applied sciences

MDPI

Review

A Survey on Consensus Protocols and Attacks on Blockchain Technology

Abhishek Guru [1], Bhabendu Kumar Mohanta [2,*], Hitesh Mohapatra [3,*], Fadi Al-Turjman [4,5], Chadi Altrjman [6] and Arvind Yadav [1]

1 Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, AP, India
2 Department of CSE, Gandhi Institute of Technology and Management (Deemed to be University), Visakhapatnam 530045, AP, India
3 School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar 751024, OD, India
4 Artificial Intelligence Engineering Department, AI and Robotics Institute, Near East University, Mersin 99138, Turkey
5 Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia 99320, Turkey
6 Department of Chemical Engineering, Waterloo University, Waterloo, ON N2L 3G1, Canada
* Correspondence: bhabendukumar@gmail.com (B.K.M.); hiteshmahapatra@gmail.com (H.M.)

Abstract: In the current era, blockchain has approximately 30 consensus algorithms. This architecturally distributed database stores data in an encrypted form with multiple checks, including elliptical curve cryptography (ECC) and Merkle hash tree. Additionally, many researchers aim to implement a public key infrastructure (PKI) cryptography mechanism to boost the security of blockchain-based data management. However, the issue is that many of these are required for advanced cryptographic protocols. For all consensus protocols, security features are required to be discussed because these consensus algorithms have recently been attacked by address resolution protocols (ARP), distributed denial of service attacks (DDoS), and sharding attacks in a permission-less blockchain. The existence of a byzantine adversary is perilous, and is involved in these ongoing attacks. Considering the above issues, we conducted an informative survey based on the consensus protocol attack on blockchain through the latest published article from IEEE, Springer, Elsevier, ACM, Willy, Hindawi, and other publishers. We incorporate various methods involved in blockchain. Our main intention is to gain clarity from earlier published articles to elaborate numerous key methods in terms of a survey article.

Keywords: consensus protocols; ARP spoofing attack; DDoS; sharding attack; ECDSA

check for updates

Citation: Guru, A.; Mohanta, B.K.; Mohapatra, H.; Al-Turjman, F.; Altrjman, C.; Yadav, A. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2604. https://doi.org/10.3390/app13042604

Academic Editors: Gianluca Lax and Yu-Dong Zhang

Received: 11 December 2022
Revised: 20 January 2023
Accepted: 2 February 2023
Published: 17 February 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Santoshi Nakamoto introduced the initial blockchain in his published whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 [1]. In this, he described the cryptocurrency's technical specifications and motivations and also suggested how Bitcoin provides a strong case for the invention of a new payment system. He also explored how transactions work, how individuals are rewarded for their efforts [1], the use of a network, and also outlines how privacy is key to Bitcoin in the same way it is for the banking industry.

Decentralization is the most important feature of blockchain technology, which means that the storage of data is distributed and stored on a number of blocks in the network. This type of distributed system provides more robustness to blockchain technology. In this distributed system, if some nodes have faults, they do not affect the other nodes. This is one of the best features of this technology and it is very useful for cyber-physical systems and other systems.

Currently, the manufacturing of cyber-physical systems is facing issues such as security, privacy, flexibility problems [2–7] and data integrity, transparency, and many more. The industry has various problems related to security [8–12]. Blockchain technology has

various features to overcome these issues [13,14]. Many industries now use blockchain technology to secure their system. Blockchain technology is very efficient, not only in financial technology but also [7–9] in industry. In [8], the five-level architecture known as 5C-CPS was anticipated for evolving CPSs in manufacturing sectors. The use of blockchain technology in real-time applications is widespread; however, we have found that issues remain in networking, data privacy, data security, and centralization, paving the way for further research and development.

Additional security and privacy features are required for use in secure distributed storage. To improve the privacy and security of blockchain technology, we must use hybrid cryptography or advanced cryptography [15–17]. For blockchain scaling, we have proof of luck for efficiency in the consensus protocols arena. However, following an in-depth study on major consensus algorithms, there is a need for future case-specific applicability of these consensus algorithms. The security and privacy of blockchain needs to be upgraded because with the enhancement of technology, the protection of data is a major issue. Many hackers are updating their computational power and therefore the security of blockchain can be broken down in the future [18–20]. These consensus algorithms [21–27] are delegated Byzantine fault tolerance (dBFT), tangle (IOTA), proof of stake (PoS), delegated proof of stake (DPoS), proof of weight, proof of elapsed time, proof of history, proof of stake velocity, proof of importance, proof of reputation, proof of burn, proof of identity, proof of activity, proof of time, ouroboros, proof of retrievability, proof of capacity, Byzantine fault tolerance, delayed proof of work, RAFT, stellar consensus, proof of believability, directed acyclic graphs, Hashgraph, proof of work (PoW), holochain, block lattice (nano), proof of existence, SPECTRE, proof of authority, ByteBall, etc. [28–32].In this paper, we focus on consensus protocols and the attacks on them. Detailed security features need to be improved, as recently we have suffered attacks on consensus algorithms, such as DDoS attacks and sharding, in a permissionless blockchains, and with the presence of Byzantine adversaries such as these, many attacks are happening.

A consensus mechanism is a fault-tolerant technique used in blockchain systems to obtain the necessary agreement among distributed processes or multi-agent systems, such as cryptocurrencies, on a single data value or a single state of the network. It is useful for keeping records, among other things. Many researchers reviewed and surveyed consensus protocols, and some of them surveyed popular consensus protocols, such as PoW (proof of work), PoS (proof of stack), PoW (proof of weight), and PoET (proof of elapsed time) [1,3,5,6]. Some studies surveyed on the basis of PoW (proof of work), and the IoT, surveying popular consensus protocols and discussing their performance, vulnerabilities, and their properties. We include 30 consensus protocols in this paper. We surveyed 30 consensus protocols on the basis of security because this blockchain technology is adopted by many sectors for keeping records secure.

Recently, blockchain technology has been proliferating technology [21–26] in academia, industry, and government sectors around the world. This technology has numerous application domains in almost all spheres of human life [27–32]. This technology's potential has encouraged research and industry communities to explore its usefulness in different application domains. As a result, we have a plethora of blockchain systems omnipresent in several domains with real-time use. Presently, security and privacy in blockchain scenarios are in four groups:

- Contract privacy
- Auditability and transparency
- Transactional privacy
- Accountability and non-repudiation
- However, many of these need advanced cryptographic protocols.

The main intention of this survey is to provide a brief study on existing consensus protocols and the attacks on blockchain technology that occurred until 2022. To achieve this, we have surveyed recently published referenced articles from various sources, such as IEEE, Scopus, Hindawi, Elsevier, Springer, ACM, and others sources. We have used some

keywords to identify referenced publications, such as "Blockchain consensus Protocols," "Security issues of Blockchain Technology," "Attacks on Blockchain," and "Privacy issues of Blockchain Technology." By using these queries, we identified many existing reference articles and conducted our survey. We have represented the attacks on blockchain and consensus protocols in tabular format in Tables 1–4 and at the end, we have discussed some recent surveys of blockchains in Table 5.

Table 1. Comparison of the consensus algorithms with respect to generic parameters.

Authors, Year	Algorithm	Blockchain Type	Mining	Scalability	Latency
L.Luu et. al. 2016 [33]	ELASTICO (2016)	Permissionless	Computational power	Scalable	Low
Z. Renl et. al. 2017 [34]	Implicit consensus (2017)	Permissioned	Proof-based	Not Scalable	High
j. Zou et al. 2017 [35]	Proof of trust (PoT) (2018)	Permission-based consortium	Probabilistic and voting mining	Scalable	Low
Neo white paper [36]	DBFT consensus algorithm (2018)	Permissioned	Random selection of miner	Not Scalable	Very Low
D. Schwartz et al. 2014 [37]	Ripple (2014)	Permissioned	Voting mining	Scalable	Low
K. Li, H. Li et al. 2017 [38]	Proof of vote (2017)	Consortium	Voting mining		Very Low
C. Dwork et al. 1992 [39]	Proof of work (2008)	Permissionless	Computational power	Not Scalable	Very High
Kiayias et al. 2016 [40]	Proof of stake (2011)	Permissioned and permissionless	Node wealth and staking age	Scalable	High
L. Ren 2014 [41]	Proof of stake velocity (2014)		Stake and amount (velocity)	Scalable	Low
L. Bentov et al. 2014 [42]	Proof of activity (2014)	Permissionless	Effectiveness of work by the miner	Scalable	Low
Wiki [43]	Proof of burn (2014)	Permissioned and permissionless	Coin burning (probabilistic lottery)	Scalable	Average
M. Castro et al. 1999 [44]	Practical Byzantine consensus algorithm (1999)	Permissioned	Round of mining	Not Scalable	Very Low

Table 2. Blockchain Privacy and Security Issue.

Author, Year	Category of Blockchain Privacy and Security Issues	Discussion
Yourong Chen et al. [45] 2022	Attack of consensus excitation	The consensus stimulation attack includes an attacker generating additional proceeds by tampering with the block consensus outcome on the blockchain. In the consensus excitation attack, the mining pool employs block withholding, selfish mining attacks, and pool hopping.
Sherin Hijazi et al. [46] 2019	The middle protocol attack	1. This attack alludes to the behavior of attackers who launch hackers against smart contracts and node communication. Middle protocol attacks use network communication attack methods, such as Sybil, eclipse, and DDoS. One of the smart contract attack methods is re-entrance. 2. An attacker's behavior in an application scenario is designed to compromise user privacy. Identity theft and transaction information attacks are examples of application service attacks that violate privacy. Among the defense, methods are the mixed coin protocol, ring signature., and zero-knowledge proof.

Table 3. Attacks on the blockchain with description.

Authors Year	Attack	Description
Firdous Kausar et al. 2022, [47]	Core-oriented	This sort of assault targets the architecture, components, and protocols of the blockchain. It spreads to the lower levels, including the machines that run them and the industry network protocols that those machines use to connect with one another.
	Transaction malleability	The signature secures the transaction, but nothing secures the signature. The purpose of a hacker could be to sabotage the transaction by modifying the signature in an arbitrary way, rendering it invalid. As a result, the transaction is canceled.
	Liveness attack	These attacks operate in three stages: delay, prep, and deny, and can cause a delay in the target transaction's acknowledgment. During the preparation process, the attacker seeks to gain an advantage over honest players in order to establish an isolated blockchain. If the attacker thinks the delay is not long enough, they move on to the blockchain render step, where they try to slow down the chain transaction's growth rate.
	Spatial partitioning and BGP hijacking	The full nodes' ledger views and the simplified payment verification nodes' ledger views are derived from the nodes. The entire nodes are widely dispersed over the globe. By owning one or more independent systems that perform traffic routing, ISPs control the flow of traffic on the web. A hostile AS that hosts the majority of full nodes can intercept communication from a target AS.
	Stress testing	DDoS stress testing is a service that evaluates a company's readiness for several DDoS attack scenarios and flood magnitudes. Controlled tests are performed on your IT infrastructure at a predetermined period and with real-time online assistance.
	Memory pool flooding	This is a one-of-a-kind DDoS attack. Miners usually prioritise communications in the memory pool grounded on the mining payment. To put it another way, the highest-mining-fee transactions are chosen and mined first.
	Block withholding	Malicious nodes commit this act by purposefully masking, forging, or withholding critical information that must be relayed across the network.
	Finney	In this attack, the miner can generate a block containing a transaction from address A to address B, where both addresses belong to them. Then, using the same currencies, you will make another payment from address A to address C. (which belongs to another user). If the user accepts the transaction without receiving network confirmation, the attacker can release the block containing their initial transaction. This renders the merchant's transaction invalid, allowing the attacker to double spend.
	51% attack	This is a situation in which a single entity or organisation controls 50% or more of the hashing rate computation power. In such a case, the mining will always be won by the attacker.
	Consensus delay	This form of attack aims to inject latency into the network, resulting in block rejection, and preventing peers from achieving consensus on any other sabotage reasons or status of the blockchain, and this could be accomplished in a number of ways. They could inject erroneous blocks, such as blocks with double-spending transactions.
	Client-oriented attack	This section looks into attacks on blockchain client programs, such as those that run on user or miner machines.
	Wallet thief	If malware is installed on a computer, it may be possible to steal a user's private keys or conduct transactions as their representative unless those keys are protected and encrypted.

Table 3. *Cont.*

Authors Year	Attack	Description
M. Saad, et al. 2018 [48]	Crypto-jacking attack	Crypto-jacking is the unlawful mining of cryptocurrencies on someone else's computer. Hackers achieve this by infecting an online ad or website with program code that auto-executes by convincing the victim to click on a malicious link in an email that installs crypto-mining code on the computer.
Rajasekhar Chaganti et al. [49]	Double spending	The term "double spending" refers to the same transaction twice or more.
	DNS attack	When a node first connects to a network, it consults a DNS server to see which nobles are currently available. A hacker could poison the DNS server at the resolver or introduce an erroneous list of speeder nodes before that time. As a result, the node will believe it is connected to the genuine Bitcoin network when, in fact, it is connected to the attackers.
	DDoS attack	DDoS attacks are a type of DoS attack. A DDoS attack entails a network of connected online devices, known as a botnet, that are used to flood a target website with bogus traffic. DDoS attacks, unlike other types of cyberattacks, do not attempt to breach your security perimeter. A DDoS attack, on the other hand, seeks to make your website and servers unavailable to legitimate users.
Yuval Marcus et al. 2018 [50]	Eclipse	When an eclipse attack is carried out, the attacker attempts to redirect the target user's outbound and inbound connections away from genuine nearby nodes and toward attacker-controlled nodes, effectively isolating the target from the rest of the network.
Jayashree Sengupta et al. 2020 [51]	Sybil	The eclipse attack hides the true ledger state from a single node, whereas the Sybil attacks the entire network. With a number of alienated nodes, the attacker will overwhelm the network. Alternatively, they can slag to get relay blocks, essentially barring other network users, or they can allow a 51 percent or double-spending assault to take place.
X. Fu, H. Wang et al. 2021 [52]	Time-jacking	Nodes on the crypto coin preserve an inner counter that indicates network time. The node gains the network time by entreating it from neighbouring nodes during the bootstrapping phase, calculates and stores the median, and so on. The system time will be used if the median is greater than 70 min. An eclipse attack, for example, would be used in an attack to allow neighbouring nodes to supply false timestamps.
Sarah Bouraga 2021 [53]	Selfish mining	Selfish mining is a shady cryptocurrency mining approach in which a single miner or a group solves a hash, creates a new block, and keeps it off the public blockchain. This step generates a fork, which is then mined to gain an advantage over the public blockchain. The group's blockchain can introduce its newest block to the network if it gets ahead of the honest blockchain. As the network is set up to recognize the most recent block, the fork by the group would erase the original blockchain. By modifying the blockchain, miners might effectively steal money from other users.
Eyal 2018 [54]	Fork after withholding	The following is how the FAW attack is carried out. Infiltration mining occurs when a miner enters a selected pool while remaining a miner in their preferred pool. If they mine a block using FPoW at their preferred pool, they immediately submit it and earn legitimate profit as pool manager.

Table 4. Attacks and their targeted areas and effect.

Authors Year	Attack	Targeted Area	Effect of Attack
T. Bamert et al. 2013 [55]	Brute Force	Computing Power	Data Encryption
P. Mecorry et al. 2017 [56]	Refund	Payment Protocol	Lose Reputation
E.-R. Latifa et al. [57]	Wallet	Private key	Loss of Bitcoin
T. Bamert et al. 2014 [58]	Time Hijacking	Network	Fake Peers
S. Jarecki et al., 2016 [59]	Long Range	Database	Changes the Transaction History
D. Mills et al. 2010 [60]	BGP Hijacking	Database Protocol	Fake Transaction
A. Gkaniatsou et al. 2017 [61]	Sybil	Network	Pseudonymous Identities
	DDoS	Network	Unnecessary messages about transaction
Y. Marcus et al. 2018 [50] JOE STEWART 2018 [62]	Eclipse Attack	Network	Different view of the network
BENNETT GARNER 2018 [63]	DAO	Computing Power	Fake Transaction
Hackernoon 2018 [64]	Nothing at Stack	Block	Slow Consensus
A. Begum et al. 2020 [65]	Pool Mining	Block	Slow Verification Time
H. Lee, M. Shin et al. 2018 [66]	Double Spending	Bitcoin Transactions, Pow Consensus	Lose Products
I. Eyal and E. G. Sirer 2018 [67]	Selfish Mining	Computing Power	Enhance Personal Share on Transaction
Dave Gutteridge 2018 [68]	Spam	Network	Slow Transaction Network

Table 5. Previous surveys and their outcome.

Authors Year	Consensus Protocols	Outcome
L. S. Sankar et al. [29], 2017	Stellar consensus protocol (SCP), Byzantine fault tolerance (BFT)	They focused on analyzing the feasibility and efficiency of these consensus protocols.
	Survey of consensus protocols on blockchain applications	They had surveyed previously proposed consensus protocols and analyzed their efficiency characteristics.
Salimitari. et al. [69], 2018	PoW, PoS, PoC, PoET, DPoS	Surveyed consensus protocols for IoT networks where they reviewed existing consensus methods that have been implemented to realize a blockchain-based IoT network and also discussed open research challenges in blockchain and IoT networks.
Wahab A. et al. [70], 2018	PoW, PoS, PoL	Surveyed some popular consensus protocols and identified that each protocol has its own strengths and weaknesses. They conclude that many researchers are working to develop a scalable, secure, and efficient consensus protocol for the growth the of economy and infrastructure.
Xiao, Y et al. [71], 2020	Classical fault tolerance consensus and general blockchain consensus protocols	They conducted this survey on the basis of fault tolerance, performance, and vulnerabilities.
Rani Poonam et al. [72], 2022	Consensus algorithms which are based on PoW (proof of work)	Analyzed all six variants of PoW on the basis of the scalability maintenance cost, pros, cons, and block generation time, transaction cost, energy consumptions, etc.
Jain Arpit, et al. [73],2021	General consensus protocols	Conducted a comprehensive survey of consensus algorithms on the basis of their transaction, performance, and architecture.

The paper is arranged as follows. Section 2 describes blockchain, how it works, and its structure. Section 3 describes the types of blockchains. Section 4 describes the literature on consensus protocols. Section 5 includes the classification of attacks on blockchain. Section 6 discusses the DDoS attacks and ARP spoofing attacks. Section 7 describes other recent important attacks. Section 8 includes some of the preventive measures from past works and research.

2. Overview of Blockchain

A blockchain is a "distributed database that maintains a growing list of ordered records called blocks." These blocks are "linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data [74]. As a decentralized, public digital ledger used to record transactions, records cannot be retroactively changed without changing the consensus of all subsequent blocks and networks." An example of blockchain is shown in Figure 1. A block only has one parent block if the block header contains a preceding block hash. It is important to note that the hashes of uncle blocks, or the children of a block's forebears, would also be kept in the Ethereum blockchain. The first block of the blockchain is called the genesis block which has no parent block [33]. The following section details the internals of the blockchain.

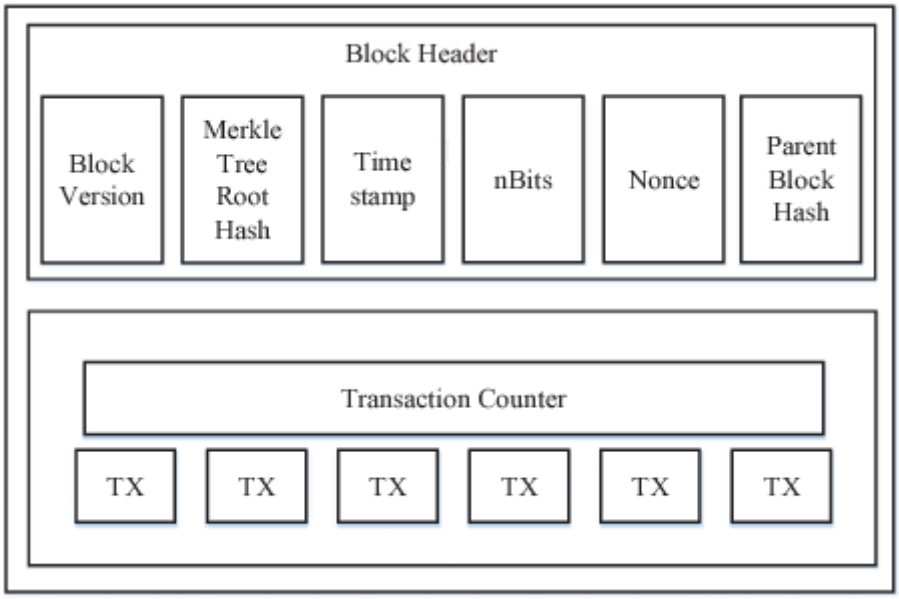


Figure 1. Architecture of Blockchain.

➢ Blocks in the Blockchain

A block contains a block header and the block body as shown in Figure 2. In particular, the block header has:

- Block version: decides which set of block validation guidelines should be used.
- Merkle tree root hash: the sum of the hashes for each transaction in the block.
- Time stamp: since 1 January 1970, the current time is expressed in seconds in universal time.
- nBits: optimum block hashing threshold.
- Nonce: a four-byte field that typically starts at zero and gets bigger with each hash computation.
- Parent block hash: a 256-bit hash that directs the user to the prior block.
- Transaction counter: a transaction counter and transactions make up the block body. A block can contain a maximum number of transactions depending on the block size and the size of each transaction.

Blockchain validates the authenticity of transactions via an asymmetric cryptography algorithm. Asymmetric cryptography-based digital signatures are utilized in an unreliable setting. The illustration of a digital signature is as follows:

➢ Digital Signature

Digitally signed transactions are sent across the network. A typical digital signature has two phases: a signing phase and a verification phase. For example, user Alice wants to send a message to another user, Bob. (1) At the signing stage, Alice encrypts the data with her private key and sends the encrypted result and the original data to Bob. (2) During the

verification phase, Bob verifies the value with Alice's public key. This way Bob could easily see if the data had been tampered with or not. A typical digital signature algorithm used in the blockchain is the elliptic curve digital signature algorithm (ECDSA).

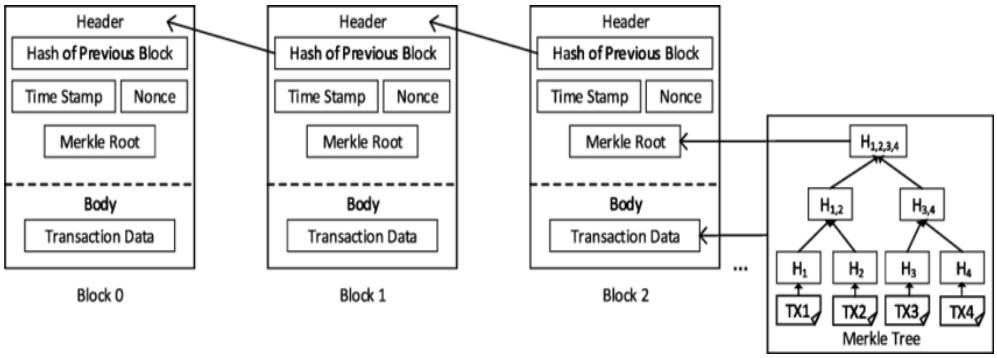


Figure 2. Structure of blockchain.

3. Types of Blockchain

To meet the needs of various applications, blockchains are often divided into public blockchains, private blockchains, and consortium blockchains based on the rules governing which nodes can access, verify, and authenticate the transactions initiated by other nodes [74]. There are three types of blockchains:

1. Permissionless or Public Blockchains: A blockchain network that is public or permissionless allows for unrestricted participation by anyone. On a public blockchain that is managed by laws or consensus algorithms, the majority of cryptocurrencies operate.
2. Permissioned or Private Blockchains: Organizations can restrict who has access to blockchain data using a private, or permission, blockchain. Specific sets of data can only be accessed by users who have been given permission. An example of a permissioned blockchain is the Oracle blockchain platform.
3. Federated or Consortium Blockchains: A blockchain network where a predetermined group of nodes or a predetermined number of stakeholders tightly regulate the consensus process (mining process).

4. Consensus Protocols

A consensus algorithm is a procedure that allows each peer of a blockchain network to establish a common agreement on the state of a distributed ledger. In other words, a consensus algorithm is a protocol that allows all nodes in a blockchain network to reach a common consensus regarding the current state of data in the ledger and trust unknown peers in the network. In past surveys, we saw that many of them had undertaken comparatively limited numbers of consensus protocols, such as proof of work, proof of stack, and proof of activity, etc. [21,27,29,33–36]. However, at present, we have approximately 30 consensus protocols, and these protocols have their own security features which must be discussed for further enhancement of security. In this paper, we survey 30 consensus protocols from various sources and we discuss the elliptic curve digital signature algorithm (ECDSA), because it is used in most blockchain-based systems.

Abdul Wahab and Waqas Mehmood [70] surveyed several popular consensus protocols. Every consensus protocol has trade-offs between security, scalability, efficiency, and performance. Each of these protocols has benefits and drawbacks, and they all serve different purposes and offer domain-specific solutions. Above all, they all serve a common purpose in a distributed ledger, which is to prevent double-spending. The PoW payment system pioneered a decentralized payment system that prioritized security and data integrity over scalability and computational cost. Instead of hashing, it was proposed that the useless work of PoW be replaced with useful work, such as solving a scientific problem. This is still a conceptual blockchain design that may or may not be implemented. Although POS effectively solved the problem of ineffective mining, the design introduced risks of

centralization. Many researchers were drawn to it because of its efficiency and secure implementation, and a few PoW-based implementations, such as Ethereum, have also migrated to POS. The current trend is toward a hybrid approach, in which implementation is based on two or more consensus protocols, such as Decreed, which employs both PoW and POS.

In [71], the authors provide a detailed review of blockchain consensus which has gained popularity. They produced an instantaneous review of traditional fault tolerance consensus research, a five-component framework, performance analyses, protocol abstractions, methodology, and conversation on protocol design for blockchain consensus protocol. They investigated the fault tolerance, performance, and vulnerabilities of various protocols, as well as their applications.

In [72], the authors initiated a consensus algorithm operational model that allows them to describe blockchain and directed acyclic graph-based consensus algorithms. Furthermore, emanating from the proposed process model, they reclassified and compared the prevailing mainstream blockchain consensus algorithms, and presented the estimation context of consensus algorithms. They also discussed the safety principles for improving the most frequent attacks, for example, eclipse attacks, denial of service (DoS) attacks, and double spending, and analyzed the blockchain in dissimilar situations from the point of view of security. To verify performance and security, researchers are increasingly favoring the incorporation of trusted execution environments into blockchains. Blockchain performance can be enhanced at a low source cost if a weakly centralized trusted execution environment assistant is allowed.

Shijie Zhang et al. [75] have conducted thorough studies on the consensus protocols of blockchain. They introduced some common blockchain consensus protocols and analyzed and compared their strength, shortcomings, and application scenarios. They came to the conclusion that when creating a good consensus protocol, it is important to think about not only fault tolerance, but also how to make the best use of it in the right application scenario.

Ashok Kumar Yadav and Karan Singh [76] surveyed the fundamentals of blockchain technology, analysis, and important consensus algorithms and application areas. The following research will cover various enactment platforms, such as Ethereum and Hyperledger.

Qianwen WANG et al. [77] summarized the popular blockchain consensus algorithm. The internal application, advantages, and disadvantages of the DPOS, POW, POS, and BPFT are explained by outlining their varied requirements and conditions. Current research is focused on the POW–POS hybrid consensus mechanism. It is also an innovative way of leveraging smart contracts to make consensus rules more transparent. The consensus algorithm's deployment in practice is also an examination of the algorithm. The novel attack approach may be useful in identifying the flaws in the current consensus algorithm. They can employ alternative underlying consensus methods for different throughput requirements, business scenarios, and security assumptions to better support top-level applications. To better support the highest applications for different business scenarios, quantity requirements, and security expectations, they employ different underlying consensus algorithms.

The authors of [78] surveyed the hardware implementation of the PoW consensus. The Ethereum blockchain employs this type of consensus. They were able to prove that to successfully implement this consensus on low-resource platforms, an on-chain system that successfully receives and transfers data can be combined with an off-chain system that performs the consensus and sends the result to the on-chain node. Despite its complexity, this system achieves a five-fold increase in execution time over a pure software system while using the least amount of energy.

Daniel Mago Vistro et al. [79] proposed a classification of all consensus protocols and their variants in our paper. The scoring and selection criteria based on the publisher have also been provided by them. A comparable analysis table was created with the most commonly used consensus protocols, and finally, all previous and existing protocols were described with their advantages and disadvantages, invention year, and implantation year.

Each protocol has a use that can be used to find the appropriate tilt. According to their analysis table, the PoW is difficult to implement because of its high computing power cost. There have been numerous different consensus methods and variants discovered, so instead of putting our efforts in danger by utilizing PoW, we can use different protocols to complete our tasks.

The authors of [80] presented a classification of the necessary qualities of a consensus algorithm and used this classification to thoroughly analyse every algorithm. In addition to these consensuses, algorithms are categorized into two main categories: non-incentivized algorithms and incentivized consensus algorithms. In the non-incentivized algorithm, participants are presumed to be trustworthy. As a result, no incentives are required to ensure desired behavior, whereas an the incentivized consensus algorithm, only used by public blockchain systems and cryptocurrencies, relies on incentives to motivate participants to behave as planned. These algorithms are typically found in private blockchain environments. They have classified incentive-based algorithms into three categories: PoS, consensus algorithms, and PoW.

In [81], the authors reviewed the consensus categories, mechanisms, and their influence in a distributed environment. Consensus mechanisms for distributed systems in general, and blockchain in particular, were discussed. They compared a number of expected consensus algorithms in terms of parameters that have a substantial impact on the consensus algorithm. The specification chosen for evaluation addresses both performance and security concerns, along with each of the parameters that have been identified. Aside from these, a number of other factors must be taken into account. Network topology, transaction rate, consistency of consensus solutions, concurrency check, and round complexity are all factors to consider (if there were several rounds or phases in the consensus algorithm). These parameters can be utilized to undertake a more complete comparison in preparation for future research. The comparative perspective offered in this work has emphasized the parameters that need to be evaluated and analyzed for several contemporary algorithms. To fill in the gaps in the comparison, a full qualitative and quantitative comparison can be performed. To accurately evaluate the strengths and limits of consensus algorithms in regard to large data needs, experiments in a cluster setting are required.

In [82], the authors examined consensus algorithms, their classification, implementation, and utility in the blockchain network. They have compared the different discussed consensus algorithms on a variety of parameters, as well as how each consensus algorithm's implementation differed from the others. They have outlined the numerous research obstacles confronted in this blockchain subdomain, in addition to the benefits.

5. Classification of Attacks on Blockchain

In this section, we discuss classifications of attacks from various past works and papers. Firstly, a description of an attack is required. An attack is an information security threat that attempts to obtain, modify, destroy, delete, embed, or disclose information without authorized access or permission. It happens both to individuals and to organizations [83–85]. There are many types of attacks: passive, active, targeted, clickjacking, brandjacking, botnets, phishing, spam, internal, and external.

In [45], Yourong Chen et al. discuss an overview of blockchain by explaining the evolution of blockchain from 1.0 to 3.0, including its characteristics and block structure. In this section, they explain the characteristics of blockchain, its block structure, as well as workflow of it. In short, they discuss the complete structure and security features of the blockchain. The authors of this paper also summarize the defense method and mining attack of the mining pool and also explain the attack and defense methods of privacy thefts.

In [47], Firdous Kausar et al. discuss the classification of attacks on blockchain. They reviewed the attached discussed in the following section.

6. DDoS Attacks and ARP Spoofing Attacks

Rajasekhar Chaganti et al. [81] reviewed a thorough examination of blockchain-based solutions for DDoS attack detection and mitigation, taking into account various network environments such as SDN, IoT, cloud, and traditional networks. The solutions are classified based on their location, which includes network-based, near-victim, and hybrid solutions. They discovered that the majority of existing solutions concentrated on storing malicious IP addresses in blockchain transactions implemented with smart contracts and distributing the IP addresses across ASs (autonomous systems) at the network level.

In [82], the authors surveyed and analyzed a few consensus protocols. Despite their differences in strengths and weaknesses, each of these protocols serve distinct purposes and domain-specific solutions. Above all, they serve as a common solution to one of the main issues with distributed ledgers, namely double-spending. The current method leans toward a hybrid approach, with execution based on two or more consensus protocols. The consensus protocol, which is the foundation of a blockchain, is available in a variety of implementations to meet the needs of different use cases. Researchers have been attempting to establish an efficient, scalable, and assured consensus protocol that may generate outstanding results and aid in the expansion of the economy and infrastructure since the introduction of the consensus protocol, PoW.

In [84], it is mentioned that the address resolution protocol is easily spoofable and subject to poisoning attacks due to its lack of security mechanisms. An ARP intoxication attack takes advantage of obtaining access to and using complex data on the network in the same way that a legitimate user would. In this study, they looked into the theory of ARP spoofing attacks as well as several existing techniques for defending against them. According to the findings, both identifying and determent systems should be used in the network for optimal security measures, with care paid to minimize their impact. They suggested and demonstrated a new method for identifying and deterring ARP poisoning, impersonation, and spoofing attacks.

In [85], Ahmed M. Abdel Salam et al. suggested a scalable solution that automatically configures static ARP entries to prevent address resolution protocol spoofing attacks. The suggested method is a client-server that automatically configures static ARP entries to prevent address resolution protocol spoofing. Both static and dynamic host configuration protocol networks can use the protocol. Their suggested protocol comprises two individual algorithms for the client-server to avoid the address resolution protocol spoofing attack. To avoid the threat of a rogue server, the client algorithm adds a static record for the server to the client address resolution protocol cache. It also automatically acquires the user's IP and MAC addresses, making it difficult for the user to submit fraudulent data to the server. To ensure that incoming register messages from clients are coming from a reliable host, the server algorithm evaluates the hash code. To send the hash code users are given only three chances. If the server flops to send the hash, the user will be blocked.

In [86], the authors describe the many types and categories of ARP protocol vulnerabilities. They also create and develop an application for ARP spoofing and MITM attacks. Then they created and built a basic distributed defense system that operates on the devices of end users to defend them from attacks. As demonstrated by deploying and executing the last protocol on the user system, the process aids in protecting the user from such threats. This is a summary of the suggested defense system. The following scenario assumes that a targeted system defense program is running and is being attacked:

1. At first, it is suspected that the router has been abandoned.
2. When the defense program is launched in the targeted machine, an ARP appeal package is received by a router, which will provide the correct MAC/IP mapping in response.
3. The application keeps track of the mapping. The router's MAC address is then monitored on a regular basis by issuing an address resolution protocol request packet and comparing the responses to the previously cached ones.

4. An attacker launches a man-in-the-middle attack (MITM) by delivering poisoned address resolution protocol answers to both the targeted system and the router.
5. The router refurbishes its address resolution protocol table based on the poisoned replies.
6. The program informs the attack, removes the infected entry from the address resolution protocol table, sends a salve packet to a router with the correct MAC/IP, and reveals the attacker's MAC and IP addresses.
7. Both the defense and attack processes will continue to try to change the router's ARP table, resulting in a race condition.
8. At last, the targeted system can report the attack incident using the exposed information.

The authors discuss ARP spoofing attacks and provide a thorough examination of existing solutions in both traditional and software-defined networking (SDN) environments. By leveraging SDN capabilities, a light, reliable, fast, and effective mechanism for preventing ARP spoofing has been proposed that does not require any additional hardware or software. A module that examines every address resolution protocol packet in the network for possible faked packets and blocks them has been added to the SDN controller in this effort. Using SDN features, this article offered an efficient solution for combating address resolution protocol requests and response-based spoofing attacks in an SDN context. Infrastructure changes, changes to the address resolution protocol, and changes to the OpenFlow protocol are not required by the proposed approach. There are no requirements to install any further software or hardware in the network. A dependable IP-MAC is required for the suggested technique to work. The main table is located on the controller and interacts with the DHCP server.

7. Other Important Attacks

In [87], Yizhong Liu et al. divided sharding blockchains into a number of components, each of which is examined for its underlying concepts, existing techniques, and potential issues. Designing a new sharding blockchain system might be reduced to putting together a number of distinct components on this basis. As a result, each component could be improved independently based on the most recent research, and the improved component could be integrated into a whole sharding blockchain system without compromising the security of other parts or the entire system. The potential problems and future research directions proposed in this paper are worthy of consideration for each component.

In [88], the authors present a knowledge systematization for blockchain sharding. They identified key components and difficulties in sharding. The ability to place participating nodes uniformly into shards is dependent on publicly verifiable randomness. A consensus protocol is required within each shard to reach an agreement on the blocks. Existing solutions are dominated by BFT-based protocols. The protocol must ensure atomic properties for cross-shard transactions. Finally, at the end of an epoch, a reconfiguration process is required. They examined several well-known blockchain sharding protocols before debating potential research directions.

In [89], Jinwen Xi et al. outlined sharding knowledge, and emphasized the need for sharding in systematized and scalable blockchain design, which includes cross-shard transaction atomicity, intra-shard consensus protocol, and general enhancements. They also presented precise computations and unique insights based on multidimensional analysis of the features and constraints of the investigated sharding processes, as well as a comprehensive comparison and evaluation.

In [90], the authors present several consensus protocols for comparing the qualities of blockchain technology in terms of computation, vulnerabilities, and other factors. They provide a complete view of public and private blockchains and also present a taxonomy of all consensus protocols. Finally, the analysis of those protocols yields a comparison table.

In [91], Saewar Sayeed et al. conducted intensive reviews on the latest and future contests in blockchain and have reviewed five major attacks, demonstrating that current protection techniques are insufficient, leaving this technology vulnerable to attackers. One of the innovative consensus methods is proof of adjourn (PoAj), which can overcome

attacks such as one endorsement attacks, 51 percent occurrence, transaction confirmation latency, zero confirmation assaults, and miner bribery.

In [92], the authors investigate the blockchain's attack surface and assign attacks to the blockchain's cryptographic constructions, the causal communication construction, and the environment in which they are utilized. They draw attention to important dangers and ongoing defense research. They believe that, despite current and established defenses, numerous attacks on blockchains can still be launched, with some of those assaults being exploited to aid the launch of others. They suggest new research avenues that must be followed in order to make blockchains more secure and effective by defining these assaults and reviewing their responses.

In [65], A. Begum et al. highlighted a study on blockchain and blockchain attacks and their solutions, as previously described. They investigated the affected and conducted areas, as well as the double-spending attack. They provided a solution after demonstrating the limitations of the double-spending attack. They create a pattern of real-world blockchain attacks which will be beneficial to new researchers in this field. On the other hand, if we can raise funds and implement a proposed model in the real world, we may be able to protect our bitcoins from a double-spending attack.

8. Prevention Measures for Attacks

In [93], the authors reviewed the blockchain concept and relevant issues, as well as a thorough examination of probable security assaults and existing results that can be used as countermeasures. In this article, they also reviewed many ways to improve blockchain security by summarizing key aspects that may be used to create security tools and blockchain systems that address security problems. Finally, the study covers outstanding concerns and future research paths in blockchain IoT systems. Using real-world examples, the authors of this review paper thoroughly examined many assaults on blockchains as well as blockchain security issues. Furthermore, while delving into these concerns in a variety of ways, this article examined the numerous security issues, weaknesses, and assaults that hamper the further adoption of blockchain technology. They also covered a variety of other blockchain applications and benefits, as well as significant business potential. Finally, they summarized existing security solutions for diverse situations as well as research challenges that have yet to be tackled.

Shikah J. Alsunaidi and Fahd A. Alhaidari [94] conducted a comprehensive study on blockchain technology, focusing on popular consensus algorithms in order to determine their features and the factors that affect security and performance. Furthermore, they awarded the consensus algorithm a categorization. They addressed in depth the consensus algorithm that was researched, as well as an analysis of the main elements affecting these algorithms, and they have referred to certain recommendations that must be considered and can help the growth of this area.

In [95], the authors propose a novel architecture that detects and prevents malevolent activities of collaboration inside the blockchain node. They demonstrated how the smart contract conducts identification and authentication of rogue nodes by setting up a blockchain network in the lab separately for proof of concept. They assessed the performance on the following classifications of attacks:

(a) Attempts to bring the blockchain down

(b) Attempts to put invalid data into the database

(c) Attempts to hijack unauthorized data

They also measure the time it takes to identify an attack to assess the architecture's performance. According to the data, the proposed architecture offers a good likelihood of identifying and isolating insider harmful behavior [63].

In [96], according to this study, blockchain is a popular technology for dealing with transactions that require high levels of security. This technology provides and complies with the secure operation and handling and crucial security considerations are required. There are several flaws that potentially lead to some of the attacks that have been found.

Even though blockchain is cohesive with existing security technologies, appropriate technology must be invented to overcome these risks and attacks. To summarize, consensus mechanisms, private key security obtained through public-key encryption schemes, illegal activity caused by cryptocurrency applications, double spending obtained through transaction authentication procedures and transaction privacy effluence obtained through a transaction design stream, and sinner smart contracts caused by smart contract applications may all pose significant risks to blockchain 1.0 and 2.0. Other dangers to blockchain 2.0 include smart contract vulnerabilities caused by a program design problem, under-optimized smart contracts caused by a program writing flaw, and under-priced processes caused by an EVM design flaw. We can simply argue that they are all linked because most attacks provide room for subsequent attacks.

In [97], Teng Hu et al. propose a blockchain-based tracking solution for insider threats. To begin, this research creates an insider network model from a unique viewpoint that intercepts insider attackers from escaping and its forensics. They then look at why locating attackers and gathering authentication during an insider threat is so difficult. The blockchain traceability system's data, transaction and block structures, consensus, data storage, and query algorithms are created, with differential privacy used to protect user privacy.

In [98], the authors discuss the Ethereum blockchain's security threats, attack scenarios, and mitigation strategies. At various levels of Ethereum, including the application layer, smart contract layer, and network layer, thirteen security attacks were explored. Based on their attack principles, the paper presented the corresponding preserved approaches. Improving the overall quality of Ethereum smart contracts can help to prevent attacks. Finally, they also presented tests to see how effective these protection systems are.

9. ECDSA [Elliptic Curve Digital Signature Algorithm]

We are aware of the current widespread use of ECDSA in blockchain-based systems and cryptocurrencies [30]. Data integrity is guaranteed using the ECDSA method to avoid data manipulation. Scott Vanstone put forth this algorithm in 1992. In any network, the data integrity of the message is crucial because an attacker can alter the information as it is transmitted from source to destination. For the secure transmission of data, many blockchain-based systems used the ECDSA. The ECDSA is now used by several cryptocurrencies and blockchain-based platforms [29]. However, the ECDSA has a problem; the elliptic curve (EC) backdoors are utilized. In this section, we address the ECDSA, which is currently used in blockchain-based systems and cryptocurrency. We have preiosuly described how the ECDSA works in blockchain security.

The EC works as follows:

Let GF (f), be a prime field.

Then let s, t GF (f) be constants, such that 4s3 + 27t2 = 0. An EC E(s, t), over GF(f) is considered as the set of points (x, y) $\in$ GF (f) $*$ GF (f) which fulfil the (1)'s requirement:

$$y2 = x3 + Sx + T \quad (1)$$

Here, S and T are constants and O is the point at infinity.

In the elliptic curve discrete logarithm problem (ECDLP) it is well known that:

If G is a group, then we use the ECDLP to get the integer a, for group elements S and T in such a way that T = aS.

Current markets require algorithms that are faster in computation, and the ECDSA [29] is one of them.

We know that the ECDSA has three steps:

1. Generation of key
2. Generation of signature
3. Verification of signature.

In the generation of key or parameter step, the required chosen EC is well-defined over a finite field Fc with the characteristic c, and with a base point G Ec(s, t) with an order of n.

Then we select a random integer h so that $1 \leq h \leq n - 1$.

Then it computes T = hG.

Here, the public key pair is (T, h).

In the signature generation step for signing a message m, the signer follows the steps:

Step 1 is selecting an integer k in such a way that $1 \leq k \leq n - 1$.

Step 2 is computing kG = (x1, y1).

Step 3 is computing r = x1 mod n, and in the case of r = 0, then we have to select new k.

Step 4 is calculating $k-1$ mod n and e = h(m).

Step 5 is computing $s = p-1(e + kr)$, if s = 0 then it should go back to step 1.

So (r, s) is the generated signature for the message m.

In the verification of signature step for verifying the signature (r, s) of message m, verifier V follows these steps:

Step 1 is V checks whether r, s ϵ [1, n − 1].

Step 2 is to compute e = h(m) and s − 1.

Step 3 involves the computation of u = es − 1 mod n and v = rs − 1 mod n.

Step 4 involves the computation of w = (x2, y2) = uG + vT, if w = 0 then stop, otherwise to compute t = x2 mod n.

The signature is valid in one case, that is t = r.

Proof of verification process is as below in (2):

$$\begin{aligned} kG &= s - 1(e + kr)G \bmod n \\ &= s - 1eG + s - 1rkG \bmod n \\ &= uG + vQ \bmod n \end{aligned} \tag{2}$$

Therefore, uG + vT = kG and so t = r, which is requisite.

10. Discussion

Blockchain technology is the most popular technology adopted by many industries, and many sectors are working on implementing this technology [96,99]. This technology has many benefits that are very useful in data security and decentralization. Some core benefits are as follows:

- Real-time transaction settlement
- More security and transparency
- No third-party involvement
- Durability and reliability
- Immutability
- Cost saving
- User pseudonymity

In [100], Nasrollahi, M. et al. discussed how studying social networks can affect many aspects of life and also help many businesses in some cases. Given the relevance of the two concerns of social networks and R&D, their study investigates the relationship between social networks, technology relationships, and information security efficiency with the performance of research and development projects at the MAPNA development company. For this case study, they distributed a questionnaire of 19 questions to 196 employees of the company, and after receiving the results they found that social networks have a positive impact on research and development performance and information technology.

In [101], Mortazavi Ravari et al. discussed this idea in a research and technology organization by investigating it from two perspectives: "the notion of effectiveness in research projects" and "the concept of effectiveness in RTOs" (RIPI). At the Research Institute of Petroleum Industry, eight technology development projects are being studied in order to evaluate and implement the recommended framework. The effectiveness of

eight technology development projects was evaluated using ARAS, COPRAS, MOORA, and TOPSIS multi-criteria decision-making approaches based on the specified indicators and their weights.

This paper discussed the consensus protocols and attacks on blockchain technology. The consensus protocols and attacks on blockchain technology are presented in detail in this study [52,102]. The ECDSA (elliptic curve digital signature algorithm) is used in many blockchain-based architectures for security consideration, but still many threads are attacking blockchain-based architectures. As a result, we have discussed the consensus protocols and classifications of attacks for research purposes. In the near future, many sectors will use this technology for better security and privacy, so our focus is to enhance the security and efficiency of blockchain [103–106]. This paper will guide other researchers to identify the privacy and security gaps in blockchain technology.

In Table 5 we have mentioned some existing surveys and their outcomes. In previous surveys, we found that most of them used popular consensus protocols and attacks, but now there are many consensus protocols proposed and they have to be reviewed for further enhancement of blockchain technology [107,108]. Three are also many attacks happing in blockchain technology that need to be reviewed. In this survey article we tried to provide researchers with detailed information regarding all 30 consensus protocols. By analyzing this paper, they can implement new ideas to enhance the security features of blockchain. As this technology is not limited to cryptocurrency, many other sectors such as education, healthcare, government, etc., are adopting this for securing their records.

Due to the distinctive characteristics of blockchain, it may be applied in a variety of fields, such as IoT networks, healthcare, data storage, inventory monitoring, and finance [77]. The main problem is figuring out how to tailor blockchain technology to specific application requirements. As each application has unique requirements, a new or customized blockchain solution is required.

In this paper we addressed the following research questions:

RQ 1: How many consensus protocols exist in 2022?

Various types of consensus algorithms have been devised over time for varying applications. In Table 1, we can see consensus protocols that have been proposed as of 2022 and each consensus protocol has its own pros and cons. For consensus protocols, we surveyed many resources, and as mentioned, we used the keywords "Consensus Protocols of Blockchain" and identified all the above protocols. Table 5 contains recent surveys, but they have one common limitation: they surveyed only popular blockchain consensus protocols such as PoW, PoS, delegated PoS, etc., but as we know that as of 2022, there are approximately 30 consensus protocols. For further enhancement of blockchain technology, they all needed to be reviewed.

RQ 2: What were the various attacks on blockchain technology as of 2022?

Blockchain may appear to be the ultimate security infallible technology, with immutability, distributed consensus, established trust, distributed identity, and eternal verifiable claims [109]. However, new-age security assaults are emerging that are more sophisticated and can inflict massive irreparable damage. It is critical for everyone building and deploying blockchain systems to understand these threat vectors. In Table 2, we can see the privacy and security issues in blockchain technology, and in Table 3 we have mentioned attacks on blockchain as of 2022. In Table 3, attacks on blockchain and their targeted areas are listed. To identify these attacks, we surveyed many resources, including Elsevier, IEEE, Hindawi, ACM, and other sources.

11. Conclusions

A distributed ledger is a disruptive technology that has revolutionized business processes with its application and adaptability. Behind every great distributed ledger implementation, there is a consensus protocol that powers it. In this paper, we surveyed consensus protocols and attacks on blockchain technology for research purposes. No consensus protocol is perfect, and there are always certain trade-offs related to performance,

security, and scalability efficiency. Each of these protocols provides domain-specific solutions and serves different purposes in spite of having their strengths and weaknesses. Presently, the trend is shifting towards a hybrid approach; that is, implementation will be based on two or more consensus protocols. There are many attacks happening on blockchain, including DDoS, ARP, sharding, etc., and to address security concerns these are consensus protocols that must be reviewed. For further enhancement of blockchain security and privacy, this paper will guide researchers. However, recently discussed security attacks must be aimed at improving the security and efficiency of blockchain technology so that blockchain-based architectures can become more secure and more efficient architectures in the near future.

Author Contributions: Writing—original draft preparation, conceptualization, and formal review, A.G.; writing—review and editing, B.K.M.; writing—review and editing, H.M., F.A.-T.; review and editing, C.A.; review and editing, A.Y.; review and editing All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors would like to thank the editor-in-chief, editor, and anonymous reviewers for their valuable reviews.

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

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 November 2017).
2. Monostori, L.; Kádár, B.; Bauernhansl, T.; Kondoh, S.; Kumara, S.; Reinhart, G.; Sauer, O.; Schuh, G.; Sihn, W.; Ueda, K. Cyber-physical systems in manufacturing. *CIRP Ann.* **2016**, *65*, 621–641. [CrossRef]
3. Li, Z.; Barenji, A.V.; Huang, G.Q. Toward a Blockchain cloud manufacturing system as a peer-to-peer distributed network platform. *Robot Comput. Integr. Manuf.* **2018**, *54*, 133–144. [CrossRef]
4. Yu, T.; Lin, Z.; Tang, Q. Blockchain: The introduction and its application in financial accounting. *J. Corp Account. Financ.* **2018**, *29*, 37–47. [CrossRef]
5. Vora, J.; Nayyar, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.J.; Rodrigues, J.J. Bheem: A Blockchain-based framework for securing electronic health records. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018.
6. Sethi, A.; Sethi, S. Flexibility in manufacturing: A survey. *Int. J. Flex. Manuf. Syst.* **1990**, *2*, 289–328. [CrossRef]
7. Lee, J.; Kao, H.A.; Yang, S. Service innovation and smart analytics for Industry 4.0 and big data environment. *Procedia Cirp* **2014**, *16*, 3–8. [CrossRef]
8. Lee, J.; Bagheri, B.; Kao, H.A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
9. Yang, L. Industry 4.0: A survey on technologies, applications and open research issues. *J. Ind. Inf. Integr.* **2017**, *6*, 1–10.
10. Xu, X. From cloud computing to cloud manufacturing. *Robot Comput. Integr. Manuf.* **2012**, *28*, 75–86. [CrossRef]
11. Palma, L.; Vigil, M.A.G.; Pereira, F.L.; Martina, J.E. Blockchain and smart contracts for higher education registry in Brazil. *Int. J. Netw. Mgmt.* **2019**, *29*, e2061. [CrossRef]
12. Zissis, D.; Lekkas, D. Addressing cloud computing security issues. *Future Gener. Comput. Syst.* **2012**, *28*, 583–592. [CrossRef]
13. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Inc.: Newton, MA, USA, 2015. Available online: https://link.springer.com/article/10.1365/s40702-018-00468-4 (accessed on 3 September 2022).
14. IBM Blockchain Based on Hyperledger Fabric from the Linux Foundation. 2017. Available online: https://www.ibm.com/Blockchain/Hyperledger (accessed on 6 September 2022).
15. IOTA Developer Hub. 2017. Available online: https://www.iota.org/research/meetthe-tangle (accessed on 6 September 2022).
16. Pustišek, M.; Kos, A. Approaches to Front-End IoT Application Development for the Ethereum Blockchain. *Procedia Comput. Sci.* **2018**, *129*, 410–419. [CrossRef]
17. Viktor Trón, F.L. Ethereum Specification. 2015. Available online: https://github.com/ethereum/go-ethereum/wiki/Ethereum-Specification (accessed on 7 September 2022).
18. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 71.

19. Bailis, P.; Narayanan, A.; Miller, A.; Han, S. Research for practice: Cryptocurrencies, Blockchains, and smart contracts; hardware for deep learning. *Commun. ACM* **2017**, *60*, 48–51. [CrossRef]
20. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain technologies: The foreseeable impact. *Computer* **2017**, *50*, 18–28. [CrossRef]
21. Cachin, C.; Vukoli, M. Blockchains Consensus Protocols in the Wild. *arXiv* **2017**, arXiv:1707.01873.
22. Iota: A Cryptocurrency for Internet-Of-Things. Available online: https://www.iota.org/ (accessed on 8 September 2022).
23. Tangle. Available online: https://iota.org/IOTA_Whitepaper.pdf (accessed on 10 September 2022).
24. Bano, S.; Sonnino, A.; Al-Bassam, M.; Azouvi, S.; McCorry, P.; Meiklejohn, S.; Danezis, G. Consensus in the Age of Blockchains. *arXiv* **2017**, arXiv:1711.03936.
25. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in Blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
26. Banerjee, M.; Lee, J. Raymond Choo KK, A Blockchain future for internet of things security: A position paper. *Digit. Commun. Netw.* **2017**, *4*, 149–160. [CrossRef]
27. Baliga, A. Understanding Blockchain Consensus Models. 2017. Available online: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf (accessed on 10 September 2022).
28. Pilkington, M. *11 Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016; pp. 225–253.
29. Sankar, L.S.; Sindhu, M.; Sethumadhavan, M. Survey of consensus protocols on Blockchain applications. In Proceedings of the 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017; IEEE: New York, NY, USA, 2017; pp. 1–5.
30. Underwood, S. Blockchain beyond bitcoin. *Commun. ACM* **2016**, *59*, 15–17. [CrossRef]
31. Seibold, S.; Samman, G. Consensus: Immutable Agreement for the Internet of Value. 2016. Available online: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmgBlockchain-consensus-mechanism.pdf (accessed on 1 December 2022).
32. Mukhopadhyay, U.; Skjellum, A.; Hambolu, O.; Oakley, J.; Yu, L.; Brooks, R. A brief survey of cryptocurrency systems. In Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; IEEE: New York, NY, USA, 2016; pp. 745–752.
33. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open blockchains. In Proceedings of the 2016 23rd ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; ACM: New York, NY, USA, 2016; pp. 17–30.
34. Ren, Z.; Cong, K.; Pouwelse, J.; Erkin, Z. Implicit Consensus: Blockchain with Unbounded Throughput. *arXiv* **2017**, arXiv:1705.11046v3 [cs.DC].
35. Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.; Li, L. Proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. *IEEE Trans. Serv. Comput.* **2018**, *12*, 429–445. [CrossRef]
36. A Distributed Network for Smart Economy, in Neo, White Paper. 2019. Available online: https://docs.neo.org/docs/en-us/basic/whitepaper.html (accessed on 3 December 2022).
37. Schwartz, D.; Youngs, N.; Britto, A. The ripple protocol consensus algorithm. *Ripple Labs Inc. White Pap.* **2014**, *5*, 151.
38. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of vote: A high performance consensus protocol based on vote mechanism and consortium blockchain. In Proceedings of the 2017 IEEE 19th International Conference on High Performance Computing and Communications (HPCC), Bangkok, Thailand, 18–20 December 2017; IEEE: New York, NY, USA, 2017; pp. 466–473. [CrossRef]
39. Dwork, C.; Naor, M. Pricing via processing or combatting junk mail. In Proceeding of the 12th Annual International Cryptology Conference Santa, Barbara, California, USA, 16–20 August 1992; Springer: Berlin/Heidelberg, Germany, 1992; pp. 139–147.
40. Kiayias, A.; Russell, A.; David, B. Oliynykov, Ouroboros: A Provably Secure Proofof-Stake Blockchain Protocol. 2016. Available online: https://eprint.iacr.org/2016/889.pdf (accessed on 5 December 2022).
41. Ren, L. Proof of Stake Velocity: Building the Social Currency of the Digital Age. 2014. Available online: https://www.reddcoin.com/papers/PoSV.pdf (accessed on 5 December 2022).
42. Bentov, L.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of Activity: Extending bitcoin's proof of work via proof of stake. *ACM SIGMETRICS Perform. Eval. Rev.* **2014**, *42*, 34–37. [CrossRef]
43. Proof of Burn. Available online: https://en.bitcoin.it/wiki/Proofofburn (accessed on 22 March 2020).
44. Castro, M.; Liskov, B. *Practical Byzantine Fault Tolerance, in Proceedings of the Third Symposium on Operating Systems Design and Implementation*; USENIX Association: Berkeley, CA, USA, 1999; pp. 173–186.
45. Chen, Y.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z. A survey on Blockchain system: Attacks, Defences, and Privacy Preservation. *High-Confid. Comput.* **2022**, *2*, 100048. [CrossRef]
46. Hijazi, S.; Obaidat, M.S. A New Detection and Prevention System for ARP Attacks Using Static Entry. *IEEE Syst. J.* **2019**, *13*, 2732–2738. [CrossRef]
47. Kausar, F.; Senan, F.M.; Asif, H.M.; Raahemifar, K. 6G technology and taxonomy of attacks on Blockchain technology. *Alex. Eng. J.* **2022**, *61*, 4295–4306. [CrossRef]
48. Saad, M.; Khormali, A.; Mohaisen, A. End-to-end analysis of in-browser Cryptojacking. *arXiv* **2018**, arXiv:1809.02152.
49. Chaganti, R.; Bhushan, B.; Ravi, V. A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. *Comput. Commun.* **2023**, *197*, 96–112. [CrossRef]

50. Marcus, Y.; Heilman, E.; Goldberg, S. Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. *IACR Eprint Cryptol. Rep. Issue* **2018**, 236.
51. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
52. Fu, X.; Wang, H.; Shi, P. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Sci. China Inf. Sci.* **2021**, *64*, 121101. [CrossRef]
53. Bouraga, S. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Syst. Appl.* **2021**, *168*, 114384. [CrossRef]
54. Eyal, I. The Miner's Dilemma. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015.
55. Bamert, T.; Decker, C.; Elsen, L.; Wattehofer, R.; Welten, S. *Have a Snack, Pay with Bitcoins*; IEEE: Trento, Italy, 2013.
56. Mecorry, P.; Shahadashti, S.F.; Hao, F. *Refund Attacks on Bitcoin's Payment Protocol*; Springer Link: Berlin/Heidelberg, Germany, 2017.
57. Latifa, E.-R.; Ahemed, E.K.M.; Mohamed, E.G.; Omar, A. Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures. *J. Internet Bank. Commer.* **2017**, *22*, 1–29.
58. Bamert, T.; Decker, C.; Wattenhofer, R.; Welten, S. *Bluewallet: The Secure Bitcoin Wallet*; Springer Link: Berlin/Heidelberg, Germany, 2014; Volume 8743, pp. 65–80.
59. Jarecki, S.; Kiayias, A.; Krawczyk, H.; Xu, J. *Highly-Efficient and Composable Password-Protected Secret Sharing*; IEEE: Saarbrucken, Germany, 2016.
60. Mills, D.; Martin, J.; Burbank, J.; Kasch, W. *Network Time Protocol Version 4: Protocol and Algorithms Specification*; IETF: Fremont, CA, USA, 2010.
61. Gkaniatsou, A.; Arapinis, M.; Kiayias, A. *Low-Level Attacks in Bitcoin Wallets*; Springer Link: Berlin/Heidelberg, Germany, 2017; pp. 233–253.
62. Stewart, J. Bravenewcoin. 2018. Available online: https://bravenewcoin.com/insights/bitcoin (accessed on 5 December 2022).
63. Garner, B. Coincentral. 2018. Available online: https://coincentral.com/sybil-attack-blockchain/ (accessed on 5 December 2022).
64. Hackernoon. 2018. Available online: https://hackernoon.com/protocol-evolution-and-the-future-ofblockchain-governance-24ffd53c052b (accessed on 5 December 2022).
65. Begum, A.; Tareq, A.; Sultana, M.; Sohel, M.; Rahman, T.; Sarwar, A. Blockchain attacks analysis and a model to solve double spending attack. *Int. J. Mach. Learn. Comput.* **2020**, *10*, 352–357.
66. Lee, H.; Shin, M.; Kim, K.S.; Kang, Y.; Kim, J. *Recipientoriented Transaction for Preventing Double Spending Attacks in Private Blockchain*; IEEE: Hong Kong, China, 2018.
67. Eyal, I.; Sirer, E.G. *Majority Is not Enough: Bitcoin Mining Is Vulnerable*; ACM: New York, NY, USA, 2018.
68. Gutteridge, D. *Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack*; CCN: Singapore, 2018.
69. Salimitari, M.; Chatterjee, M. A Survey on Consensus Protocols in Blockchain for IoT Networks. *arXiv* **2018**, arXiv:1809.05613. [CrossRef]
70. Wahab, A.; Mehmood, W. Survey of consensus protocols. *arXiv* **2018**, arXiv:1810.03357.
71. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus protocols for Blockchain Network. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. [CrossRef]
72. Rani, P.; Kaur, P.; Jain, V.; Shokeen, J.; Nain, S. Blockchain-based IoT enabled health monitoring system. *J. Supercomput.* **2022**, *78*, 17284–17308. [CrossRef]
73. Jain, A.; Jat, D.S. A Review on Consensus Protocol of Blockchain Technology. In *Intelligent Sustainable Systems*; Nagar, A.K., Jat, D.S., Marín-Raventós, G., Mishra, D.K., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2022; Volume 334. [CrossRef]
74. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
75. Zhang, S.; Lee, J.-H. Analysis of the main Consensus Protocols of Blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
76. Yadav, A.K.; Singh, K. Comparative Analysis of Consensus Algorithms of Blockchain Technology. In *Ambient Communications and Computer Systems*; Hu, Y.C., Tiwari, S., Trivedi, M., Mishra, K., Eds.; Advances in Intelligent Systems and Computing; Springer: Singapore, 2020; Volume 1097.
77. Wang, Q.; Huang, J.; Wang, S.; Chen, Y.; Zhang, P.; He, L. A Comparative Study of Blockchain Consensus Algorithm. In Proceedings of the 2nd International Symposium on Big Data and Applied Statistics, Dalian, China, 20–22 September 2019.
78. Frikha, T.; Chaabane, F.; Aouinti, N.; Cheikhrouhou, O.; Ben Amor, N.; Kerrouche, A. Implementation of Blockchain consensus algorithm on embedded architecture. *Hindawi Secur. Commun. Netw.* **2021**, *2021*, 9918697. [CrossRef]
79. Vistro, D.M.; Farooq, M.S.; Rehman, A.U.; Malik, S. Smart Application Based Blockchain Consensus Protocols: A Systematic Mapping Study. In Proceeding of the 3rd International Conference on Integrated Intelligent Computing Communication Security, Karnataka, India, 6–7 August 2021.
80. Chaudhry, N.; Yousaf, M.M. Consensus Algorithm in Blockchain: Comparative Analysis, Challenges and Opportunities. In Proceedings of the 2018 12th International Conference on Open-Source Systems and Technologies (ICOSST), Lahore, Pakistan, 19–21 December 2018.

81. Chaganti, R.; Bhushan, B.; Ravi, V. The role of Blockchain in DDoS attacks mitigation: Techniques, Open Challenges and future Directions. *arXiv* **2022**, arXiv:2202.03617.
82. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A Research Survey on Application of Consensus Protocols in Blockchain. *Hindawi Secur. Commun. Netw.* **2021**, *2021*, 6693731. [CrossRef]
83. Katal, A.; Sethi, V.; Lamba, S. *Blockchain Consensus Algorithms: Study and Challenges*; Springer International Publishing: Cham, Switzerland, 2021. [CrossRef]
84. Al Sukkar, G.; Saifan, R.; Khwaldeh, S.; Maqableh, M.; Jafar, I. Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defence. *Commun. Netw.* **2016**, *8*, 118–130. [CrossRef]
85. AbdelSalam, A.M.; Elkilani, W.S.; Amin, K.M. An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries. *Int. J. Adv. Comput. Sci. Appl.* **2014**, *5*, 105–112.
86. Khalid, H.Y.; Ismael, P.M.; Al Khalil, A.B. Efficient Mechanism for Securing Software Defined network against ARP Spoofing attack. *J. Univ. Duhok* **2019**, *22*, 124–131. [CrossRef]
87. Liu, Y.; Liu, J.; Salles, M.A.V.; Zhang, Z.; Li, T.; Hu, B.; Henglein, F.; Lu, R. Building Blocks of Sharding Blockchain System: Concepts, Approaches, and Open Problems. *arXiv* **2021**, arXiv:2102.13364. [CrossRef]
88. Wang, G.; Shi, Z.J.; Nixon, M.; Han, S. SoK: Sharding on Blockchain. In Proceedings of the Proceedings of the 1st ACM Conference on Advances in Financial Technologies, New York, NY, USA, 21–23 October 2019; pp. 41–61. [CrossRef]
89. Xi, J.; Zou, S.; Xu, G.; Guo, Y.; Lu, Y.; Xu, J.; Zhang, X. A Comprehensive Survey on Sharding in Blockchains. *Mob. Inf. Syst.* **2021**, *2021*, 5483243. [CrossRef]
90. Bashar, G.; Hill, G.; Singha, S.; Marella, P.; Dagher, G.G.; Xiao, J. Contextualizing Consensus Protocols in Blockchain: A Short Survey. In Proceedings of the 1st IEEE International Conference in Trust, Privacy and Security in Intelligent Systems and Applications, Los Angeles, CA, USA, 12–14 December 2019.
91. Sayeed, S.; Marco-Gisbert, H. Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks. *Appl. Sci.* **2020**, *10*, 6607. [CrossRef]
92. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.H.; Mohaisen, D. Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1977–2008. [CrossRef]
93. Singh, S.; Hosen, A.S.M.S.; Yoon, B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
94. Alsunaidi, S.J.; Alhaidari, F.A. A Survey of Consensus Algorithms for Blockchain Technology. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–6. [CrossRef]
95. Ajayi, O.; Saadawi, T. Detecting Insider Attacks in Blockchain Networks. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021. [CrossRef]
96. Sabani, M.J.A.; Shafana, M.S.; Kariapper, R. Security Issues by Allied Attacks in Blockchain Technology. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 5371–5376.
97. Hu, T.; Xin, B.; Liu, X.; Chen, T.; Ding, K.; Zhang, X. Tracking the Insider Attacker: A Blockchain Traceability System for Insider Threats. *Sensors* **2020**, *20*, 5297. [CrossRef] [PubMed]
98. Duan, L.; Sun, Y.; Zhang, K.; Ding, Y. Multiple-Layer Security Threats on the Ethereum Blockchain and Their Countermeasures. Security and Communication. *Networks* **2022**, *2022*, 5307697. [CrossRef]
99. Aponte-Novoa, F.A.; Orozco, A.L.S.; Villanueva-Polanco, R.; Wightman, P. The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access* **2021**, *9*, 140549–140564. [CrossRef]
100. Nasrollahi MFathi, M.R.; Kiabakhshi, M. Investigating the relationship between social networks, technology relations and data protection efficiency with the performance of research and development projects (Case Study: MAPNA Development Company). *Q. J. Ind. Technol. Dev.* **2019**, *17*, 49–58.
101. Mortazavi Ravari, S.S.; Fathi, M.R.; Mohammadi, M.; Bandarian, R. Investigating the Concept of Effectiveness in Technology Development Projects in Research and Technology Organizations; Evaluating Eight Technology Development Projects in the Research Institute of Petroleum Industry (RIPI). *Pet. Bus. Rev.* **2020**, *4*, 21–41.
102. Alizadeh, M.; Andersson, K.; Schele, O. A Survey of Secure Internet of Things in Relation to Blockchain. *J. Internet Serv. Inf. Secur.* **2020**, *10*, 47–75.
103. Digiconomist, I. Bitcoin Energy Consumption Index, Digiconomist. 2018. Available online: https://digiconomist.net/bitcoin-energy-consumption (accessed on 5 December 2022).
104. Kausar, F.; Sadiq, M.A.K.; Asif, H.M. *Convergence of Blockchain in IoT Applications for Heterogeneous Networks, Real-Time Intelligence for Heterogeneous Networks*; Springer: Cham, Switzerland, 2021. [CrossRef]
105. Zhou, Z.; Chen, X.; Zhang, Y.; Mumtaz, S. Blockchain-Empowered Secure Spectrum Sharing for 5G Heterogeneous Networks. *IEEE Netw.* **2020**, *34*, 24–31. [CrossRef]
106. Li, X.; Zhao, M.; Zeng, M.; Mumtaz, S.; Menon, V.G.; Ding, Z.; Octavia, A. Dobre, Hardware Impaired Ambient Backscatter NOMA Systems: Reliability and Security. *IEEE Trans. Commun.* **2021**, *69*, 2723–2736. [CrossRef]
107. Zhou, Z.; Zhang, C.; Wang, J.; Gu, B.; Mumtaz, S.; Rodriguez, J.; Zhao, X. Energy-Efficient Resource Allocation for Energy Harvesting-Based Cognitive Machine-to-Machine Communications. *IEEE Trans. Cognit. Commun. Netw.* **2019**, *5*, 595–607. [CrossRef]

108. Kwon, Y.; Kim, D.; Son, Y.; Vasserman, E.; Kim, Y. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17), Dallas, TX, USA, 30 October–3 November 2017.
109. Heilman, E.; Kendler, A.; Zohar, A.; Goldberg, S. Eclipse attacks on Bitcoin's peer-to-peer network. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15), Washington, DC, USA, 12–14 August 2015; USENIX Association: Washington, DC, USA; pp. 129–144.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.