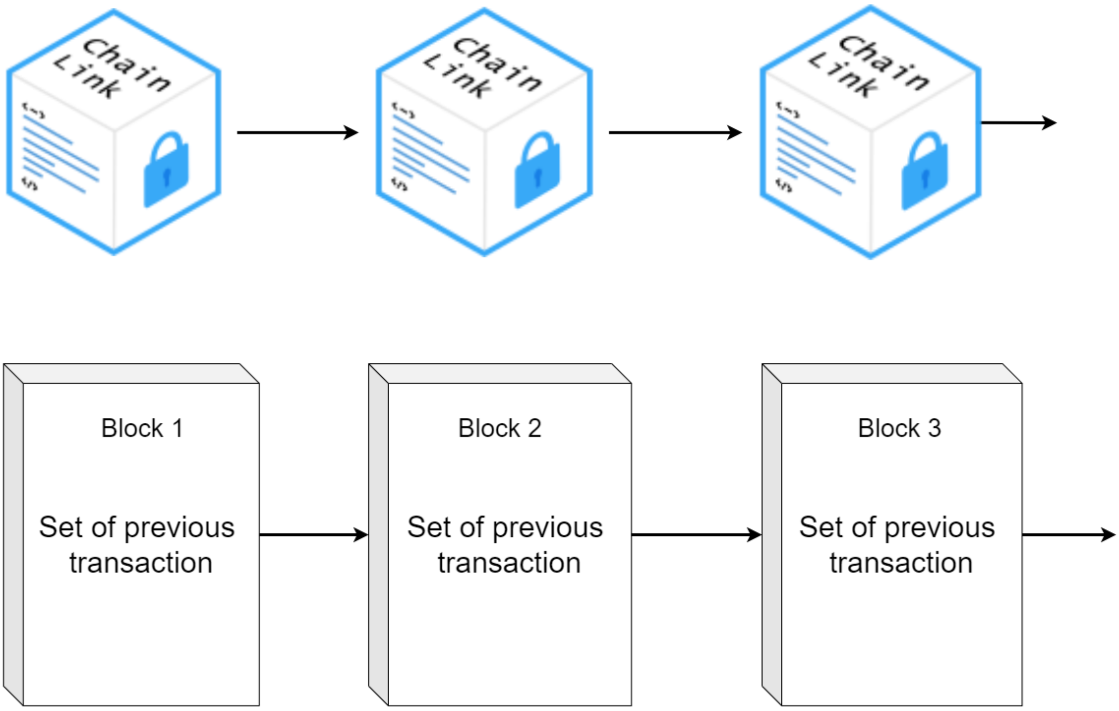
Chain Link
Chain Link
Chain Link
Block 1
Set of previous transaction
Block 2
Set of previous transaction
Block 3
Set of previous transaction

Figure 4. Structure of Blockchain.

Table 4. Types of blockchain and their properties.

Properties	**Public Blockchain**	**Private Blockchain**	**Consortium Blockchain**	**Hybrid Blockchain**
Access Restrictions	Permissioned for public	Permission needed to join the network	Permissioned	Permissioned
Transaction Restrictions	Permissioned for public	Restricted	Customized	Customized
Mining	Permissioned for public	Restricted	Customized	Customized
Decentralization	Fully decentralized	Centralized	Less centralized than private, and less decentralized than public blockchain.	Decentralized
Need for a Controlling Entity	None	Managed by a single organization	Managed by multiple organizations	Public and private module
Transparency	Yes	No	Little transparency	Little transparency
Incentive for mining	Yes	No	No	No
Examples	Bitcoin, Ethereum, Litecoin, NEO	Hyperledger and R3 Corda, Multichain, Hyperledger Sawtooth	Marco Polo, Energy Web Foundation, IBM Food Trust	Dragonchain, XinFin's Hybrid blockchain
Uses	Voting, fund raising	Supply chain management	Banking, Research	Retail, Real estate

In an IoT scenario, blockchain's classification is done by authentication and authorization of IoT devices. Nowadays, in industries [77], investments are made in a huge amounts. Technical issues and challenges related to blockchain technology are gaining significant interest of researchers. Some challenges include forking, consensus protocol targeting, 51% vulnerability and problems with the creation of new blockchain [78]. Another important challenge is the huge amount of power required for blockchain maintenance.

3.2. *Applications*

Blockchain is being used in a number of fields in our everyday life. Some of the applications are discussed here.

Figure 5 shows some applications of blockchain in different fields, including IoT, healthcare, finance, agriculture and cryptocurrency.

In IoT, blockchain is used to secure smart appliances [79,80] and supply chain management [81]. In healthcare, applications of blockchain include medical supply chain [82], drug traceability [83], secure record keeping [84], patient identity validation [85] and smart contracts [86,87]. In finance industry, the blockchain solutions include insurance [88], payments [89], asset management [90] and real estate management in smart cities [91]. In agriculture industry, some of blockchain applications include food supply chain [92], agriculture insurance [93] and smart farming [94,95]. Cryptoccurrency applications of blockchain include bitcoin and ethereum.

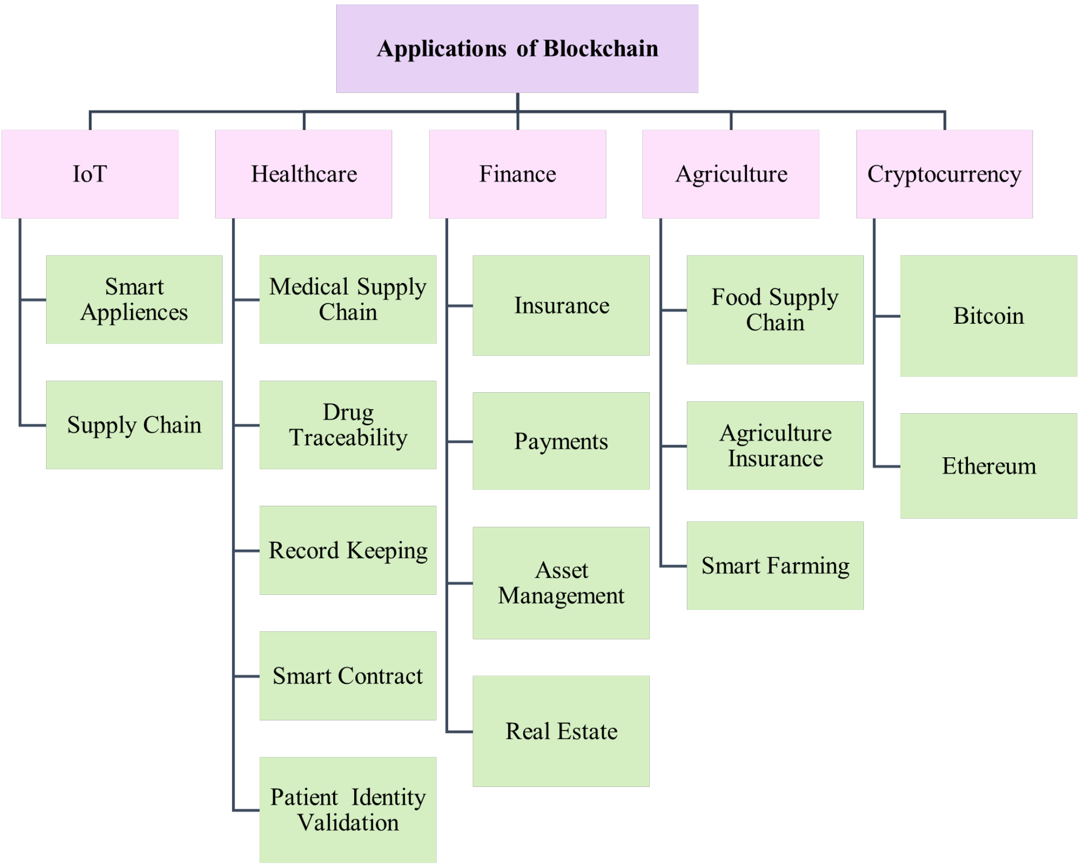

Figure 5. Applications of Blockchain.

Although it is infeasible to discuss all applications, we describe some of the most important applications of blockchain in the following subsections.

3.2.1. Banking

As blockchain ensures secure storage and immutability, it makes exchanging of funds more secure. Transactions, using blockchain, become transparent and private.

In [96], the authors have discussed the strengths of blockchain integration in commercial banking. This research analyzes the advantages for different aspects, including overseas payments, billing operations and asset security. The authors have concluded that the blockchain technology has the potential to decrease transaction costs and provide better efficiency.

A theoretical model is proposed in [97] in order to analyze the pattern, which allows enterprises to assess bank loans using blockchain. The authors demonstrate that blockchain allows consensus regarding the debt payments and other activities including lending and borrowing. This results in low-risk and high-quality of a small and medium sized enterprise's credibility.

In [98], Wang et al. proposed a model called IBPS (Inter-Bank Payment System) that utilizes Hyperledger Fabric enterprise blockchain technology. The proposed model provides efficiency and secure payment services.

3.2.2. Healthcare

Healthcare industry is benefiting from blockchain in many ways. Medical records can be stored in blockchain to be made more secure. The interaction among different IoT devices and wearable sensors is crucial in healthcare systems. There are systems that immediately notify the medical personnel upon an "event". An example of this event could be high sugar in a patient detected by a device that she is wearing.

The advantages of using blockchain in healthcare IoT are numerous, including security of records, secure management of data, privacy preservation of sensitive data, reliable remote monitoring of patients, non-repudiation, immutability and decentralization, as pointed out by [52]. The authors point out that most blockchain-based healthcare solutions use Ethereum platform. It is also shown that the healthcare systems mostly utilize private blockchain.

A blockchain-based framework is proposed in [99] that allows continuous patient monitoring using IoT. This scheme provides role-based access control and improves security and authentication in patient's smart devices.

To resolve issues regarding data sharing, scalability and quality of service, a blockchain-based solution is proposed in [100]. The proposed scheme is called ssHealth (smart and secure Healthcare system). This scheme allows remote monitoring of students while addressing the issues mentioned above.

In order to resolve security and privacy related challenges, a blockchain-based scheme is proposed in [101], which utilizes consortium blockchain in addition to a new consensus algorithm called MBFT (Mixed Byzantine Fault Tolerance). The proposed scheme provides privacy, fault tolerance and and better transaction handling. In [102], a scheme is proposed to eliminate single-point-of-failure, man-in-the-middle and data sniffing attacks using public blockchain. This scheme preserves data privacy, provides immutability and efficient identity management.

3.2.3. Supply Chain

Blockchain is used by suppliers to record the supplies purchased or to be purchased. An advantage provided by default by blockchain benefits supply chain greatly, which is non-repudiation. Due to non-repudiation, a buyer cannot deny purchasing materials from a seller.

In [103], a multi-ledger tracking framework is proposed that simplifies supply chain management. The proposed framework consists of two layers; layer 1 uses multiple private sub-ledgers and layer 2 utilizes a public ledger. A single shipment is represented by the sub-ledgers. Public ledger is used to track information, which is publicly available. The framework consists of index server, peers, admin node and external monitoring nodes. A record of all activities is maintained by the admin node. The index server stores the addresses of the nodes in the network, peers include nodes, admin node is used to keep record of all networking activities and external nodes verify and track the shipment status.

Chen et al. have proposed a blockchain-based conceptual framework in [103] to improve supply chain management. The proposed framework consists of four layers; IoT sensors layer, data layer, contract layer and business layer. In this way, the functionalities of each service are provided. Sensor layer is used to track the goods, data layer consists of blockchain and smart contracts, the contract layer ensures data quality and contract layer executes the processes related to business management.

3.2.4. Electronic Voting

Election fraud is prevented using blockchain. Blockchain in voting works in the way that a block is added to the blockchain upon a successful vote. As blockchain brings immutability and integrity, it ensures that the records cannot be changed. Voting also benefits from transparency that blockchain brings, as the records are kept transparent in the network. In this subsection, we briefly discuss the strengths of blockchain-based voting schemes proposed in recent literature. Blockchain-based electronic voting is discussed in detail in [53]. This survey reviews the literature and discusses its strengths and limitations. The authors point out that transparency and decentralization are most useful features of blockchain to be used by electronic voting systems, whereas limitations include scalability issues and coercion resistance.

In [104], a blockchain-based transparent ballot box protocol has been proposed that follows e-voting properties and provides decentralization. The proposed scheme allows the elector to modify the vote in allowed voting phase. A protocol has been proposed in [105] called VYV (Verify Your Vote) based on blockchain. This protocol provides fairness, vote privacy and verifiability. In [106], a scheme is proposed to eliminate the need of a third party and decentralize the voting network using blockchain. The strengths of this scheme include public verifiability, consistency, auditability, transparency and user anonymity. A blockchain-based protocol is proposed in [107] that utilizes homomorphic ElGamal encryption. The authors claim that their scheme guarantees privacy preservation and anonymity.

3.2.5. Smart Cities

Blockchain smart contracts can be integrated with properties like cars, houses, patents, etc. Decentralization, immutability, pseudonymity and transparency are useful features of blockchain for smart cities. In [51], authors review recent literature on blockchain-based energy consumption systems. Authors conclude that energy consumption in smart cities can be made efficient using blockchain, because blockchain provides decentralization, anonymity, transparency, and tamper-proofing.

In [108], blockchain is used to propose personal archive storage scheme to provide authenticity, accuracy and transparency. The different actors in the proposed scheme include subject, certifier, client and stake node. Subject owns digital artifacts, certifier issues a certificate to the subject, client is someone who requests to access personal digital artifacts and stake node maintains blockchain ledger. This scheme provides secure storage and efficient authentication.

In [109], a blockchain-based framework called BC-PDS (Blockchain-based Personal Data Store) has been proposed for personal data storage. This scheme utilizes existing OpenPDS/SafeAnswers framework. For anonymization, this scheme uses AutoNomy-based Access Control (ANAC).

3.3. Smart Contracts

In public blockchain, all participating nodes have the privilege to deploy smart contracts without needing any prerequisites. In Ethereum, solidity language is used for creating contracts while Metamask is used for ID creation and Remix IDE is used for its online demonstration and results of applications.

Computer programs and codes that can work anonymously are known as smart contracts. They provide an agreement or a consensus between the two parties involved. Users cannot alter or delete a smart contract once it is published on the blockchain network. No central authority involvement is needed for validation of tasks. The results computed by the nodes in the network do not have any interference from outside the network. Banking, supply chain, IoT and insurance industries are deploying permissioned smart contracts.

In [110], Rathee et al. proposed a framework for connected and autonomous vehicles (CAV), in which smart contracts with blockchain are implemented for security assurance of vehicles. Verification of registration providers and tracking or alteration of user data can be handled through it.

Through smart contracts, mobility services and smart transportation are implemented and defined by IPFS in [111], in which DLTs (Distributed Ledger Technologies)-based infrastructure with distributed data management technologies have been used for data sharing and providing smart services. In [112], Ethereum smart contract and IOTA-based architecture for authenticity has been proposed by Zichichi et al., in which the entities' co-ordination, access authorization, and privacy of users have been achieved. Zero knowledge proof for privacy offering and the guarantee for proof of location has been used.

A system CHORUS mobility in [113], whereas, in [114], a decentralized system has been presented for smart transportation system with the combination of VANETs and Ethereum for rules enforcement.

3.4. Consensus

An important part and key contribution of blockchain is its consensus mechanisms. Consensus mechanisms are used to make agreement between different parties in a distributed environment to append blocks in the blockchain. There are two main types of consensus mechanisms; proof-based consensus and voting-based consensus. Proof-based consensus involves adding blocks by the qualified individuals and voting-based mechanism involves sharing the results of transaction in order to make the final decision. A very important and basic part of bitcoin is POW (Proof of Work) [4], which involves intensive mathematical computations. In terms of resource and energy consumption, POW is very expensive. Given the heaviness and cost of the task, PoW still seems the best solution because it prevents spamming and DoS attacks.

POW is hard to be performed but it is easy to be verified once performed. In case of bitcoin, this task is performed by the miners and verifiable by everyone in the network who is a part of blockchain peer-to-peer network. Miners are given incentives because the task they perform successfully is fundamentally very expensive. A new block in blockchain can only be added after solving an expensive mathematical task.

3.4.1. Proof-Based Consensus

There are following proof-based consensus algorithms.

- Proof of Work (POW) Consensus: First use of PoW consensus started with Bitcoin and became popular after it. It was originally used to verify the transactions and for mining purpose. When a miner mines a transaction, he has to solve a mathematical puzzle. The puzzle involves looking for a value that when hashed generates a specific value. This puzzle is fundamentally computationally expensive. A new block cannot be added to the blockchain without successfully mining it. Once a miner finds a solution to the puzzle, it is broadcasted in the network and can be verified by any or all of the peers. Validation is a cheap task in terms of computational resources it consumes, as it only involves hashing a value, and hence can be done by anyone in the network. As it takes lots of computing resources to solve this puzzle, the miners are given an intentive. After Bitcoin, PoW has been implemented in other several cryptocurrencies, namely Litecoin, Dash and Monero.
- Proof of Stake (PoS) Consensus: In PoW, multiple miners are attempting to solve the mathematical puzzle at the same time. The first successful miner is given an incentive for adding a block in the blockchain, but for other miners, this process was a waste of computing resources. This limitation of PoW is covered by PoS. In PoS, miners are in no competition with each other. The validator receives a transaction fee for addition of a new block. In this way, the total amount of currency always remains the same in the network. Also, the validator is elected beforehand in PoS, unlike PoW, where anyone with enough computational resources in the nwtwork can mine. No one except this elected validator can add a new block. Anyone who wants to be elected has to put a part of his currency at stake. The amount of currency put

at stack is directly proportional to the chances of being elected as a validator. After the successful validation, the validator receives the staked currency as well as the transaction fees, and the other candidates get their staked amount back. PoS is used by Nxt.

- Hybrid PoW and PoS: A comparison between PoS and PoW is given in Table 5. It shows properties of both the consensus mechanisms and hybrid consensus mechanism. However, some schemes use a hybrid of both PoS and PoW consensus mechanisms. The key advantage of using this hybrid is getting the advantages from both of these schemes and using one scheme to overcome the limitation of the other one. A hybrid consensus mechanism has been used by Decred cryptocurrency.

Table 5. A comparison between PoW and PoS.

Criteria	PoW	PoS	Hybrid
Energy consumption	A lot of energy wastage	Less energy consumed (energy efficient)	A significant amount of energy is consumed
Scalability	Not scalable	Scalable	Partially scalable
Centralization	Decentralized	Partially centralized	Partially centralized
Forking	Likely	Difficult	Possible
Speed of block creation	Slow	Fast	Low
Double spending attack	Possible	Difficult	Not as severe as in PoW
51% hash power attack	Possible	Not applicable	Not applicable
Advanced hardware requirement	Required	Not required	Required
Applications	Bitcoin	NextCoin	Blackcoin

3.4.2. Voting-Based Consensus

Voting-based consensus algorithms include the following.

- Proof of Capacity (PoC) Consensus: Started with Burstcoin, the PoC mechanism decreases the usage of computational resources and uses storage resources. Before mining is started, miners store the set of possible solutions of the puzzle. The miner who has more storage tends to store more solutions. Thus, the miners with more storage space have higher chances of mining.
- Proof of Burn (PoB) Consensus: A concept named “eater address” is used in PoB. Before starting mining, the miners send coins to an invalid address randomly. Blocks are created and these addresses are changes. The coins sent to these addresses are not usable anymore because of the fact that these addresses are invalid and unknown. The process is repeated until there is only one miner left that has some more coins to invest. This miner receives the mining coins and the transaction fees as a reward. Miners that have been investing in creation of blocks in the past are given more privileges. PoB is used by Slimcoin.
- Proof of Importance (PoI) Consensus: PoI is a score-based protocol that was first used with NEM cryptocurrency. The individual who invests more coins in the network makes the higher score. This score is affected by the number of transactions and the size of transactions. The lower limit for investing coins in 10,000 coins. The user with highest score has the highest chance of being a validator.

4. Integration of Blockchain and IoT

Many researches integrate blockchain in IoT to enhance security and provide an efficient data storage system. In [56], authors review the recent literature on blockchain’s integration with IoT. It is pointed out that blockchain helps to improve security and scalability in IoT scenarios. In [62], authors highlight some attacks that IoT systems are prone to, and review the researches that use blockchain to mitigate privacy-related issues in IoT.

This section explains why blockchain is useful in an IoT environment.

4.1. Opportunities Brought by Blockchain in IoT

Blockchain brings many opportunities in IoT. Integration of blockchain in IoT has been increasing in IoT since Bitcoin.

4.1.1. Secure Storage

IoT devices collect data and transmit it across other devices. These devices are connected to each other through Internet, and a lot of IoT devices use cloud computing in order to keep the data synchronized. This data, if compromised, can result in loss of security and privacy of a user. Blockchain can be used to securely use and transmit this data across the network. Also, blockchain makes the records immutable, so no records can be modified by a malicious user, specifically healthcare records that need to be kept secure.

4.1.2. Decentralization

As IoT devices are distributed, blockchain provides an efficient and convenient solution for decentralization. Data can be maintained in the blockchain and published without the fear of potential modifications to be made by a malicious third party. As seen in bitcoin, blockchain provides decentralization solution in P2P networks [4]. The data are distributed using blockchain among other IoT devices in a decentralized fashion. In this way, the use of blockchain also eradicates the need of a central entity, such as a cloud server. Another advantage that comes from this property of blockchain is removal of a single-point-of-failure, because when a central entity is involved, it becomes a target of malicious users.

4.1.3. Encryption

Blockchain stores hashes of the data in the ledger, which makes it light-weighted, as hash functions generate a small and fixed size of output for any size of input. The actual data are usually stored on a cloud server and hashes are kept in the blockchain. Blockchain usually utilizes SHA-256 algorithm for hashing. Symmetric encryption in blockchain provides user and transaction security, prevents double-spending problem and verification of digital asset transfer. Because of secure encryption mechanisms that blockchain provides, authors of [58] point out that it can be used to guarantee privacy preservation in IoT and IIoT. It is concluded that blockchain can help to pave better and more efficient ways for businesses in IoT industry, such as mobile commerce, food logistics management, electric vehicles, etc.

4.1.4. Access Control

Traditional access control systems are shifting toward blockchain in IoT-based environments. Blockchain provides attribute-based and fine-grained encryption, granular attribute-based, and role-based access control solutions [36] for IoT.

Zhao et al. [115] proposed a message encryption scheme using symmetric key encryption. In this scheme, the data owner uses attribute-based encryption to encrypt a message with default attributes and sends the ciphertext to the encryption proxy server. Xu et al. [116] utilize smart contracts with capability-based solutions that achieve high scalability and interoperability while focusing on delegation. However, authorization model is not provided in the paper.

A blockchain-based architecture for IoT privacy preservation is proposed by Rahulamathavan et al. [117], in which an attribute-based encryption has been used with Testbed platform to achieve data privacy and confidentiality, but there is a slight time increase due to involvement of multiple attribute authorities and using PoW consensus mechanism.

4.2. Applications of Blockchain in IoT

This section describes the uses of blockchain in different IoT scenarios.

4.2.1. Healthcare System

Different sensors have been introduced to detect and upload patient's information on cloud in emergency situations from a remote location. These sensors/devices can automatically communicate with the medical personnel upon detecting a certain threshold. Using IoT, patients can be checked up from remote locations through these sensors and it is often possible. In addition to checkup, it is also used to treat the patients. This can, in many cases, help save a life and provide medical help to patients in emergency situations in time. Blockchain comes with many benefits that could be helpful for IoT when it comes to healthcare systems. It can protect the privacy and security of critical data stored in eHealth systems. When needed, it can also allow to use the data without modifying it.

4.2.2. Software Defined Network

Software defined networking technology has been proposed for increasing bandwidth of IoT devices. The processing of decision making is simplified and intelligent routing is provided. An example is DiskBlockNet; an IoT network architecture with distributed network that provides flexibility and scalability without central controlling server. In this distributed network of blockchain, two kinds of nodes are present, verification node for maintaining the information flow of tables and responding node to update table flow rules.

4.2.3. Crowdsensing Applications

Crowdsensing is a novel kind of mobile IoT, like geo sensing. On blockchain cryptocurrencies, privacy preservation incentive mechanism was developed by Wang et al. [70]. Which eliminates privacy and security issues like impersonation attacks, with the help of transparent blockchain and data verification by the miners.

4.2.4. Energy Systems

Future of energy systems is known as smart grids which are the replacement of traditional energy systems due to the involvement of ICT (Information and Communication Technology). Because of various advantages like cost effectiveness, uninterrupted power supply and two-way communication, smart grid is considered as the next generation of energy systems [118].

4.2.5. Internet of Vehicles

Establishment of smart communication between heterogeneous networks and vehicles (V) like V to Road, V to V, V to Infrastructure, V to Sensor, V to Everything and V to Human are some emerging technologies in IoT. Many authors proposed various decentralized security models like LNSC, for managing charging pile and electric vehicle [119] by using ECC and hash functions.

4.3. Blockchain-Based IoT Privacy Preserving Schemes

As IoT consists of billions of devices accross the world, it poses serious threats to the privacy of the users. Other than providing decentralization, consensus and smart contracts for IoT, blockchain is being used at a large scale to assure privacy preservation in IoT. Table 6 presents a summary of recent researches based on the scheme utilizing blockchain for privacy preservation in IoT.

Table 6. Recent research on blockchain-based privacy preservation in IoT.

Ref#	Model	Limitations	Parameters	Strengths	Tools-Technology
[120]	Software defined networking for IoT	Lack of location privacy	Distributed blockchain cloud architecture	Dos/Dos attacks, Data protection, Access control, reduced end to end delay between IoT devices	SDN controller, 6 desktops, 64 Gb DDR3 ram, intel i7
[121]	Collaborative video delivery	Lack of privacy and anonymity	Smart contracts	Provide requested service through network service chains	Hyperledger fabric, pbft consensus, CLCs
[70]	Crowd sensing app	Collusion attacks	whitewashing attack, QAIM	privacy preserving, impersonation attacks	K anonymity, server with k nodes, EM algo in Ubuntu 16.04 environment
[122]	Scalable access management	Cryptocurrency fees, processing time	Mobility, accessibility, concurrency, lightweight, scalability, transparency	Access control	Ubuntu 16.04 desktop, intel core i7 -950 , 3.07 !GHz
[11]	Secured Grid monitoring	Lack of location privacy	Sovereign blockchain network, cryptographic keys	Data integrity, data confidentiality, data provenance and auditing	Smart contracts, sha256, smart meters
[71]	Internet of Energy	data provenance and auditing	SCADA network, data encryption and broadcast	False data injection attacks	54 generators, 118 nodes, 186 branches, 676 communication channels, 676 sensors.
[75]	Consortium blockhain in industrial IoT	Lack of privacy and anonymity, optimal energy aggregator selection	Optimal pricing, credit-based payment	Secure energy trading	50 pairs if IIoT nodes, Traditional blockchain, EAGs
[72]	Decentralized energy trading through multisig and BC	Collusion attacks	Anonymous encrypted message streams,	Privacy, double spending attacks	Python 2.7 with bitcoinlib, libbitcoin toolkit, PYBitmessage API, pysolar
[123]	Consortium BC in Mobile devices	Lack of privacy and anonymity	Fuzzy comparison method, MFM	Malware detection	Intel core i7-3770, 16 GB, Ubuntu 15.10, DREbin dataset
[75]	Secure firmware in IoT environment	Data credibility assessment	Remote firmware updates, p2p sharing	Firmware verification and update	BAN logic, Scyther tool, merkle tree
[124]	Bitcoin	Public key privacy	Paillier cryptosystem, Overlay attack, Double-spending attack	Provably Secure	Multi-layered Linkable Spontaneous Anony-mous Group signature (MLSAG), ring signature

4.3.1. Anonymization

Recently, many schemes have been proposed for blockchain-based privacy preservation in IoT. For electric vehicles, a blockchain-based privacy preserving charging system has been proposed in [125]. In this scheme, for every session, a new pair of keys are generated by the system. Other than that, for providing anonymity protection in blockchain, the techniques like ring signatures, non-interactive zero knowledge and mixing services are frequently used.

Some limitations of anonymization include high computation cost, de-anonymization and loss of meaningful information through generalization and suppression.

4.3.2. Ring Signatures

To improv privacy in blockchain significantly, a set of choices need to be made without the need of a central manager. For generation of anonymous signatures from possible signers group, without identity disclosure, a scheme is proposed by fujisaki et al. in [126]. Linkability and anonymity are properties that are achieved through ring signatures-based privacy preserving mechanisms [127–129].

In [127], Saberhagen et al. proposed CrptoNote. In this scheme, with single private key, the user can sign one valid transaction. It is a modification of ring signatures, which mitigates the attacks like double spending by replacing tags with image of key computing. The signer identity can only be disclosed when he uses the same pair of keys for second signature.

RingCT is an improvement of CryptoNote, which provides transactional privacy as well as identity privacy by Noether et al [128]. Ring signatures with Greg Maxwell's Confidential Transaction [130]a are used for hiding the amount whereas the amount is placed at MLSAG (Multilayer Linkable Spontaneous Anonymous Group Signature) [131]. Monero is a strong implementation of this approach [129]. In [132], heavily centralized intermediaries were used but they are also vulnerable to security attacks. In Creditcoin [57], anonymized ring signatures announcements have been proposed in which user's privacy can achieved. In this work, an incentive-based network has also been created.

Limitation of ring signatures include the following:

- Large size of transactions increases the storage space of blockchain records.
- Size of ring signature is directly proportional to the number of participants, that is why only limited number of outputs are generated.
- Auditing difficulty is also faced due to hidden amount.

4.3.3. Non Interactive Zero Knowledge

It is an alternative approach of zero knowledge proof. Message verification can be done in an anonymous way because of not having an interaction between verifier and prover. A scheme was proposed by Blum et al. [133], in which, the correctness of assertion can be proven without leaking any information.

ZeroCash [134] and ZeroCoin [135] are two blockchain-based anonymization schemes in which ZKP concept has been used for the prevention of transactional data leakage. At high computational cost, Zerocash achieves the highest level of anonymization. In contrast, Hawk [136] is the first work to provide programmability and transactional privacy in blockchain.

Limitations of non interactive zero knowledge include high computational cost of transactions proof, fixed coin dominations in zerocoin and unprotected public transaction lists.

4.3.4. Mixing

For mitigation of analytical attack, which is used for accessing the sender or receiver transaction's privacy information, in a blockchain system, mixing approach has been used, which is also known as laundry or tumbler. Chaum [137] presented the service, in which communication content as well as sender and receiver information can be hidden.

Currently, to reduce de-anonymization risk and obfuscation of transaction history, the researchers are focusing on centralized and decentralized mixing strategies. Many mixing websites like onion bc, bitcoin fog, bitmixer, helix by grams, bit laundry, send shared and bitblender are available. By providing some fees they can provide anonymous mixing transaction service. Some services are only provided through TOR network, on which, free worldwide anonymous communication has been enabled.

By not transferring data to the receiver, the attacker steals the user asset [138]. Disclosure of personnel data is not ensured by the system because, in transactions, routing the service provider keeps the user log. Conditional execution is the first solution, in which the mixer only gets reward when it correctly operates, otherwise it does not get any rewards from the user. CoinSwap is a bitcoin mixing protocol introduced by Gregory et al. [130], in which transactions are done in escrow mechanism structure with hash lock protection. An accountable mechanism based on signatures, Mixcoin has been proposed by Bonneau et al. [139] that exposes the misbehaving mixer by unambiguous proof made by the users.

Another solution is Blind signature scheme, in which a message is blinded by the system before the signing of the message. Blinding, signing and unblinding are three steps. It is publicly verifiable, whereas the origin and connection is hidden from the signer. Blindcoin [140] is a combination of append-only public log with blind signature scheme for accountability of mixing process. For mixing fairness and providing anonymity, smart contracts with blind signatures are applied by Hielman et al. in [141].

Dash [142] made the first anonymity attempt in digital currency environment which was released in 2014. Removal of a user's unique information on blockchain is done in this project, called PrivateSend. To avoid coin theft and achieve complete unlinkability, TumbleBit [143] was proposed. A strategy for financial transactions decentralization, CoinShuffle by Ruffing et al. [144] was introduced. Through decentralized blockchain behavior mixing with third party, removal has been ensured.

Mixing Limitations include the following:

- For fair exchange of transactions, the executional process or online participants waiting creates a huge delay.
- A single point of failure exists due to centralized nature of the server. This makes the server vulnerable to DoS attacks.
- High mixing fees are a problem for users in fair exchange of transactions. Due to low anonymity level, mixing protocol can easily be compromised through Sybil attacks [145].
- The leakage of transaction privacy through backtracking analysis of transactional graph is a serious issue.

4.3.5. Differential Privacy

To achieve the data confidentiality without leakage risks through privacy preservation, a technique has been proposed known as differential privacy by C Dwork, who made a database protection mechanism which adds noise at each query evaluation [146]. For protection of health care systems, data perturbation mechanism has been used by Dagher et al. in [147]. In [148], a scheme is presented to protect a smart home resident's privacy through multiple pseudonym techniques. Traffic encryption has been done for providing data authenticity, access control and confidentiality.

Differential privacy limitations include:

- Differential privacy provides privacy-utility trade-off. Precision in Data and loss of certainty are the results of increasing noise addition for enhancing the privacy level [149].
- It is prone to timing analysis attack in traffic flow obfuscation mechanisms [150].

5. Conclusions

Despite of all the opportunities that IoT brings, it suffers from issues like heterogeneity of IoT devices, resource constraints, and poor interoperability between these devices. Other important challenges in IoT include privacy, availability, confidentiality and integrity. Blockchain comes with opportunities like immutability, decentralization, transparency, integrity, consensus, confidentiality, non-repudiation, privacy and security in a distributed network. When blockchain is implemented in IoT, it provides solutions to the problems faced.

The aim of this paper has been to provide a comprehensive survey of the problems faced by IoT and the solutions provided by the blockchain technology. We first discussed blockchain and IoT separately. We looked at the applications, advantages and limitations of both of these technologies. We then analyzed the impact that blockchain has on IoT. We discussed how IoT is benefited by blockchain, based on the opportunities and strengths of blockchain. We reviewed researches based on the implementation of blockchain in IoT in resource constrained environments. It is highlighted that the use of blockchain is increasing in IoT and providing the solutions that it needs, from healthcare to smart homes to military.

IoT uses a large number of devices and most of these devices are resource-constrained. Blockchain being light-weighted is a great solution for privacy preservation in resource-constrained devices. The privacy aspect of blockchain comes from its ability to provide transparency in a distributed network. We have seen that the use of blockchain, other than providing immutability, decentralization, and consensus, it helps preserving user′s privacy in IoT environment.

6. Future Research Directions and Challenges

Privacy preservation is important because users' data is collected by almost all IoT devices. We present some future research directions in terms of privacy preservation.

6.1. IOTA Ledger

In order to provide security and privacy, integration of the Tangle in IoT can be very useful. Tangle is a data structure that IOTA is based on. It utilizes a directed acyclic graph and utilizes less energy as compared to a blockchain network. IOTA is light-weighted and quantum resistant. Another important advantage is that IOTA does not need miners. The network participants issue new transactions without having to involve another node that has better computing resources. Having no miners makes IOTA fee-less.

6.2. Strong Privacy Preservation Mechanisms

Strong privacy preservation is still a challenge when using blockchain. For example, in order to resist Sybil attack, a certain amount of honest participants are required in decentralized mixing protocol. Hawk reinitializes and creates a different trusted process for every smart contract, so privacy preservation having few trust assumptions needs to be enhanced.

6.3. Security Framework

A single security solution for all blockchain-based IoT devices cannot fulfill security requirement due to resources-constrained nature of devices. The designs of such kinds of frameworks are required to provide dynamic and adaptable security. Implementation of other privacy preserving solutions, such as data anonymization and differential privacy along with blockchain, can provide better privacy. A framework is needed that can preserve privacy using both the techniques, keeping resource-constrained nature of IoT devices in mind.

6.4. Blockchain-Based Infrastructure

The storage in decentralized large-sized blockchain is also an issue, as we have seen that IoT devices are storing data continuously whether it is useful or not which increases the blockchain data and makes it heavy. Since all nodes in the blockchain network are required to keep a local copy of the ledger, it becomes infeasible for light-weighted devices to store a copy of the ledger. A framework is required that reduces the storage overhead on small IoT devices caused by blockchain maintenance.

Author Contributions: Conceptualization, Z.I., S.Y.A.Z. and M.A.S.; Funding acquisition, Y.J. and Z.I.K.; Investigation, Y.J., Z.I.K. and K.A.; Project administration, Y.J., M.A.S., Z.I.K., S.M. and K.A.; Supervision, Y.J., M.A.S., Z.I.K., S.M. and K.A.; Validation, Y.J., Z.I.K., S.M. and K.A.; Writing—original draft, Z.I. and S.Y.A.Z.; Writing—review & editing, Z.I., S.Y.A.Z. and M.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

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

References

1. Gartner, R. *Forecast: The Internet of Things, Worldwide, The Internet of Things*; Forecast: Egham, UK, 2017.
2. Baccelli, E.; Hahm, O.; Günes, M.; Wählisch, M.; Schmidt, T. RIOT OS: Towards an OS for the Internet of Things. In Proceedings of the 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Turin, Italy, 14–19 April 2013; pp. 79–80.
3. Dunkels, A.; Gronvall, B.; Voigt, T. Contiki-a lightweight and flexible operating system for tiny networked sensors. In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, Tampa, FL, USA, 16–18 November 2004; pp. 455–462.
4. Nakamoto, S.; Bitcoin, A. A Peer-To-Peer Electronic Cash System. Bitcoin. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 12 October 2020).
5. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
6. Sankar, L.; Sindhu, M.; Sethumadhavan, M. Survey of consensus protocols on blockchain applications. In Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017; pp. 1–5.
7. 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), Bangalore, India, 19–20 May 2017; pp. 2145–2148.
8. Khalilov, M.; Levi, A. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2543–2585. [CrossRef]
9. Conti, M.; Kumar, E.; Lal, C.; Ruj, S. A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3416–3452. [CrossRef]
10. Fernández-Caramés, T.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
11. Gao, J.; Asamoah, K.; Sifah, E.; Smahi, A.; Xia, Q.; Xia, H.; Dong, G. Gridmonitoring: Secured sovereign blockchain-based monitoring on smart grid. *IEEE Access* **2018**, *6*, 9917–9925. [CrossRef]
12. Peters, G.; Panayi, E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of money. In *Banking beyond Banks and Money*; Springer: Cham, Switzerland, 2016; pp. 239–278.
13. Brandão, A.; São Mamede, H.; Gonçalves, R. Systematic review of the literature, research on blockchain technology as support to the trust model proposed applied to smart places. In *World Conference on Information Systems and Technologies*; Springer: Cham, Switzerland, 2018; pp. 1163–1174.
14. Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security Services Using Blockchains: A State of the Art Survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 858–880.
15. Ziegeldorf, J.; Morchon, O.; Wehrle, K. Privacy in the Internet of Things: Threats and challenges. *Secur. Commun. Netw.* **2014**, *7*, 2728–2742. [CrossRef]
16. Sadeghi, A.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial Internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8 June 2015; pp. 1–6.
17. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
18. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the Internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; pp. 648–651.
19. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the Internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
20. Atzori, M. Blockchain-Based Architectures for the Internet of Things: A Survey. 2017; SSRN 2846810. Available online: https://www.semanticscholar.org/paper/Blockchain-Based-Architectures-for-the-Internet-of-Atzori/d92af0f420fd7bb72cdd08bd35cfd91b6c94fc88 (accessed on 4 February 2021).
21. Conoscenti, M.; Vetro, A.; De Martin, J. 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.
22. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. *Chall. Oppor. Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
23. Yeow, K.; Gani, A.; Ahmad, R.; Rodrigues, J.; Ko, K. Decentralized consensus for edge-centric Internet of things: A review, taxonomy, and research issues. *IEEE Access* **2017**, *6*, 1513–1524. [CrossRef]
24. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
25. Neudecker, T.; Hartenstein, H. Network layer aspects of permissionless blockchains. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 838–857. [CrossRef]

26. Wahab, J. Privacy in Blockchain Systems. *arXiv* **2018**, arXiv:1809.10642.
27. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
28. Elijah, O.; Rahman, T.; Orikumhi, I.; Leow, C.; Hindia, M. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet Things J.* **2018**, *5*, 3758–3773. [CrossRef]
29. Aashraya, A. IoT based military robot using raspberry Pi3. *Eur. J. Mol. Clin. Med.* **2020**, *7*, 4200–4212.
30. Routray, S.K.; Javali, A.; Sahoo, A.; Sharmila, K.; Anand, S. Military Applications of Satellite Based IoT. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20 August 2020; pp. 122–127.
31. Aslam, F.; Aimin, W.; Li, M.; Ur Rehman, K. Innovation in the era of IoT and industry 5.0: Absolute innovation management (AIM) framework. *Information* **2020**, *11*, 124. [CrossRef]
32. García-Magariño, I.; Nasralla, M.M.; Nazir, S. Real-time analysis of online sources for supporting business intelligence illustrated with bitcoin investments and iot smart-meter sensors in smart cities. *Electronics* **2020**, *9*, 1101. [CrossRef]
33. Arfi, W.B.; Nasr, I.B.; Kondrateva, G.; Hikkerova, L. The role of trust in intention to use the IoT in eHealth: Application of the modified UTAUT in a consumer context. *Technol. Forecast. Soc. Chang.* **2021**, *167*, 120688. [CrossRef]
34. Nebbione, G.; Calzarossa, M.C. Security of IoT application layer protocols: Challenges and findings. *Future Internet* **2020**, *12*, 55. [CrossRef]
35. Mahmood, Y.; Kama, N.; Azmi, A.; Ya'acob, S. An IoT based home automation integrated approach: Impact on society in sustainable development perspective. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 240–250. [CrossRef]
36. Darwish, A.; Hassanien, A.; Elhoseny, M.; Sangaiah, A.; Muhammad, K. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 4151–4166. [CrossRef]
37. Nicolazzo, S.; Nocera, A.; Ursino, D.; Virgili, L. A privacy-preserving approach to prevent feature disclosure in an IoT scenario. *Future Gener. Comput. Syst.* **2020**, *105*, 502–519. [CrossRef]
38. Shodan. March, Devices Vulnerable to Heartbleed. 2019. Available online: https://www.shodan.io/report/0Wew7Zq7 (accessed on 3 January 2021).
39. Janjua, K.; Shah, M.A.; Almogren, A.; Khattak, H.A.; Maple, C.; Din, I.U. Proactive forensics in iot: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies. *Electronics* **2020**, *9*, 1172. [CrossRef]
40. Zaman, S.; Khandaker, M.R.; Khan, R.T.; Tariq, F.; Wong, K.K. Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare. *arXiv* **2021**, arXiv:2103.01322.
41. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
42. Chatterjee, B.; Das, D.; Maity, S.; Sen, S. RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet Things J.* **2018**, *6*, 388–398. [CrossRef]
43. 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.
44. 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.
45. Smys, S.; Basar, A.; Wang, H. Hybrid intrusion detection system for internet of Things (IoT). *J. ISMAC* **2020**, *2*, 190–199. [CrossRef]
46. Jo, M.; Maksymyuk, T.; Strykhalyuk, B.; Cho, C. Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing. *IEEE Wirel. Commun.* **2015**, *22*, 50–58. [CrossRef]
47. Alcácer, V.; Cruz-Machado, V. Scanning the industry 4.0: A literature review on technologies for manufacturing systems. *Eng. Sci. Technol. Int. J.* **2019**, *22*, 899–919. [CrossRef]
48. Sahu, P.; Singh, D. Data breaches in iot a study and solution by puf approach. *Int. J. Adv. Electron. Comput. Sci.* **2019**, *6*, 12–16.
49. Puthal, D.; Malik, N.; Mohanty, S.; Kougianos, E.; Das, G. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [CrossRef]
50. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304.
51. Bao, J.; He, D.; Luo, M.; Choo, K.K.R. A survey of blockchain applications in the energy sector. *IEEE Syst. J.* **2020**. [CrossRef]
52. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. *IEEE Trans. Eng. Manag.* **2020**. [CrossRef]
53. Taş, R.; Tanrıöver, Ö.Ö. A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry* **2020**, *12*, 1328.
54. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
55. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Blockchain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731.

56. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29.
57. Li, C.; Palanisamy, B. Privacy in Internet of things: From principles to technologies. *IEEE Internet Things J.* **2018**, *6*, 488–505. [CrossRef]
58. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2019**, *10*, 100081. [CrossRef]
59. Singh, A.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R.; Dehghantanha, A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Comput. Secur.* **2020**, *88*, 101654. [CrossRef]
60. Wang, Z.; Jin, H.; Dai, W.; Choo, K.K.R.; Zou, D. Ethereum smart contract security research: Survey and future research opportunities. *Front. Comput. Sci.* **2021**, *15*, 1–18. [CrossRef]
61. 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.* **2020**, *149*, 102471. [CrossRef]
62. Hassan, M.; Rehmani, M.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
63. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
64. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **2019**, *3*, 1–17. [CrossRef]
65. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
66. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A survey on the scalability of blockchain systems. *IEEE Netw.* **2019**, *33*, 166–173.
67. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2020**. [CrossRef]
68. Cui, Y.; Pan, B.; Sun, Y. A survey of privacy-preserving techniques for blockchain. In Proceedings of the International Conference on Artificial Intelligence and Security, New York, NY, USA, 26–28 July 2019; pp. 225–234.
69. Wilson, D.; Ateniese, G. From pretty good to great: Enhancing PGP using bitcoin and the blockchain. In Proceedings of the International Conference on Network and System Security, New York, NY, USA, 3–5 November 2015; Volume 11, pp. 368–375.
70. Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access* **2018**, *6*, 17545–17556. [CrossRef]
71. Liang, G.; Weller, S.; Luo, F.; Zhao, J.; Dong, Z. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Trans. Smart Grid* **2018**, *10*, 3162–3173. [CrossRef]
72. Aitzhan, N.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
73. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]
74. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 2016 13th international conference on service systems and service management(ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6.
75. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial Internet of things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3690–3700. [CrossRef]
76. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
77. US Federal Advisory Report about Blockchain Technology to Committee on Insurance. Available online: https://casetext.com/analysis/federal-advisory-committee-on-insurance-discusses-blockchains-impact-on-the-insurance-industry (accessed on 10 May 2021).
78. Bahack, L. Theoretical bitcoin attacks with less than half of the computational power. *arXiv* **2013**, arXiv:1312.7013.
79. Afzal, M.; Huang, Q.; Amin, W.; Umer, K.; Raza, A.; Naeem, M. Blockchain enabled distributed demand side management in community energy system with smart homes. *IEEE Access* **2020**, *8*, 37428–37439. [CrossRef]
80. Minoli, D. Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. *Internet Things* **2020**, *10*, 100147. [CrossRef]
81. 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]
82. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics* **2019**, *8*, 505. [CrossRef]
83. Kumar, R.; Tripathi, R. Traceability of counterfeit medicine supply chain through Blockchain. In Proceedings of the 2019 11th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 7–11 January 2019; pp. 568–570.
84. Pandey, P.; Litoriya, R. Securing and authenticating healthcare records through blockchain technology. *Cryptologia* **2020**, *44*, 341–356. [CrossRef]

85. Kalaipriya, R.; Devadharshini, S.; Rajmohan, R.; Pavithra, M.; Ananthkumar, T. Certain Investigations on Leveraging Blockchain Technology for Developing Electronic Health Records. In Proceedings of the 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020; pp. 1–5.
86. Sharma, A.; Tomar, R.; Chilamkurti, N.; Kim, B.G. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics* **2020**, *9*, 1609. [CrossRef]
87. Kormiltsyn, A.; Udokwu, C.; Karu, K.; Thangalimodzi, K.; Norta, A. Improving healthcare processes with smart contracts. In Proceedings of the International Conference on Business Information Systems, Seville, Spain, 26–28 June 2019; pp. 500–513.
88. Kar, A.K.; Navin, L. Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telemat. Inform.* **2020**, *58*, 101532. [CrossRef]
89. Das, M.; Luo, H.; Cheng, J.C. Securing interim payments in construction projects through a blockchain-based framework. *Autom. Constr.* **2020**, *118*, 103284. [CrossRef]
90. Lu, Q.; Binh Tran, A.; Weber, I.; O'Connor, H.; Rimba, P.; Xu, X.; Staples, M.; Zhu, L.; Jeffery, R. Integrated model-driven engineering of blockchain applications for business processes and asset management. *Softw. Pract. Exp.* **2021**, *51*, 1059–1079. [CrossRef]
91. Ullah, F.; Al-Turjman, F. A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. *Neural Comput. Appl.* **2021**, 1–22. [CrossRef]
92. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-based agri-food supply chain: A complete solution. *IEEE Access* **2020**, *8*, 69230–69243. [CrossRef]
93. Xiong, H.; Dalhaus, T.; Wang, P.; Huang, J. Blockchain technology for agriculture: Applications and rationale. *Front. Blockchain* **2020**, *3*, 7. [CrossRef]
94. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. *IEEE Internet Things J.* **2021**. [CrossRef]
95. 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]
96. Wu, B.; Duan, T. The advantages of blockchain technology in commercial bank operation and management. In Proceedings of the 2019 4th International Conference on Machine Learning Technologies, Association for Computing Machinery New York, NY, USA, 21 June 2019; pp. 83–87.
97. Wang, R.; Lin, Z.; Luo, H. Blockchain, bank credit and SME financing. *Qual. Quant.* **2019**, *53*, 1127–1140. [CrossRef]
98. Wang, X.; Xu, X.; Feagan, L.; Huang, S.; Jiao, L.; Zhao, W. Inter-bank payment system on enterprise blockchain platform. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 614–621.
99. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]
100. Abdellatif, A.A.; Al-Marridi, A.Z.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Refaey, A. ssHealth: Toward secure, blockchain-enabled healthcare systems. *IEEE Netw.* **2020**, *34*, 312–319. [CrossRef]
101. Du, M.; Chen, Q.; Chen, J.; Ma, X. An optimized consortium blockchain for medical information sharing. *IEEE Trans. Eng. Manag.* **2020** [CrossRef]
102. Ali, M.S.; Vecchio, M.; Putra, G.D.; Kanhere, S.S.; Antonelli, F. A decentralized peer-to-peer remote health monitoring system. *Sensors* **2020**, *20*, 1656. [CrossRef] [PubMed]
103. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A blockchain-based supply chain quality management framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; pp. 172–176.
104. Hardwick, F.S.; Gioulis, A.; Akram, R.N.; Markantonakis, K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1561–1567.
105. Chaieb, M.; Yousfi, S.; Lafourcade, P.; Robbana, R. Verify-your-vote: A verifiable blockchain-based online voting protocol. In Proceedings of the European, Mediterranean, and Middle Eastern Conference on Information Systems, Limassol, Cyprus, 4–5 October 2018; pp. 16–30.
106. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. *IACR Cryptol. EPrint Arch.* **2017**, *2017*, 1043.
107. Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale election based on blockchain. *Procedia Comput. Sci.* **2018**, *129*, 234–237. [CrossRef]
108. Chen, Z.; Zhu, Y. Personal archive service system using blockchain technology: Case study, promising and challenging. In Proceedings of the 2017 IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, HI, USA, 25–30 June 2017; pp. 93–99.
109. Yan, Z.; Gan, G.; Riad, K. BC-PDS: Protecting privacy and self-sovereignty through BlockChains for OpenPDS. In Proceedings of the 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 6–9 April 2017; pp. 138–144.
110. Rathee, G.; Sharma, A.; Iqbal, R.; Aloqaily, M.; Jaglan, N.; Kumar, R. A blockchain framework for securing connected and autonomous vehicles. *Sensors* **2019**, *19*, 3165. [CrossRef]

111. Benet, J. Ipfs-content addressed, versioned, p2p file system. *arXiv* **2014**, arXiv:1407.3561.
112. Zichichi, M.; Ferretti, S.; D'Angelo, G. A distributed ledger based infrastructure for smart transportation system and social good. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6.
113. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Adjunct, Heidelberg, Germany, 12–16 September 2016; pp. 137–140.
114. Leiding, B.; Vorobev, W. Enabling the vehicle economy using a blockchain-based value transaction layer protocol for vehicular ad-hoc networks. *Proc. Medit. Conf. Inf. Syst. MCIS* **2018**, *5*, 1–31.
115. Zhao, Z.; Wang, J. Verifiable outsourced ciphertext-policy attribute-based encryption for mobile cloud computing. *TIIS* **2017**, *11*, 3254–3272.
116. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* **2018**, *7*, 39. [CrossRef]
117. Rahulamathavan, Y.; Phan, R.W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6.
118. Rehmani, M.; Reisslein, M.; Rachedi, A.; Erol-Kantarci, M.; Radenkovic, M. Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2814–2825. [CrossRef]
119. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [CrossRef]
120. Sharma, P.; Chen, M.Y.; Park, J. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access* **2018**, *6*, 115–124. [CrossRef]
121. Herbaut, N.; Negru, N. A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains. *IEEE Commun. Mag.* **2017**, *55*, 70–76. [CrossRef]
122. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
123. Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. Consortium blockchain-based malware detection in mobile devices. *IEEE Access* **2018**, *6*, 12118–12128. [CrossRef]
124. Wang, F.; Hu, L.; Hu, J.; Zhou, J.; Zhao, K. Recent advances in the Internet of things: Multiple perspectives. *IETE Tech. Rev.* **2017**, *34*, 122–132. [CrossRef]
125. Knirsch, F.; Unterweger, A.; Engel, D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Comput. Sci. Res. Dev.* **2018**, *33*, 71–79. [CrossRef]
126. Fujisaki, E. Sub-linear size traceable ring signatures without random oracles. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 14–18 February 2011; pp. 393–415.
127. Saberhagen, N.v. CryptoNote v 2.0. 2013. Available online: https://bytecoin.org/old/whitepaper.pdf (accessed on 18 May 2021).
128. Noether, S.; Mackenzie, A. Ring confidential transactions. *Ledger* **2016**, *1*, 1–18. [CrossRef]
129. Sun, S.; Au, M.; Liu, J.; Yuen, T. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In Proceedings of the European Symposium on Research in Computer Security, Oslo, Norway, 11–15 September 2017; pp. 456–474.
130. Maxwell, G. CoinSwap: Transaction Graph Disjoint Trustless Trading. Transaction Graph Disjoint Trustless Trading: CoinSwap. 2013. Available online: https://bitcointalk.org/index.php?topic=321228.0 (accessed on 10 May 2021).
131. Liu, J.; Wei, V.; Wong, D. Linkable spontaneous anonymous group signature for ad hoc groups. In Proceedings of the Australasian Conference on Information Security and Privacy, Sydney, Australia, 13–15 July 2004; pp. 325–335.
132. Li, F.; Zheng, Z.; Jin, C. Secure and efficient data transmission in the Internet of Things. *Telecommun. Syst.* **2016**, *62*, 111–122. [CrossRef]
133. Blum, M.; Feldman, P.; Micali, S. Non-interactive zero-knowledge and its applications. In Proceedings of the Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, New York, NY, USA, 4 October 2019; pp. 329–349.
134. Miers, I.; Garman, C.; Green, M.; Rubin, A. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 397–411.
135. Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 459–474.
136. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP. IEEE), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
137. Chaum, D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* **1981**, *24*, 84–90. [CrossRef]

138. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, 23 October 2013; pp. 127–140.
139. Bonneau, J.; Narayanan, A.; Miller, A.; Clark, J.; Kroll, J.; Felten, E. Mixcoin: Anonymity for bitcoin with accountable mixes. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; pp. 486–504.
140. Valenta, L.; Rowan, B. Blindcoin: Blinded, accountable mixes for bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; pp. 112–126.
141. Heilman, E.; Baldimtsi, F.; Goldberg, S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 43–60.
142. Duffield, E.; Diaz, D. Dash: A Payments-Focused Cryptocurrency. Whitepaper. 2018. Available online: https://github.com/dashpay/docs/raw/master/binary/Dash%20Whitepaper%20-%20V2.pdf (accessed on 7 July 2021).
143. Heilman, E.; Alshenibr, L.; Baldimtsi, F.; Scafuro, A.; Goldberg, S. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. *Netw. Distrib. Syst. Security Symp.* **2017**. [CrossRef]
144. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. Coinshuffle: Practical decentralized coin mixing for bitcoin. *European Symposium on Research in Computer Security*; Springer: Cham, Switzerland, 2014; pp. 345–364.
145. Advances in Cryptology—ASIACRYPT 2001. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 December 2001.
146. Bugliesi, M.; Preneel, B.; Sassone, V. Automata, Languages and Programming. In Proceedings of the 33rd International Colloquium (ICALP 2006), Venice, Italy, 10–14 July 2006.
147. Dagher, G.; Mohler, J.; Milojkovic, M.; Marella, P. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
148. Liu, J.; Zhang, C.; Fang, Y. Epic: A differential privacy framework to defend smart homes against Internet traffic analysis. *IEEE Internet Things J.* **2018**, *5*, 1206–1217. [CrossRef]
149. Hassan, M.; Rehmani, M.; Chen, J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 746–789. [CrossRef]
150. Feghhi, S.; Leith, D. A web traffic analysis attack using only timing information. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1747–1759. [CrossRef]