electronics

MDPI

Review

Approaches towards Blockchain Innovation: A Survey and Future Directions

Divya Guru [1], Supraja Perumal [1] and Vijayakumar Varadarajan [2,*]

[1] Department of Information Technology, SRM Institute of Science and Technology, Kattakulathur 603203, India; divyag2@srmist.edu.in (D.G.); suprajap@srmist.edu.in (S.P.)
[2] School of Computer Science and Engineering, The University of New South Wales, Sydney, NSW 2052, Australia
* Correspondence: v.varadarajan@unsw.edu.au

Abstract: A blockchain is a decentralized peer to peer platform which provides security services based on some key concepts, namely authentication, confidentiality, integrity and authorization. It is the process of recording and keeping track of the resources without the intervention of a centralized authority. This paper provides an overview of blockchains, the structure of blockchains, consensus algorithms, etc., It compares the algorithms based on their utility and limitations. Though blockchains provide secure communication, there are some minimal data leaks which are discussed. Various security issues in blockchains are discussed such as denial of service attacks, etc., In addition to security, some other blockchain challenges are presented like scalability, reliability, interoperability, privacy and consensus mechanisms for integration with AI, IoT and edge computing. This paper also explains about the importance of blockchains in the fields of smart healthcare, smart grid, and smart financial systems. Overall, this paper gives the glimpse of various protocols, algorithms, applications, challenges and opportunities that are found in the blockchain domain.

Keywords: blockchain; consensus algorithm; smart contract; attacks; smart cities; security and privacy

Citation: Guru, D.; Perumal, S.; Varadarajan, V. Approaches towards Blockchain Innovation: A Survey and Future Directions. *Electronics* **2021**, *10*, 1219. https://doi.org/10.3390/electronics10101219

Academic Editor: Guillermo L. Taboada

Received: 10 March 2021
Accepted: 7 May 2021
Published: 20 May 2021

1. Introduction

A blockchain is a distributed data structure which is replicated on various nodes or various computer systems that are not linked based on memory addresses, giving a different notion of linking between nodes and each of these nodes is called a block. We can imagine a blockchain as a series of blocks where each block in the blockchain is connected to its previous block and so it is replicated all over the blocks. The fundamental benefit of this replication is that, on the off chance that one of the imitation blocks becomes corrupted, different reproductions are available to ensure that the honesty of the information contained in the data structure is maintained and furthermore replication gives one some sort of assurance of the trustworthiness of the data, conveyed as a guarantee that the distinctive PCs engaged in the blockchain platform are really running appropriate calculations to ensure the data consistency and fiability. The consistency of the data is maintained by a process called consensus. Consensus is that everybody agrees that the data that goes into the data called structure is what they agree to put there. For linking, we cannot use memory addresses, so we rely on the cryptographic technique called hashing. Blockchains use hash linking and the integrity of the data is thus maintained because of the use of cryptographic techniques and consensus and replication. Therefore, a blockchain is an information structure that is distributed, duplicated and maintains the integrity of data, i.e., the information cannot be altered. Another view is that blockchain is an immutable ledger of events/transactions, a log that cannot be changed by a malicious party or by mistake. Any tampering with the data is made virtually impossible.

Figure 1 shows a step by step view of a blockchain. At first, a user requests a transaction. Once a request is made, a block representing the transaction is created, this block

contain a timestamp, hash value, block version and data. Then, this block is communicated to every one of the other nodes of the network. Each and every node in the network validates the block and the transaction. Once the validation is done, the block is added to the chain. The main motivation is to distribute the computational task to all nodes, i.e., to create a decentralized network which provides more security.

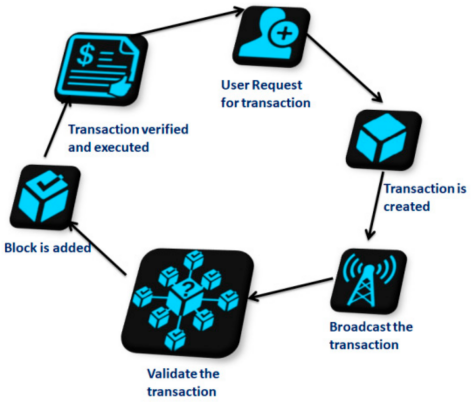

Figure 1. Blockchain technology.

2. Background Study

A blockchain is a decentralized computation and data sharing stage that empowers numerous definitive spaces, who don't confide in one another to collaborate, cooperate and coordinate in a normal dynamic cycle. Figure 2 describes the structure of a block. Each block is linked via a reference hash. The first block in a blockchain network is known as the genesis block. Each block in a blockchain contains a 4 byte Nonce which starts from 0 and augments in each hash task, the size of the hash value, current timestamp, and block version, of the previous hash value which is 256 bits and a Merkle root tree which contains all the hashes of the transaction. Each transaction in a block is checked and approved by so-called miners. To validate the transaction, miners employ an asymmetric cryptography algorithm such as a digital signature [1].

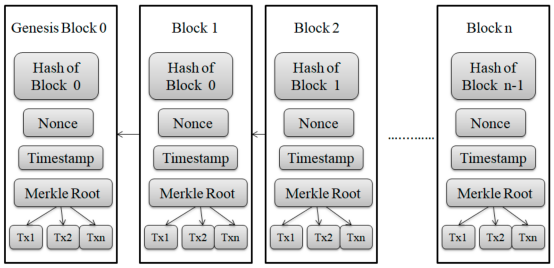

Figure 2. Structure of a block.

Blockchains are classified into three kinds based on their authentication and control mechanism: public blockchains, private blockchains and consortium blockchains, which are depicted in Figure 3.

A public blockchain is a decentralized and open source platform where each individual can join and perform mining autonomous of its organisation where the participants are resilient and anonymous [2]. Here the transaction approval frequency is too long. Energy consumption and scalability are high. This public blockchain is powerless against Sybil attacks since the members are obscure prior to mining. Proof-of-work (PoW), Proof of stack (PoS) and delegated proof of stack (DPoS) are few consensus algorithm used in public blockchains. Proof-of-work (PoW) consensus is one of the efficient mechanisms which can overcome this issue of Sybil attacks, but it is still vulnerable to applications which deal with voluminous data.

A private blockchain is a restricted controlled platform and only an authorised user can join and perform mining dependent on their organisation where the participants are trusted [3,4]. Here the transaction approval frequency is moderate, energy consumption is low and transparency and scalability are high. Practical Byzantine fault tolerance (PBFT) and Raft are some of the few consensus algorithms used in private blockchains. PBFT consensus is the most efficient mechanism which provides transparency in private blockchains. Private blockchains are suitable for banks and other monetary-related associations [5].

A consortium blockchain [6] is a blend of both public and private blockchains. Here the transaction approval frequency is short. Mining is done by a multi-signature scheme and validation is done only if it is signed by an authorized node. Though it provides high transparency and efficiency, it suffers from tampering attacks [7].

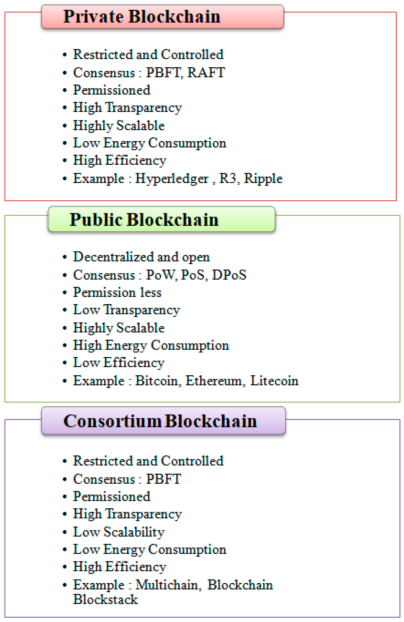

Figure 3. Types of blockchain.

3. Blockchain Architecture

A blockchain is a peer-peer distributed ledger [8] which is a type of data structure that records the transaction of asserts and the details are recorded in multiple places at the same time. Figure 4 explains the detailed architecture of a blockchain [6,9]. Figure 5, explains its layers.

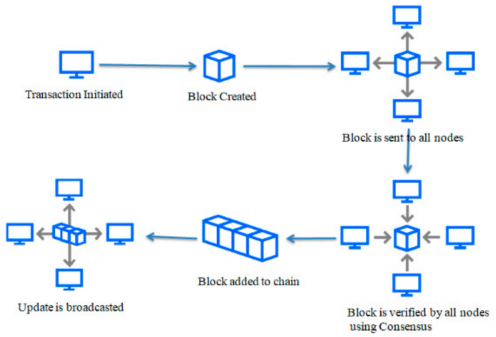

Figure 4. Blockchain architecture.

3.1. Data Layer

The information model captures the present status of the ledger, a time-stamped sequence of cryptographically encoded transactions. As a blockchain consists of a list of blocks, each block stores information which could be personal information, government information, a list of transactions that depends on the application. To secure this information hashing is done. Hashing uses different algorithms (such as MD5, SHA-256, SHA-512) to generate a simple hash key for the block data. The hash key is 256 bits though the input size is different. The reason for utilizing hashing is that in the event that anybody attempts to change the content of information, it will influence the hash value [10].

The primary motivation behind the information model is to epitomize the time stamped information block. In each block, confirmed transactions are stored which contain timestamps (time when the block was made) which empower situating and the recognizability of information. Metadata, Nonces, and Merkle roots are utilized to check the trustworthiness of information and the hashes of past blocks.

3.2. Network Layer

In a blockchain network communication is done between participants [11]. The primary obligation of the network layer is to confirm and advance the transaction along the network. When the transaction is done, this data is communicated to the adjoining nodes that confirm the transaction depending on a predefined determination. Once the verification is done the verified transaction is forwarded to other node or otherwise it will be discarded. In order to verify the transaction a digital signature mechanism is used [12]. Signing and verification are done using digital signatures. During the signing phase, a signature is generated after block creation using a private key. In the verification phase, the signature is verified using a public key. This layer provides a data verification and communication mechanism [7,13].

3.3. Consensus Layer

Since a blockchain a decentralized network, it doesn't contain any trusted third party to authenticate a node. To overcome this a consensus mechanism is used for decentralized nodes. Table 1 below lists a few consensus protocols for blockchains [14].

Table 1. Comparison of consensus protocols.

Consensus Protocol	Description	Language Used	Advantage	Disadvantage
Proof-of-Work (POW) [15,16]	Miners contend with one another to address a numerical puzzle to add a block in the chain and a get reward	Solidity C++ Golang	Double spending is avoided Everyone mines	More computational power 51% attack Longer processing time
Proof-of-Stake (POS) [15,17]	Miners are replaced with validators Validators are chosen based on a combination of random selection and wealth (stake value) If a validator acts maliciously then its stake gets slashed	Native	More secure Energy efficient	"The nothing at stake" problem Only a few selected "validators"
Delegated Proof-of-Stake (DPoS) [18,19]	An election system is maintained to choose the node which verifies the block	Native	Protects from double spending attacks Energy efficient	"The nothing at stake" problem Partially centralized
Proof-of-Burn (PoB) [14]	Coin burning strategy	C++ Golang Solidity Serpent	Minimal energy consumption Less energy consumption.	Requires lot of resources Need more testing
Proof-of-Authority (PoA) [16]	Combination of PoW and PoS	Native	High performance and fault tolerance Avoids 51% attack	Not fully decentralized Scalability issue

Table 1. *Cont.*

Consensus Protocol	Description	Language Used	Advantage	Disadvantage
Proof-of-Elapsed Time (PoET) [14]	Follows a lottery system A random waiting time is generated and the node with the shortest waiting time will win the block	Python	Less power consumption Cost efficient Enhanced transparency	Hardware security Same node may be elected as leader
Proof-of-Capacity (PoC) [14]	Hard disk space is used to choose the miners Here you will pay for hard drive space	-	Energy efficient No need to upgrade hard drives	High energy consumption Node with more disk space chosen as miner
Practical Byzantine Fault Tolerance (PBFT) [14,19]	Consensus is obtained even if the network contain malicious nodes Here malicious node should not exceed one-third of the total number of nodes	Golang Java	Does not compute mathematical calculations Does not require multiple confirmations	Communication overhead
RAFT [5]	Voting based method Elect leader in randomized way and perform verification process to achieve consistency	Scala Java Go C++	Easy to implement Process speed is high	Low security Tolerant in handling network partition

3.4. Incentive Layer

When a miner does the verification process and adds a block into a chain, that miner will get a reward for performing the verification task. Based on their contributions towards the validation process, miners will get incentives (such as digital currency) as rewards. This process motivates each node to contribute their power to validate the transaction [9].

3.5. Contract Layer

Here any type of programming code built into the blockchain is represented as a smart contract. Each node executes this code to update the ledger. A smart contract is a self-upholding understanding embedded in the programming code in the blockchain. Using this self-verification, self-execution and tamper resistance are achieved. Fewer intermediaries are achieved using smart contracts. Smart contracts can be written in any language depending on the need that fits a project. A smart contract development framework is used to deploy and test smart contracts. Table 2 below shows a list of frameworks used to build smart contracts [20].

Table 2. Comparison of smart contract frameworks.

Framework	Description	Language	Testing	Blockchain
Hardhat	Open source	JavaScript	Waffle	Hardhat runtime environment/local, testnets, mainnet
Truffle	Open source with paid upgrades	JavaScript	Has testing	Ganache/local, testnets, mainnet
Brownie	Open source	Python	Has testing	Ganache/local, testnets, mainnet
Embark	Open source	JavaScript	Has testing	Ganache/local, testnets, mainnet

3.6. Application Layer

The application layer consists of the user interface, scripts, and APIs that act as an intermediate step between an end client and the blockchain network. The end user initiates the transaction. There are various applications such as smart cities, IoT [4], financial applications, business applications and market security. Application layers use a software development kit/command line tool to communicate with the blockchain network.

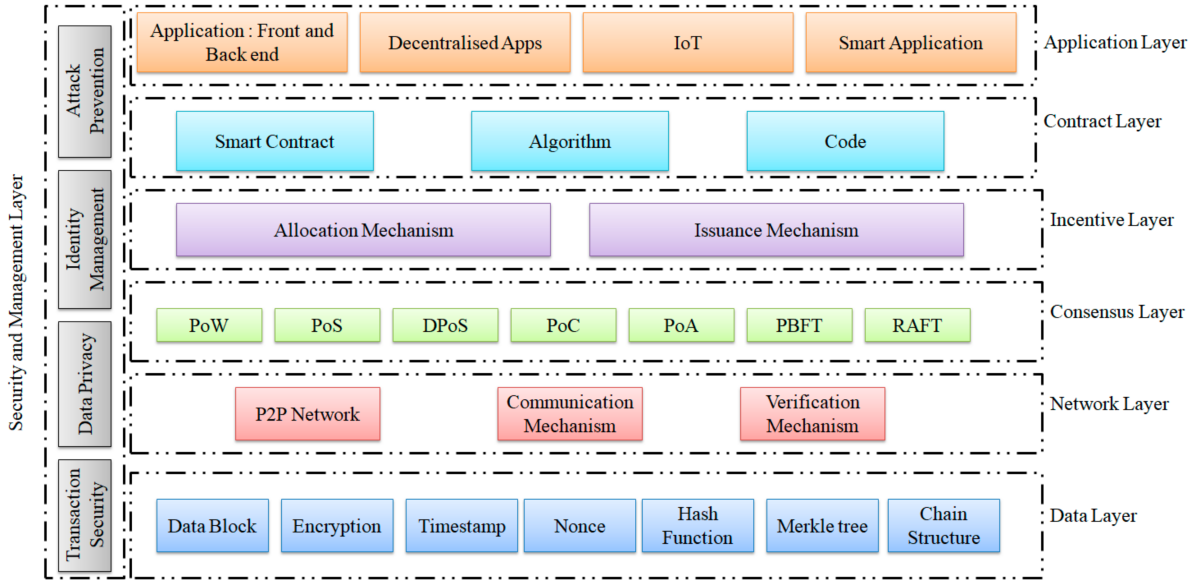

Figure 5. Blockchain layers.

4. Blockchain Applications

Nowadays, smart cities have become quite popular in many countries that are planning to implement this smart technology. For the implementation and deployment of this technology though we need high financial investment and skilled human resources, and smart cities face several technological challenges in security and privacy [21]. To implement and deploy this technology we need blockchain technology which possesses some features that provide effective solutions for the major challenges in smart cities. This blockchain technology is a decentralized network which eliminates single point of failure, offers immutability by using cryptography, and uses consensus algorithms for decision making process which leads to their democracy, while providing privacy for user identity by using pseudonymous addresses and also providing security and transparency. Because of these features this blockchain technology is used in several democratic cities [22]. In this section, existing blockchain works are explained from various points of view.

4.1. Smart HealthCare

Smart healthcare is the technology that uses IoT devices to monitor patients and provide services [23,24]. These devices gather patient data such as heartbeat rate, glucose level, pulse, blood pressure, etc., and administrators monitor and gather this data and produce reports, were each report is investigated by a specialist who can suggest a treatment [25,26]. This report is shared on the network in an encrypted format and stored it in a cloud platform, and when the patient requests the cloud service provider to access this report then the encrypted file is transferred to the patient. By using this setup hospital expenses are reduced and they provide timely treatment for various health conditions [27,28]. To secure this patient records blockchain technology is used so as to guarantee their transparency, privacy and security [21].

Mettler et al. proposed a blockchain technology against falsifying the medication in public medical care boards based on Ethereum which results in tamperproof information audits and secure information access, yet at the same time it isn't appropriate for an enormous number of clients. To address this versatility issue in health services Zhang et al. have proposed a DApp which ensures transparency and security but doesn't ensure information accessibility and distance access. Yue et al. proposed a medical care information entryway which gives regulatory and legal provisions in health care systems but doesn't thinking about the incentive mechanism. Zhang et al. proposed a blockchain innovation for information sharing and to build up secure connections to access healthcare

data, yet this framework doesn't ensure tamperproof information. Wang et al. used a consortium blockchain for data access but it has vulnerability in data integrity and scalability. Ismail et al. proposed a PBFT algorithm for a healthcare network, this avoiding the forking problem but real implementation is not yet been done. Jiang [29] proposed BlocHIE, a blockchain-based healthcare information exchange system using two approximately coupled blockchains to deal with various medical care information situations while providing privacy and authentication services. To improve the system throughput two fairness-based packing algorithms are proposed.

4.2. Smart Transportation

Smart transportation uses IoT devices which gather data like toll systems, traffic management, vehicle tracking, vehicle to vehicle communication, etc. Applying blockchain technology to a transport system provides efficient data processing, privacy, network monitoring and secure service delivery to end users. Li et al. [30] proposed this blockchain technology for transportation systems to provide security and privacy. Knirsch et al. proposed blockchain-based four phase protocols for charging EVs utilizing bitcoin technology for data identified with charging station offers; although it provides transparency it is not reasonable for huge arrangements of information. Zhang et al. [31] proposed a consortium blockchain-based plan utilizing a PoW algorithm to improve electricity trading in vehicles for enhancement, but the adaptability was not completely clarified. Sadiq et al. [32] composed a smart contract by PoA to get the exchange between charging stations and EVs which guarantees security. Kang et al. proposed two phase protection by applying both PoW and PoS algorithms to secure voting collusion between users in the Internet of Vehicles. Maaroufi et al. [33] proposed a consortium-based secure energy exchange system to improve security and execution. Lei et al. consolidated a PoW and a PoB algorithm for secure key management system where the key transfer time is diminished. Li et al. [30] proposed a blockchain-based impetus vehicular system which ensures unwavering quality of vehicular declaration however then the issue of versatility arises. Luo et al. proposed a confided in-based blockchain-empowered area security safeguarding plan. Though it gives protection it doesn't ensure adaptability of the proposed framework.

4.3. Smart Grids

Most of the countries like the UK, use the electrical grid for energy distribution between networks [34]. It interconnects the generating stations to end users using a transmission and distribution system. Here a centralized power generating station is used to feed power into the grid so as to supply energy to customers. Forecasting the load depends on time slots. The load will be different based on the time slot. To monitor the load demand a separate team is used. When there is a sudden change in load it may lead to changes in frequency and voltage which result in problems like brownouts. When the load demands an increase in one area, they need to cut-off the essential loads and provide supply to that particular area, due to this load shedding a problem may arise

To overcome such issues, smart grids have been introduced which are advanced electricity generation and delivery systems. These systems are properly managed, monitored and metered. Here lots of data is exchanged between customers and the electrical end. This system is a bidirectional data communication system, which balances the supply and demand and provides stability and safe system. This system uses sensors, smart meters, artificial intelligence and wireless communication to provide a stable system which is an effective use of renewable energy. Since the data is exchanged between nodes, security and privacy need to be considered.

Blockchains take the smart grid concept to next level to provide security and privacy. Here the measure of energy abundance is shared or offered to the electrical grid. By doing so the power lattice pays a certain measure of cash for individuals who contribute energy. Blockchain innovation is utilized to get this exchange log. By utilizing certain agreement calculations it shields the information from weaknesses [35].

Guo et al. [36] proposed a PoW consensus mechanism with stacks to high latency in traditional methods under a blockchain-based electricity trading ecosystem. Samy et al. [37] proposed a protected blockchain model utilizing a PoW algorithm to secure the information created by smart meters. This framework ensures information uprightness and classification however it doesn't ensure information flexibility. Muhammad et al. [38] proposed 6G-enabled smart grids to prevent cyberattacks. Niloy et al. [39] utilized a microgrid framework for customers to transfer energy to the grid in an appropriate adjustment of energy utilization through the use of renewable energy. Tao et al. [40] proposed a multi-microgrid strategy to optimize the load, improving economic and environmental protection, speed and accuracy. This framework also guarantees security. Ayaz et al. [41] proposed a proof of quality factor-based blockchain model for vehicular message scattering which reduces validation process failures.

4.4. Financial Systems

Blockchain technology is used in financial systems to secure transactions between two people in a decentralized manner. In a decentralized system we need to preserve the privacy of the customer and we should also maintain security for the transaction data.

Utilizing blockchain innovation, an agreement is first sent by the payer to the bank, and afterward this agreement is forwarded to the arranging bank. This arranging bank in turn sends an encouraging letter to the payee requesting affirmation. Presently the payee sends the archive to the arranging bank which is sent to the bank. This archive is delivered to the payer who can utilize it to start a smart agreement with the payee. In this way a protected exchange is done between two individuals utilizing a blockchain.

Chen et al. proposed a BPCSS for secure exchange between stock stores and clients utilizing bitcoin innovation. This framework empowers straightforwardness and dependability of the framework yet doesn't recognize deceitfulness assaults. McCallig et al. incorporated conveyed capacity with network examination and multiparty calculation to guarantee straightforwardness and to decrease the office cost of monetary announcing frameworks. Kabra et al. incorporated staggered confirmation, a QR age strategy and two factor verification conventions by utilizing PoA calculation for consistent progression of activity without including any delegates. Gao et al. organized a back proliferation neural organization, with PSO and SVR calculation to update fitting effects on yield rate assumptions.

5. Security Attacks in Blockchain

Security and privacy play a major role in blockchain technology. For example, if you take smart cities which are an emerging platform to provide high quality facilities to people by optimising the resources, smart cities develop the daily life of citizens in aspects like transport, health, education and energy consumption. Smart technology should have good properties like transparency, decentralization and immutability while using this blockchain technology. Security mechanisms in smart cities should focus on communication, monitoring and response, booting, updating and patching, authentication and access control and application protection. To address these security issues in blockchain technology, the paper explains a few security attacks that can threaten blockchain technology [42]. Blockchain technology faces many security issues based on technology. Here we categorize these issues into five attacks as described in Figure 6.

5.1. Blockchain Network Attacks

Blockchain networks are made up of nodes which create a transaction and provide necessary services. For example, if you take a smart grid, each home network will have a smart meter which stores the history of transactions it made; it can also add a new transaction into the ledger. For the energy exchange process each node sends and receives a transaction and miners will add and approve the transactions. Here, cybercriminals seekfor network vulnerability. DDoS attacks try to disconnect a network mining pool, bringing down a server. In 2017, Bitfinex suffered from a DDoS attack [43]. Transaction

malleability attacks will try to trick the victim to pay twice for a transaction. The Mt. Gox bitcoin exchange went bankrupt in 2014 at as result of a malleability attack. They solved this problem by introducing a segregated witness process. In timejacking attacks the hacker modifies the organization time counter of a hub and power of the hub to acknowledge the transaction. This will add fake peers to the network. Routing attacks will tamper with the transaction in ways which will be difficult to detect. These attacks may partition the network or tamper with the messages [44]. During Sybil attacks, the victim is surrounded by fake nodes; during verification the hacker takes control of the network mining, which may lead to double spending attacks [45]. Eclipse attacks will take control of IP addresses. Here the attacker will overwrite the address and wait until the node restarts. Long range attacks on PoS networks copy the transactions of authorized nodes.

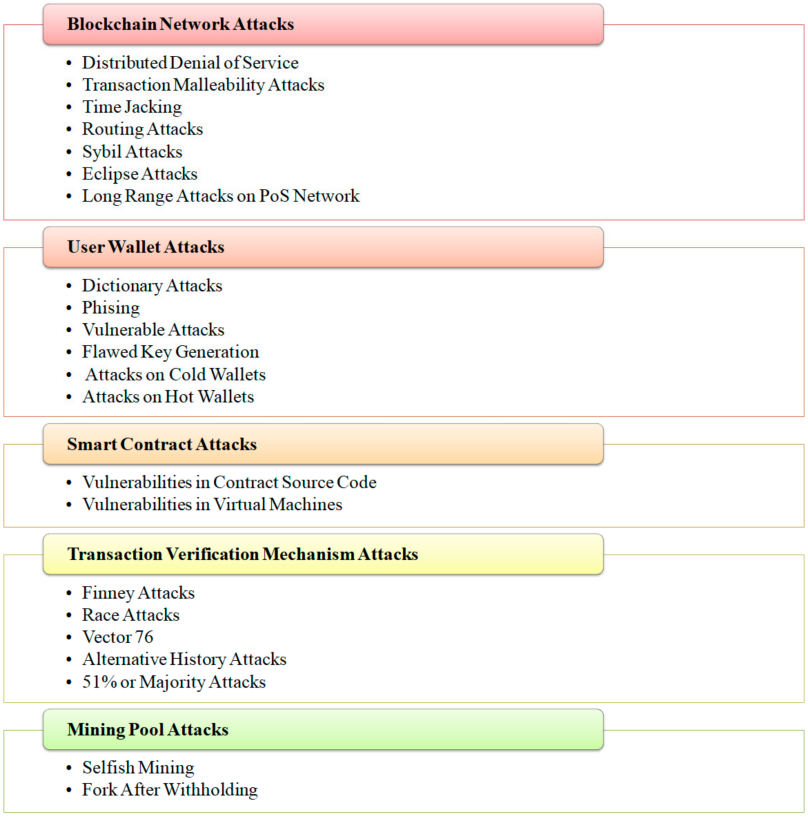

Figure 6. Blockchain attacks.

5.2. User Wallet Attacks

The user wallet is the main target for a hacker [46]. Here the attacker seeks weaknesses in the cryptographic algorithm. In 2018 wallet hacking was done on the IOTA wallet. In a dictionary attack, the hacker tries to find cryptographic hash values such as user credentials, and also vulnerability in the cryptographic signatures. Defective key age is powerless in key age; here the programmer gains admittance to private keys. Attacks on cold wallets lead to access to the private key as well as PINs. Attacks on hot wallets are also possible where all the keys are stored in internet-connected apps.

5.3. Smart Contract Attacks

Smart contract attacks are related to bugs in the source code, runtime environment, and virtual machines [46]. If there is a vulnerability in the source code, such as bugs in an Ethereum contract cost, there is the possibility of delegating control to an untrusted function. Vulnerability can also occur in EVM when a smart contract is executed. Here bugs in access control, immutable defects, and short address attack will occur [46].

5.4. Transaction Verification Mechanism Attacks

Double spending [47] is the common transaction attack which occurs during the verification process. It is an act of spending the same digital currency twice by creating a fake transaction. The majority of these attacks occur in a situation where a miner owns over half of all the organization's hash power, which in turn may act maliciously and lead to vulnerability of the network [46,48]. This attack can double-spend your money or prevent the transaction from being confirmed, but it cannot create a new account, cannot steal funds, reverse transactions or create false transactions.

5.5. Mining Pool Attacks

In blockchain technology it is impossible to earn profits, so the miners use their computational power by creating mining pools. If the miners create more blocks they will receive more rewards [46]. For example, BTC.com, AntPool and ViaBTC are the largest bitcoin mining pools. Vulnerability is also present in mining pools; these are a few attacks that can occur in mining pools like selfish attacks and forks after withholding. [49] In selfish attacks the miners increase their reward but they don't broadcast the mined block, then after some time they broadcast the blocks in network at once and make other miners lose their blocks. This attack can be prevented by adding trusted miners [50].

Table 3 explains the various attacks in blockchain such as its types, impact and solutions.

Table 3. Comparison of various security attacks in blockchains.

Attacks	Types	Description	Impact	Solution
Blockchain Network Attacks [44,45,51]	Distributed Denial of Service	Disconnect mining pool	Theft Malicious mining	fee-based and age-based designs increase block size
	Transaction Malleability Attacks	Tricks a victim to pay twice	Throughput Leads to DoS, DDoS attacks	Segregated Witness (SegWit) process
	Time Jacking	Vulnerability in timestamps	Chain Splitting Revenue Loss Delay Malicious mining	Restricting acceptance time range Use node system time Synchronized clocking
	Routing Attacks	Tampering	Partition attack Delay attack	Peer Monitoring
	Sybil Attacks	Hacker will take control of multiple nodes	Throughput Leads to DoS, DDoS attacks Double spending	Behaviour Monitoring Incentive Mechanism
	Eclipse Attacks	Hack large number of IP addresses	Partitioning	Disabling incoming connections Peer Monitoring Choose specific outgoing connections
	Long Range Attacks on PoS Network	Based on PoS	Attempt to mint more blocks Stake bleeding Posterior corruption	-
User Wallet Attacks [52,53]	Dictionary Attacks	Find weakness in cryptographic algorithm	Find wallet credentials	-
	Phising		Hack logs	-
	Vulnerable Attacks	Vulnerability in cryptographic signature	Theft	-
	Flawed Key Generation	Vulnerability in key generation	Poor randomness of input to generate key Still possible in ECDSA algorithm	-
	Attacks on Cold Wallets	Exploits bugs in the network. Obtain private key as well as PIN	Theft Revenue Loss	Backups
	Attacks on Hot Wallets	Internet-connected apps are used to store keys	Steal fund	Wallet Insurance

Table 3. *Cont.*

Attacks	Types	Description	Impact	Solution
Smart Contract Attacks [54]	Vulnerabilities in Contract Source Code	Bugs in source code	Delay Theft Revenue Loss	-
	Vulnerabilities in Virtual Machines	Vulnerability in EVM with DAO attacks	Immutable defects Bugs in access control Short address attack	-
Transaction Verification Mechanism Attacks [48,55]	Finney Attacks	Create identical transactions	Revenue Loss	Increase Block Reward
	51% or Majority Attacks	Get 51% control of network hash rate	Chain Splitting Revenue Loss Malicious mining Double spend Prevent transaction from being confirmed	Two phased proof of work
Mining Pool Attacks [49,50,56]	Selfish Mining	Peer to peer system	Revenue Loss Malicious mining	Time-stamped blocks
	Fork After Withholding	Malicious miners hide the winning blocks	Malicious mining	Enforce PoW submission

6. Challenges

The major challenge in blockchains is how to maintain security and privacy [42]. One of the main issues when maintaining security and privacy in blockchain networks is that the users in such network could be someone who uses a false name and cannot be identified by name. With the straightforward idea of blockchain technology, this prompts following of user exercises and again admittance to privileged insights. Therefore, in blockchain the main challenge is how to ensure anonymity [57].

Most of the applications in blockchains use cloud services for storage due to the need for large storage capacity and computational resources [58]. Several centralized data storage schemes has been proposed, still there is a vulnerability to DoS attacks and the untrusted nature of cloud service providesr leads to the proposal of a blockchain-based decentralized storage scheme. Chavan et al. proposed a decentralized token system by using proof of retrievability to file storage and earning digital coins for contributions. Ruj et al. proposed a decentralized storage framework to ensure higher transparency and security. Here, free storage space in a wallet is assigned for rent. Though there are many schemes for decentralizing storage systems, they suffer from trust, privacy and security issues.

One of the most serious issues in blockchain technology is how to reduce the energy costs. Several consensus algorithms are used for security purposes, but some consensus algorithms still do not consider the energy efficiency issue. For example if you take a PoW consensus algorithm, it requires more energy to solve mathematical puzzles and its complex computational calculations. Thus this consensus algorithm is not an energy-efficient approach. However if one considers less computationally expensive algorithms like PoS, PBFT and DPoS, though they require less energy they are reasonable for enormous scope frameworks. A new algorithm proof of trust has been proposed to address this issue but still it needs to be investigated [59].

Due to the enormous number of data formats involved in blockchains the implementation of interoperability is a challenging task nowadays [60]. This complexity of implementation is increased further due to the different consensus mechanisms used by blockchain systems. For example PoW algorithms use Ethereum and PBFT algorithms use hyperledger, and these two mechanism cannot be synchronized, thus interoperable blockchain systems need to be developed.

Decentralizing the blockchain platform is also one of the major issues to be considered [61]. For example, if you take cryptocurrencies many countries have banned their use due to regulatory issues. Here in blockchain technology different unstructured data formats are generated, and stringing this type of data into a blockchain is not an effective approach. Regulatory rules to be ensured in blockchains for data integrity [62].

Supply chains in blockchain platforms are also one of the major issues to be considered. Jiang [63] explained critical challenges in supply chains in terms of versatility, throughput, access control, information recovery and surveyed the promising arrangements [64].

Table 4 explains the current issues in blockchain technology and what needs to be investigated in the future.

Table 4. Research directions and their challenges.

Research Direction	Uses	Issue	Challenge
Security and privacy [65,66]	Decentralized network	Users remain pseudonymous than being anonymous	Ensure anonymity
Storage [58,67]	Cloud storage Decentralized storage system Proof of retrievability	Immense storage capacity Lack of trust Lack of privacy and security	Ensure privacy and security
Energy Efficiency [68]	Consensus schemes Proof of Trust	Computationally expensive (PoW) Lacks scalability(PBFT)	Ensure energy efficient consensus scheme
Scalability [69]	Consensus schemes	POW: enhances scalability but suffers from high latency, low throughput and double spending attack PBFT: achieves consensus in the presence of malicious replicas, but suffers from scalability problems	Ensure scalability and performance
Incentive Mechanism [70]	Incentive scheme	Double spending attacks Participation of malicious nodes	Punishment scheme for malicious nodes
Interoperability [71]	Consensus algorithm	Dissimilar consensus mechanism	Design interoperable protocols
Regulation [62,72]	Decentralization	Regularity issue Unstructured data formats No proper storage standards	Ensure regulation rule for data integrity

7. Conclusions

Nowadays decentralized computation and data sharing systems are quite popular for many new technologies. This challenge can be addressed by introducing blockchain technology which has properties like decentralization, immutability, transparency, and auditability. In this paper, blockchain-related consensus algorithms are explained along with their benefits and also the security issues related to these algorithms. The main motivation behind this work is to apply this technology to the realm of smart cities, expllaining the impacts of applying consensus algorithms in smart cities. Based on the survey it focuses on future challenges that need to be investigated. Further, this paper audits the utility of blockchains in smart innovation applications like smart grids, financial systems, transport and healthcare. This paper also explains the various attacks that may occur in blockchain networks. Overall, this paper gives the brief look at the types of blockchain, various protocols (consensus algorithms), applications, difficulties, attacks and recent research challenges in blockchain technology.

Author Contributions: All authors contributed equally to this work and were involved at every stage in its development. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Puthal, D.; Mohanty, S.; Kougianos, E.; Das, G. When Do We Need the Blockchain? *IEEE Consum. Electron. Mag.* **2021**, *10*, 53–56. [CrossRef]
2. Aleksieva, V.; Valchanov, H.; Huliyan, A. Smart Contracts based on Private and Public Blockchains for the Purpose of Insurance Services. In Proceedings of the 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 1–3 October 2020; pp. 1–4. [CrossRef]
3. Baucas, M.J.; Gadsden, S.A.; Spachos, P. IoT-based Smart Home Device Monitor Using Private Blockchain Technology and Localization. *IEEE Netw. Lett.* **2021**. [CrossRef]
4. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2020**. [CrossRef]
5. Kim, D.; Doh, I.; Chae, K. Improved Raft Algorithm exploiting Federated Learning for Private Blockchain performance enhancement. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 828–832. [CrossRef]
6. Guo, X.; Guo, Q.; Liu, M.; Wang, Y.; Ma, Y.; Yang, B. A Certificateless Consortium Blockchain for IoTs. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, 29 November–1 December 2020; pp. 496–506. [CrossRef]
7. Meng, T.; Wolter, K.; Zhao, Y.; Xu, C. On Consortium Blockchain Consistency: A Queueing Network Model Approach. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1369–1382. [CrossRef]
8. Kwak, S.; Lee, J. Implementation of Blockchain based P2P Energy Trading Platform. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 5–7. [CrossRef]
9. Toshniwal, B.; Kataoka, K. Comparative Performance Analysis of Underlying Network Topologies for Blockchain. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 367–372. [CrossRef]
10. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain. *IEEE Internet Things J.* **2021**. [CrossRef]
11. Abdella, J.; Tari, Z.; Anwar, A.; Mahmood, A.; Han, F. An Architecture and Performance Evaluation of Blockchain-based Peer-to-Peer Energy Trading. *IEEE Trans. Smart Grid* **2021**. [CrossRef]
12. Xiao, Y.; Zhang, P.; Liu, Y. Secure and Efficient Multi-Signature Schemes for Fabric: An Enterprise Blockchain Platform. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1782–1794. [CrossRef]
13. Zhang, L.; Ge, Y. Identity Authentication Based on Domestic Commercial Cryptography with Blockchain in the Heterogeneous Alliance Network. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 15–17 January 2021; pp. 191–195. [CrossRef]
14. Ahmad, A.; Saad, M.; Kim, J.; Nyang, D.; Mohaisen, D. Performance Evaluation of Consensus Protocols in Blockchain-based Audit Systems. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 654–656. [CrossRef]
15. Nair, P.R.; Dorai, D.R. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 279–283. [CrossRef]
16. Machacek, T.; Biswal, M.; Misra, S. Proof of X: Experimental Insights on Blockchain Consensus Algorithms in Energy Markets. In Proceedings of the 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 15–19 September 2021; pp. 1–5. [CrossRef]
17. Yang, J.; Paudel, A.; Gooi, H.B. Compensation for Power Loss by a Proof-of-Stake Consortium Blockchain Microgrid. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3253–3262. [CrossRef]
18. Cong, X.; Zi, L. DTNB: A blockchain transaction framework with discrete token negotiation for the delay tolerant network. *IEEE Trans. Netw. Sci. Eng.* **2021**. [CrossRef]
19. Zhang, J. A Hybrid Model for Central Bank Digital Currency Based on Blockchain. *IEEE Access* **2021**. [CrossRef]
20. Qu, Y.; Pokhrel, S.R.; Garg, S.; Gao, L.; Xiang, Y. A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 2964–2973. [CrossRef]
21. Jiang, S.; Cao, J.; McCann, J.A.; Yang, Y.; Liu, Y.; Wang, X.; Deng, Y. Privacy-Preserving and Efficient Multi-Keyword Search over Encrypted Data on Blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410. [CrossRef]
22. Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for Public Services: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 13904–13921. [CrossRef]
23. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access* **2021**, *9*, 37397–37409. [CrossRef]
24. Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. A Novel Blockchain-Based Integrity and Reliable Veterinary Clinic Information Management System Using Predictive Analytics for Provisioning of Quality Health Services. *IEEE Access* **2021**, *9*, 8069–8098. [CrossRef]
25. Egala, B.S.; Pradhan, A.K.; Badarla, V.R.; Mohanty, S.P. Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things with Effective Access Control. *IEEE Internet Things J.* **2021**. [CrossRef]

26. Abdellatif, A. MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange. *IEEE Internet Things J.* **2021**. [CrossRef]
27. De Brito Gonçalves, J.P.; De Resende, H.C.; Municio, E.; Villaça, R.; Marquez-Barja, J.M. Securing E-Health Networks by applying Network Slicing and Blockchain Techniques. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–2. [CrossRef]
28. Aich, S. Protecting Personal Healthcare Record Using Blockchain & Federated Learning Technologies. In Proceedings of the 2021 23rd International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 7–10 February 2021; pp. 109–112. [CrossRef]
29. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 49–56. [CrossRef]
30. Li, C.; Fu, Y.; Yu, F.R.; Luan, T.H.; Zhang, Y. Vehicle Position Correction: A Vehicular Blockchain Networks-Based GPS Error Sharing Framework. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 898–912. [CrossRef]
31. Zhang, C.; Zhu, L.; Xu, C.; Sharif, K. PRVB: Achieving Privacy-Preserving and Reliable Vehicular Crowdsensing via Blockchain Oracle. *IEEE Trans. Veh. Technol.* **2021**, *70*, 831–843. [CrossRef]
32. Sadiq, A.; Javed, M.U.; Khalid, R.; Almogren, A.; Shafiq, M.; Javaid, N. Blockchain Based Data and Energy Trading in Internet of Electric Vehicles. *IEEE Access* **2021**, *9*, 7000–7020. [CrossRef]
33. Maaroufi, S.; Pierre, S. BCOOL: A Novel Blockchain Congestion Control Architecture Using Dynamic Service Function Chaining and Machine Learning for Next Generation Vehicular Networks. *IEEE Access* **2021**. [CrossRef]
34. Yang, Q.; Wang, H. Privacy-Preserving Transactive Energy Management for IoT-aided Smart Homes via Blockchain. *IEEE Internet Things J.* **2021**. [CrossRef]
35. Xu, S.; Guo, C.; Hu, R.Q.; Qian, Y. BlockChain Inspired Secure Computation Offloading in a Vehicular Cloud Network. *IEEE Internet Things J.* **2021**. [CrossRef]
36. J, G.; Ding, X.; Wu, W. A Blockchain-Enabled Ecosystem for Distributed Electricity Trading in Smart City. *IEEE Internet Things J.* **2021**, *8*, 2040–2050. [CrossRef]
37. Samy, S.; Azab, M.; Rizk, M. Towards a Secured Blockchain-based Smart Grid. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 1066–1069. [CrossRef]
38. Tariq, M.; Ali, M.; Naeem, F.; Poor, H.V. Vulnerability Assessment of 6G-Enabled Smart Grid Cyber–Physical Systems. *Internet Things J. IEEE* **2021**, *8*, 5468–5475. [CrossRef]
39. Niloy, F.A.; Nayeem, M.A.; Rahman, M.; Dowla, M. Blockchain-Based Peer-to-Peer Sustainable Energy Trading in Microgrid using Smart Contracts. In Proceedings of the 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 5–7 January 2021; pp. 61–66. [CrossRef]
40. Tao, M.; Wang, Z.; Qu, S. Research on Multi-Microgrids Scheduling Strategy Considering Dynamic Electricity Price Based on Blockchain. *IEEE Access* **2021**. [CrossRef]
41. Ayaz, F.; Sheng, F.; Tian, D.; Guan, Y.L. A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination. *IEEE Internet Things J.* **2021**, *8*, 2468–2482. [CrossRef]
42. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659.
43. Liu, Z.; Yin, X. LSTM-CGAN: Towards Generating Low-Rate DDoS Adversarial Samples for Blockchain-Based Wireless Network Detection Models. *IEEE Access* **2021**, *9*, 22616–22625. [CrossRef]
44. Apostolaki, M.; Zohar, A.; Vanbever, L. Hijacking bitcoin: Routing attacks on cryptocurrencies. In Proceedings of the 38th IEEE Symposium on Security and Privacy (Oakland), San Jose, CA, USA, 22–26 May 2017; pp. 375–392.
45. Douceur, J.R. The sybil attack. In *The First International Workshop on Peer-to-Peer Systems, ser. IPTPS '01*; Springer: London, UK, 2002; pp. 251–260.
46. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A. Exploring the Attack Surface of Blockchain: A Systematic Overview. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 3. [CrossRef]
47. Nicolas, K.; Wang, Y.; Giakos, G.C.; Wei, B.; Shen, H. Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach. *IEEE Access* **2021**, *9*, 3838–3857. [CrossRef]
48. Bastiaan, M. Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin. 2015. Available online: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin.pdf (accessed on 19 March 2021).
49. Wang, S.; Cheng, Y.; Yin, B.; Cao, X.; Zhang, S.; Cai, L.X. A Selfish Attack on Chainweb Blockchain. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
50. Leelavimolsilp, T.; Tran-Thanh, L.; Stein, S. On the preliminary investigation of selfish mining strategy with multiple selfish miners. *arXiv* **2018**, arXiv:1802.02218.
51. Marcus, Y.; Heilman, E.; Goldberg, S. Low-resource eclipse attacks on ethereum's peer-to-peer network. *IACR Cryptol. ePrint Arch.* **2018**, *2018*, 236.
52. Fleder, M.; Kester, M.S.; Pillai, S. Bitcoin transaction graph analysis. *arXiv* **2015**, arXiv:1502.01657.

53. Vyas, C.A.; Lunagaria, M. Security concerns and issues for bitcoin. In Proceedings of the National Conference cum Workshop on Bioinformatics and Computational Biology NCWBCB, Majitar, India, 10–12 May 2014.
54. Ghiasi, M.; Dehghani, M.; Niknam, T.; Kavousi-Fard, A.; Siano, P.; Alhelou, H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access* **2021**, *9*, 29429–29440. [CrossRef]
55. Finney, H. The Finney Attack (the bitcoin Talk Forum). 2013. Available online: https://bitcointalk.org/index.php (accessed on 19 March 2021).
56. Eyal, I.; Gencer, A.E.; Sirer, E.G.; van Renesse, R. Bitcoin-ng: A scalable blockchain protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI), Santa Clara, CA, USA, 16–18 March 2016; pp. 45–59.
57. Singh, S.; Hosen, A.; Yoon, B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
58. Qi, X.; Zhang, Z.; Jin, C.; Zhou, A. A Reliable Storage Partition for Permissioned Blockchain. *IEEE Trans. Knowl. Data Eng.* **2021**, *33*, 14–27. [CrossRef]
59. Qiu, C.; Ren, X.; Cao, Y.; Mai, T. Deep Reinforcement Learning Empowered Adaptivity for Future Blockchain Networks. *IEEE Open J. Comput. Soc.* **2021**, *2*, 99–105. [CrossRef]
60. Sun, W.; Li, S.; Zhang, Y. Edge caching in blockchain empowered 6G. *China Commun.* **2021**, *18*, 1–17. [CrossRef]
61. Wu, H.; Cao, J.; Jiang, S.; Yang, R.; Yang, Y.; Hey, J. TSAR: A Fully-Distributed Trustless Data ShARing Platform. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 350–355. [CrossRef]
62. Chen, N.; Cho, D.S.-Y. A Blockchain based Autonomous Decentralized Online Social Network. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 15–17 January 2021; pp. 186–190. [CrossRef]
63. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Data Management in Supply Chain Using Blockchain: Challenges and a Case Study. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019; pp. 1–8. [CrossRef]
64. Ricci, L.; Maesa, D.D.F.; Favenza, A.; Ferro, E. Blockchains for COVID-19 Contact Tracing and Vaccine Support: A Systematic Review. *IEEE Access* **2021**, *9*, 37936–37950. [CrossRef]
65. Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. *IEEE Access* **2021**, *9*, 36868–36878. [CrossRef]
66. Mohanta, B.K.; Jena, D.; Ramasubbareddy, S.; Daneshmand, M.; Gandomi, A. Addressing Security and Privacy Issues of IoT Using Blockchain Technology. *IEEE Internet Things J.* **2021**, *8*, 881–888. [CrossRef]
67. Li, Y.; Ruan, Q. Petri Net Modeling and Analysis of the Drug Traceability System Based on Blockchain. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 15–17 January 2021; pp. 591–595. [CrossRef]
68. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access* **2021**, *9*, 12730–12749. [CrossRef]
69. Mazumder, M.M.H.U.; Islam, T.; Alam, M.R.; Al Haque, M.E.; Islam, M.S.; Alam, M.M. A Novel Framework for Blockchain Based Driving License Management and Driver's Reputation System for Bangladesh. In Proceedings of the 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 5–7 January 2021; pp. 263–268. [CrossRef]
70. Hewa, T.M.; Hu, Y.; Liyanage, M.; Kanhare, S.; Ylianttila, M. Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research. *IEEE Access* **2021**. [CrossRef]
71. Sadawi, A.; Hassan, M.S.; Ndiaye, M. A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges. *IEEE Access* **2021**, *9*. [CrossRef]
72. Rottenstreich, O. Sketches for Blockchains. In Proceedings of the 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 5–9 January 2021; pp. 254–262. [CrossRef]