mathematics

MDPI

Article

Blockchain-Based Information Sharing Security for the Internet of Things

Abdullah Aljumah [1,*] and Tariq Ahamed Ahanger [2]

[1] College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
[2] Management Information Systems Department, College of Business Administration, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia; t.ahanger@psau.edu.sa
* Correspondence: aljumah@psau.edu.sa

Abstract: The Blockchain (BCT) is the first decentralized ledger to include a trust mechanism in its design. It establishes a trustworthy framework for distributed commands by using data redundancy at several nodes. Conspicuously, the current study presents a BCT-based lightweight IoT information exchange security architecture for data exchange. The proposed technique uses a dual chain methodology, namely transaction and data BCT working together to provide distributed storage and tamper-proofing of data. Moreover, Transaction BCT is enhanced by a consensus algorithm using a practical Byzantine fault-tolerant (PBFT) mechanism. The proposed algorithm can increase data registering efficiency, transactions, and privacy protection BCT. It is deduced that local dominance can be avoided using the dynamic game strategy of node cooperation. Furthermore, by reporting the node's global reputation value, the status of the unknown node may be approximated. The high-trust measure is utilized to adjust the weight of the affected node in the combined node-set, leading to the Bayesian equilibrium. The proposed model is validated in several experimental simulations and results are compared with state-of-the-art techniques. Based on the results, enhanced performance is registered for the proposed techniques in terms of temporal delay, statistical efficiency, reliability, and stability.

Keywords: Internet of Things; security; practical Byzantine fault-tolerant; Blockchain

MSC: 68T05

Citation: Aljumah, A.; Ahanger, T.A. Blockchain-Based Information Sharing Security for the Internet of Things. *Mathematics* **2023**, *11*, 2157. https://doi.org/10.3390/math11092157

Academic Editors: Ioana Boureanu and Liqun Chen

Received: 29 March 2023
Revised: 21 April 2023
Accepted: 2 May 2023
Published: 4 May 2023

1. Introduction

Encryption, Machine-to-Machine (M2M) data transfer, consensus, and distributed storage are basic aspects incorporated by the novel vision of Blockchain (BCT) technology. Several countries and international organizations have realized its potential usage. Moreover, many businesses are investing in BCT development [1]. Figure 1 shows the predictive rise of BCT in collaboration with the Internet of Things (IoT) market (Source: https://www.precedenceresearch.com/BCT-iot-market, accessed on 15 April 2023). Existing applications of BCT technology include digital asset trading and supply chain management. BCT has the potential to unleash a wave of innovation in service modes [2]. The IoT architecture tries to use BCT technology to address the security issue of data, allowing for user-directed interaction between all connected devices and the outside world [3]. Conspicuously, the current research proposes a decentralized and trustworthy IoT information-sharing security mechanism by incorporating BCT technology over conventional storage technologies [4]. There is currently no feasible method to secure the location data of IoT devices [5]. Global literature and use cases depict safeguarding location data on mobile devices. Location information protection via least squares estimate is suggested to address the ranging-based positioning security issue [6]. With the aforementioned approach, the precise position of each reference node is concealed, and only a fraction of computation is

carried out [7]. Using the consolidated result of the reference node computation, the user makes an approximation on specific data location [8]. The approach may safeguard both the user's and the reference node's location data at the same time as the user is unable to deduce the precise position of the referencing node from intermediary computation information [9]. Due to the sensitive nature of location data, location services employ a double encryption method to safeguard their users' private data [10]. This method encrypts the user interest points and the respective location at both the server and client. The service provider checks to see if the two sets of encrypted data match [11]. Although both approaches provide useful location data, their use is limited since that data cannot be utilized to power regular services [12].

Figure 1. Rise of IoT BCT Market.

1.1. Research Domain

The information security challenges of IoT devices are being investigated from several aspects, including the use of fuzzy computing, classical encryption, and BCT technology [13].

Nevertheless, most of the aforementioned BCT technologies are still in the academic research stage, so they do not apply to the large variety of location-based information application scenarios that exist today. Moreover, it does not enable users to manage the location information of their devices autonomously [14]. According to the aforementioned study, the shortcomings of the security model, including its flawed consensus method, lack of sufficient trustworthy authentication, restricted capacity, and inadequate computing capabilities, are the primary reasons for IoT security issues. The possible solutions include enhanced transaction efficiency and security using improved techniques, and bringing resource and data transactions on the trade BCT [15]. To address the critical issue, the incorporation of a security mechanism in the BCT-IoT is the need of the hour [16]. This is because traditional encryption technology is complicated to deploy on multiple IoT devices, making manipulation feasible to encompass integrity [17]. Similarly, conventional protection measures for securing networks have found it challenging to address the security requirement of the modern IoT. Researching and summarising the progress of IoT and BCT applications, analyzing the requirement for location security, and forcing for its implementation within the secure storage of device location, user location, and protected usage of location information are examples of BCT technology [18]. Using a better consensus method based on the practical Byzantine fault-tolerant (PBFT) mechanism, we can boost the efficiency of data registration, enable information data transmission on the transaction BCT, and secure user privacy.

1.2. State-of-the-Art Contribution

1. The current research presents a comprehensive framework for IoT security using BCT technology.

2. Specifically, the global reputation value is computed for every IoT node to estimate the current state.
3. The reputation measure is utilized to adjust the weighing measure of the vulnerable node using the equilibrium technique.
4. Moreover, a BCT-based decentralized database is presented for storing the locations of IoT devices for collective utilization.
5. The proposed technique is validated in several experimental simulations in which enhanced results were registered in comparison to the state-of-the-art techniques.

Table 1 shows the list of abbreviations used in the current research.

Table 1. List of Notations.

Notations	Meaning
BCT	BCT Technology
AI	Artificial Intelligence
DoS	Denial of Service
CC	Cloud Computing
DDoS	Distributed Denial of Service
API	Application Programming Interface
IoT	Internet of Things
DS	Data Security
QoS	Quality of Service
PoW	Proof of Work

Paper Organization

This paper's remaining sections are structured as follows. Section 2 reviews some of the relevant research works in the current domain of study. Information exchange between IoT devices using BCT is presented in Section 3. Section 4 presents the proposed BCT-inspired approach for data security. Section 5 depicts the experimental simulations for validation purposes. Finally, Section 6 concludes the paper with future research directions.

2. Related Work

2.1. BCT-Based Solutions for IoT Security

There has been a rise in the number of research publications that provide overviews of the design of BCT-based solutions for IoT applications. The focus of the state-of-the-art research is (a) To verify data integrity without a third-party auditor [19]; (b) to design a new distributed access control system for IoT systems [20]; (c) to design Fair Access (a decentralized pseudonym and privacy protection authorization management framework for IoT devices); and (d) to design a new distributed access control system for IoT systems [21]. Janani et al. [22] suggested a BCT-based authentication system for automotive networks and tested its efficiency using Omnet++ simulations. Whig et al. [23] developed a novel identity management technique for BCT-based cloud apps using the BlackRidge technology on a Windows host. Chen et al. [24] offered a BCT-based out-of-band two-factor authentication strategy for IoT security. Liao et al. [25] presented an IoT security technique to discover and filter insecure devices to prevent collusion and single-point failure of centralized servers. There have been attempts to implement smart contracts in security applications [26–28] due to the importance placed on the efficiency of transactions during information sharing, particularly in time and delay-sensitive applications like agriculture, transport, agriculture, and transportation [29]. This is because smart contracts enable the traceability, efficiency, and immutability of automated programming execution in a distributed way (for example, the execution of transactions without a third party). To discover any logical threats, Santra et al. [30] developed a security analysis tool to build the topology of the interactions. The widespread use of smart contracts in the real world has prompted the development of methods for identifying security aspects in AI [31]. There is a growing interest in zero-trust networked environments (where all network communication is treated as suspect, regard-

less of its origin), and many security solutions, particularly those based on BCT technology, are built. Vikram et al. [32] proposed a security framework assess risks according to dynamically changing settings and recommended implementing risk adaptive access control to zero trust networks. A technique to link security to a particular appropriate firewall syntax was presented by Alrubei et al. [33], who built an enforcement system to address access control issues in zero-trust networks. A proof-of-concept version of the framework was tested and found to be functional. To verify the infrastructure and transactions at varying degrees of trust, Alzuabi et al. [34] developed a BCT-based middleware for zero-trust hierarchical mining. Parcha et al. [35] presented a risk-based segmentation methodology for zero-trust IoT networks. Some researchers have recommended using BCT technology to eliminate the need for intermediaries when exchanging data as it can withstand typical threats like a single point of failure and collusion. To enhance the safety of autonomous vehicles, Velayudham et al. [36] developed a public BCT-based information-sharing method. Cryptography and other protocols are also used to ensure confidentiality. To overcome the difficulty of incorporating BCT technology into the Mobile-edge computing (MEC) system in the face of constrained channel resources and system load, Sille et al. [37] developed a secure data exchange framework for the MEC system by way of an asynchronous learning methodology. The authors also presented a privacy-preserving adaptive technique that uses less energy and has lower throughput on average. Although some of the aforementioned may use BCT, they are not decentralized. In addition, the sharing procedures may disregard the participants' fairness and privacy (i.e., personal information and geographical placements). Henceforth, the current research proposes a BCT-enabled information-sharing protocol optimized for use in a zero-trust IoT, which can independently realize the sharing process without relying on compromising personal privacy while still meeting the requirement of fairness during the identity authentication process.

2.2. *Ubiquitous Security Framework*

Cabrera et al. [38] introduced the idea of universally composable (UC) security, which has been used in several contexts including public-key encryption, signature, zero-knowledge, and identity authentication. To accommodate rogue protocols and non-repudiation, Mathur et al. [39] broadened the notion of UC security. In zero-knowledge reference string models, the alternative assumptions and protocols presented cannot be realized. Kumaresan et al. [40] presented minimal formalization of the "ideal certification authority" within the context of the UC security architecture. The authors provide a method for authenticating communications that ensures that each side is studied separately using a modular, cryptographic approach. Security study of the TLS protocol, such as that described by Jain et al. [41], would include, for instance, assessing the TLS handshake's crucial exchange phase inside a universal composable security framework. By sending messages at the TLS record layer, they were able to effectively replicate the communication sessions. Samanta et al. [42] used the UC framework for the protocols of RFID authentication, provided a unique, lightweight, and practical protocol with a pseudo-random bit generator for anonymous authentication, and achieved forward secure anonymity, authenticity, and availability in the UC model. For the 1-out-of-2 variation, Chowdhury et al. [43] provided non-adaptive oblivious transfer procedures for UC. Bai et al. [44] suggested a UC-secure adaptive k-out-of-N protocol, which is safe under bilinear assumptions, to solve the difficulty of extending to the adaptive k-out-of-N environment while still guaranteeing UC security. OpenStack's security issues and potential solutions were laid out and compared by Psathas et al. [45] in their examination of OpenStack inside the UC security framework. The universal composability framework is still frequently utilized in the security literature. This model has been used to verify the security of several protocols, including those suggested by Maiti et al. [46] and by Ali et al. [47]. Based on the comprehensive literature review, Table 2 depicts a comparative analysis with state-of-the-art research works relevant to the current study.

Table 2. Comparison analysis with state-of-the-art systems (Y Yes; N No).

Reference	Technique	Framework	Implementation	IoT-Specific	Reliable	Stable
[48]	BCT	Authentication	N	N	N	N
[49]	SDN	NU	N	N	N	N
[50]	BCT and SDN	Authentication Confidentiality Integrity	N	Y	N	N
[51]	BCT	Authentication	N	Y	N	N
[52]	BCT	Authentication/Confidentiality	Y	N	Y	N
[53]	SDN	Authentication	Y	Y	N	N
[54]	SDN	Authentication/Confidentiality	N	N	N	N
This Paper	BCT	Authentication Confidentiality Integrity	Y	Y	Y	Y

3. Proposed Method

It is challenging to create a useful connection of data in IoT technology due to the absence of an efficient sharing mechanism. In recent years, concerns about the safety of data exchanged between IoT devices have risen to the forefront of the information security debate. In the IoT, systems may communicate with one another and conduct business using either local or remote data storage and exchange methods. The problems with these processes are numerous:

1. The area of application is limited, as they only focus on one part of the information transmission chain or one perspective of an application situation
2. In the face of an enormous IoT infrastructure, there is no efficient technique to certify the legitimacy of wireless technology. IoT network leads to large data, expensive investment and maintenance costs for centralized data processing infrastructure, and a challenge in keeping up with the exponential increase of data.
3. IoT computing, transmission, and other resources for information like Actuators, location sensors, and geo-sensors, RFID, both time and resources are finite.

The aforementioned aspects motivate the proposal of a BCT-based IoT information exchange system. Achieving data sharing while maintaining data security is the goal of IoT information-sharing security. Information security encompasses not only the previously mentioned aspects of data protection, but also its authenticity, traceability, non-repudiation, and dependability. When it comes to fending off external attacks, making sure that block data is unforgeable and unalterable, and getting beyond double-payment concerns, BCT technology depends on the massive computational power created by consensus methods like Proof of Work (PoW) of distributed networks. Simplified Payment Verification (SPV) is a feature of many BCT systems, and it relies on Merkle trees and variations thereof to verify transactions without requiring users to keep the whole BCT. Because of the Merkle tree, BCT technology may be used on IoT devices without requiring a full copy of all blocks to be stored locally. The information stored in a BCT is encrypted using cryptography. Before being included in the block, the information must be checked for accuracy by every node. The BCT network's nodes may be openly queried after being written to, eliminating information advantages and lowering trust costs. Figure 2 shows the security mechanism for BCT technology over cloud computing platform. The immutability and precision of the BCT's records protect IoT users' personal information and assets. The decentralized BCT IoT nodes are immune to standard DDOS attacks. The current study offers a BCT-based IoT information-sharing security architecture, which collects and transacts source data to construct a system with matching source data and interaction security. IoT is often broken down into three distinct parts—the perception layer, the transmission layer, and the service layer. The architecture incorporates a dual chaining approach, which consists of a data and transaction BCT. Certain attributes of the proposed chaining mechanism are sent to the centralized computing paradigm because of the restricted resources of specific nodes of the IoT. Fog computing is located near the IoT terminal node or the data BCT component; cloud services are more focused on the application layer. Public chains constitute the backbone of most existing BCT applications. The increased trustworthiness of the public chain comes at the expense of identity and data privacy, since any node may join the BCT network and keep

the books. Conspicuously, the current study integrates public and private chain solutions. The public BCT is deployed in several IoT use cases. Moreover, the scenario makes use of alliance chains in several contexts. Alliances are formed between different sections of the same industry. Data on the BCT can only be updated by alliance members. Nodes that are not permitted cannot connect, and private connections are used to connect local nodes. Only approved nodes are allowed to store data on the BCT, making it almost impossible for other parties to access the ledger. However, the transaction BCT can encompass either the alliance or public chain, depending on the certain applicability domain, while the data BCT is only utilized for data accumulation from the source. It ensures that the time-sensitiveness and security needs are better than with the transaction BCT.

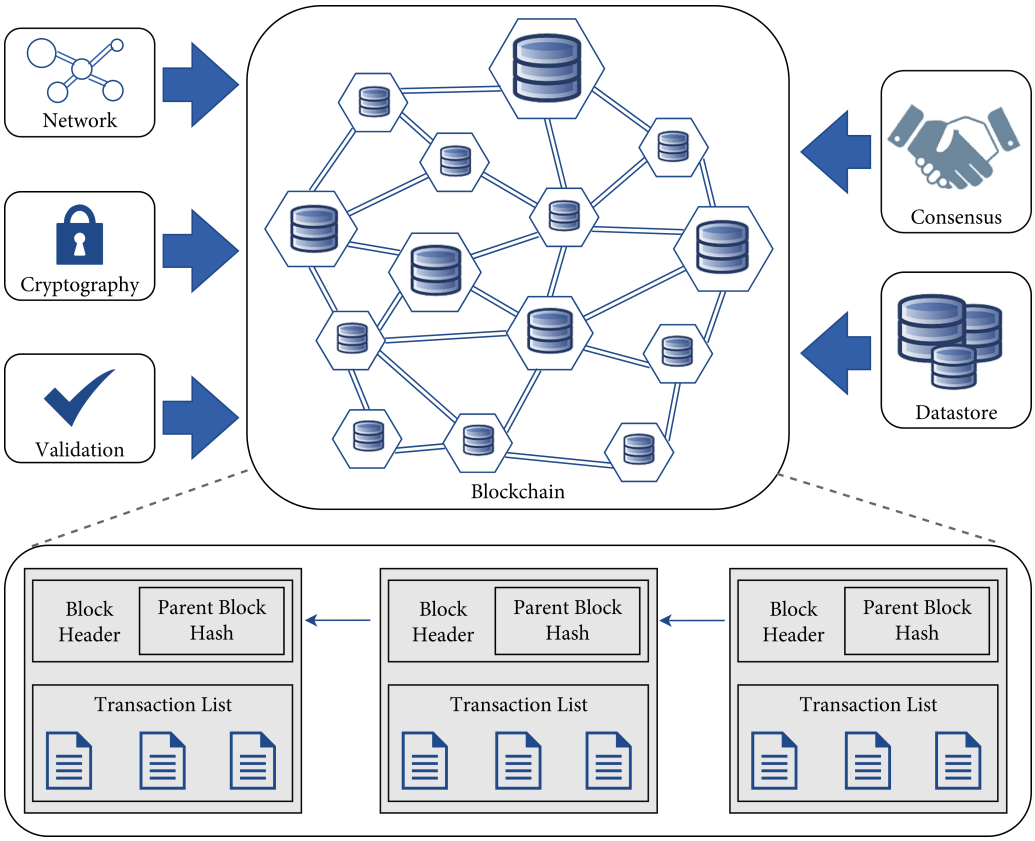

Figure 2. BCT Security structure.

3.1. Dual Mode of BCT Technology

To prevent the data from the front-end acquisition device from being tampered with or destroyed artificially, the source data must be trustworthy and accurate. With the IoT node, data is gathered via the BCT, and a data log is created using a private consensus process. Computing power, storage space, and bandwidth are all severely constrained by devices in the IoT, such as RFID readers, infrared thermometers, and other information-sensing gadgets. However, even if individual nodes of a smart device, such as a wearable computer, have a certain set of features, there should be less wasted effort and more productivity in the process of calculating and storing level data. Thus, it is important to categorize and allocate activities for the enormous heterogeneous data in the IoT. Before reducing data size and enhancing data quality, the IoT data is first separated into reduced and multimedia information. Then, by standardizing data expressions, data storage becomes simple to exchange. For distributed storage, the processed data is then separated into log data, which is a summary of the data and is kept in a node, and outsourced storage data is kept in a fog node and can be acquired in an instant when required. Traditional distributed consistency algorithms assume that no Byzantine nodes are present in the distributed system, which would allow for malicious data manipulation and the transmission of forged messages.

Byzantine networks need a fault-tolerant technique to address the issue of data consistency. Consequently, we refer to this kind of method as a Byzantine fault-tolerant distributed consensus algorithm.

The current consensus technique may be seen as a Byzantine fault-tolerant distributed consistency algorithm that synchronizes the data model with the real-world business context. BCT's consensus process is used to determine who builds each data block and how to keep the BCT consistent across all nodes. The conventional view is that one must pay to get the desired outcomes, and then use those outcomes as evidence of the price. Each new block is evaluated based on a set of predetermined criteria. This makes financial tracking more complicated. In addition, the accounting complexity is modified by inserting a random element into each page such that at any given moment, only a single node is created. The qualifying new block is the evidence of the burden, which is the cost of implementing the judgment process. For the PoW process to function as intended, it must adhere to the optimum chain and incentive technique. This means that the largest chain is rewarded and the computation of the qualifying block is. The notion of the optimum chain is a hard and fast guideline. The maximal effort is equal to the length of the longest chain. Without this strict protocol, each participant will build their BCT, rendering system-wide uniformity impossible. Building blocks may be seen as an investing habit, therefore the incentive concept is to utilize the cost of calculating to trade money to motivate individuals to keep track of it. The fundamental idea behind the workload proof technique is that more processing power means more likely block digging and stronger BCT security. Interaction with the tag is the primary indicator of terminal reader behavior in the trust architecture, while data routing, and thus whether or not it is true, is the primary indicator of intermediate reader behavior. The trust of the reader is split into two parts: trust based on routing, and trust based on authorization. In Figure 3, it can be seen how different levels of trust are associated with certain actions. Each kind of route trust is vulnerable to attacks.

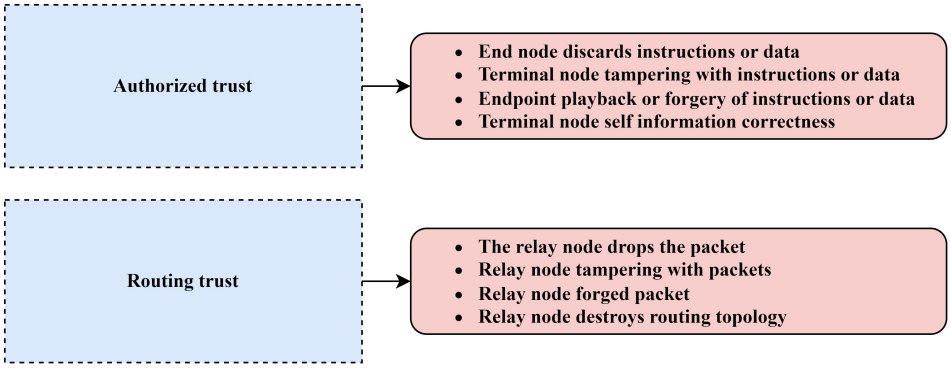

Figure 3. Types of reader trust.

3.2. BCT Structure Based on Time Stamp

The BCT organizes information into blocks of data and chains. A data block stores the current block as well as its header and content, and each block has a unique hash value as a block address matching. Each block in the chain is linked to the one before it by its hash value. The hash value and timestamp measure of the prior BCT are all included in the block header. Completed transactions are permanently stored in the block body and the BCT uses digital signatures to guarantee that the data in each transaction cannot be falsified or altered once it is been recorded. The Merkle tree hash function is used to produce all transaction data. The block header contains the one-of-a-kind Merkle tree root value. Merkle trees, a type of data storage, greatly enhance the scalability and efficiency with which transaction data can be queried and verified. At the same moment, the blocker stamps the block with the time it was formed, establishing a unique time stamp for each block. For improved data traceability in a bit currency system, additional information is included in the header region. This can be in the form of a random number, the target's

hash value, or anything else that can be used to form a possession Q dimension chain. With fewer nodes and stricter requirements for consistency and correctness, private and federal chains are the most common environments for the use of a consensus technique. The most common approach is the time-tested BFT algorithm for distributed consistency. BFT techniques include Byzantine fault tolerance (BFT) mechanisms, practical Byzantine fault tolerance (PBFT) mechanisms, Paxos mechanisms, and Raft mechanisms (without BFT). Consensus algorithms are typically used for networks with many nodes, and it can be challenging to ensure that all of those nodes are consistent and correct. PoW, PoS, and CP are the common mechanisms used on the public chain. The various consensus procedures are compared in Table 3.

Table 3. Comparison of information security consensus mechanism; H High, L Low, S strong, W Weak.

Evaluation Dimension	DPoS	PoW	PBFT	PoS
Performance efficiency	H	L	H	L
Fault tolerance	50%	50%	33.3%	50%
Compliance supervision	W	W	S	W
LF	H	H	L	H

The comparison reveals that the strong consensus method provides more security but at the expense of a more complicated algorithm (a multi-center mechanism). There is less agreement on security, even though the final consistency method is more disjointed and has a low algorithm complexity.

3.3. BCT-IoT Information Security

BCT-IoT involves the merging of digital and analog infrastructures. Some primary features include global optimization of the whole system, as well as real-time monitoring and detailed modeling of both digital and physical systems. By incorporating BCT technology into IoT, the energy information system may be converted from a specialized network using a proprietary protocol to an open network using an industry-standard protocol. Although providing technological support for the intelligence of BCT IoT systems, the widespread use of standard protocols and intelligent electronic devices in the BCT IoT information system raises concerns about network security. The future BCT will have to deal with security challenges such as internal connection and cascade failure throughout the space, as well as the interplay of the physical system and the information system. Henceforth, it is crucial to dissect the BCT's security problems, fortify the BCT's network, and make it more resistant to attacks and other risks. BCT technology operates independently of central authorities and other middlemen. With this approach, every node has the same weight, and everyone votes on whether or not a transaction is legitimate as a group. There is no risk to the integrity of the BCT as a whole if individual nodes are attacked and destroyed. BCT technology uses cryptography, digital signatures, and other methods to ensure that data cannot be altered once it has been recorded. The approach is simulated in Matlab, and the experimental results are displayed in Figure 4 to highlight the correlation between the attacker's tampering success rate and the block gap a, and the likelihood r of the attack node obtaining the next block billing right.

As seen in Figure 4, the block gap has an exponentially decreasing effect on the attacker's tampering success rate. Concurrently, it is discovered that while the block gap is constant, the attacker's forging capability (the increase in computing power) generates pseudo-power for the block. If an attacker controls more than half of the network's computing power, they may recalculate the verified blocks or prevent other nodes from producing new blocks, thereby realizing a double payment and blocking the confirmation of the transaction. The node's private key may be safeguarded through a method of secret sharing, which prevents the key from falling into the wrong hands. The node private key is split into n shares, each of which is kept secret by one of the participants; the private key can

be rebuilt only with the cooperation of participants. Each participant in the secret sharing process identifies its private key share with its own identity and utilizes its private key as the secret share, allowing for simultaneous secret distribution without any pre-processing. Every participant may check whether the share given by another participant is legitimate during private key reconstruction, eliminating the requirement for an actual secret share and allowing for faster processing times without compromising security.

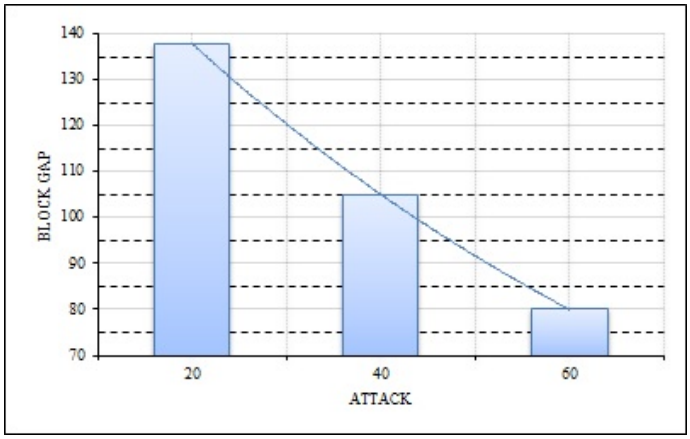

Figure 4. Tampering success rate.

Table 4 provides the request timings for digital signatures under various (u, n) combinations to demonstrate the computational cost of the aforementioned approach. The time it takes to request a private key from a secret distributor grows dramatically with a given threshold value u, and the time it takes to calculate the number of secret distributors, n, is dependent on the given threshold value u. Hence, choose the proper threshold in light of the various energy Internet applications' demands, as well as the security and operational efficiency prerequisites. The following precautions may be taken to further safeguard each user's privacy: Initially, the certifying organization plays the role of a proxy in the transaction, protecting the subject's anonymity and sensitive data from disclosure. The second is to restrict the transmission of transaction data between selected nodes and to restrict the broadcast range of transaction data. The third step is to establish the relevant access authority control mechanism to regulate the input and output of data. Fourth, one goal of technologies like ring signatures, homomorphic encryption, and zero-knowledge proof is to seal off private information from prying eyes. When the BCT protocol requires updating, certain nodes may not be able to receive new versions, or may not obtain new versions in time. This leads to hard forks and soft forks since various nodes are running different versions of the protocol. When a node running the updated protocol verifies the validity of a block, we say that the protocol has hard forked. The node still using the older protocol rejects it, causing a permanent split; the soft fork is the more stringent of the two verification procedures, thus it does not upgrade the protocol. As a result, the outdated node actively changes the protocol, and in the best-case scenario, only temporary blocks or transactions are created. This is because the block that passes the verification of the node running the updated protocol may also be accepted by the outdated node.

Table 4. Signature request time comparison.

Request Time	u = 2	t = 6
n = 6	255.2	285.15
n = 8	265.2	321.14
n = 10	268.14	354.3
n = 12	269.25	474.2
n = 14	269.14	595.2

4. Proposed BCT-Inspired Approach

Figure 5 shows the proposed technique of BCT-based data protection. BCT consensus techniques are presented to address the distributed system consistency issue. These methods, however, are computationally expensive and resource-heavy, making them inappropriate for low-power, high-performance IoT. As a result, advancements have been made to the Practical Byzantine Fault Tolerance (PBFT) algorithm. As long as $g = (n - 1)/3$ faulty nodes are involved in the consensus computation, the new technique guarantees the system will continue to function normally. Each round of consensus in the new approach is assigned a unique data set number, denoted by y, beginning with 0. Each round of consensus also assigns a unique speaker node serial number, $q = (g - u) \bmod n$ (where g is the block height). It will be aggregated and added until a consensus is established if this cannot be done. u is the agreed-upon time frame. A new consensus round is initiated whenever a new block is created, and u is incremented by one each time.

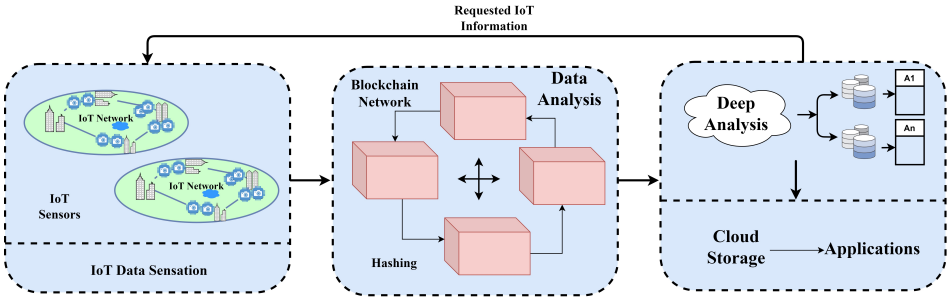

Figure 5. Proposed technique of BCT-based Data Protection.

4.1. Enhancing Consensus Algorithm

Being a decentralized, immutable, traceable, and efficient means of bill production and trustworthy billing support for transaction payment activities and behavior records across various nodes of the IoT, the trade BCT is a key component. The system can account in two ways (the procedure is shown in Table 5), either by exchanging the competition for multi-dimensional information like computing power and reputation for billing rights, or by introducing tokens or various types of digital currency with the effect of legal currency as a medium for value exchange. The strategy promotes the intelligent node's intrinsic growth, or "the capacity to perform more work." To ensure that every node in the network gets a chance to save a copy of the bill, it is necessary to broadcast transaction data for both billing systems to the whole system. IoT nodes may function as either a CSC or a CSP. There are two main issues with BCT technology: the use of public ledgers to record transactions poses a potential privacy breach, and the generation of a block in the BCT technology and waiting for the least number of blocks to confirm the payment is valid, which brings about the problem of long transaction time. The IP address and transaction topology on the BCT may provide information about a user's identity, but an attacker cannot determine the user's true identity with just the public key account. To reduce transaction confirmation times while simultaneously increasing system security and to set up a coin center with a trusted public key address as the real payment, this research provides an enhanced technique based on a partial blind signature process that uses cloud service. A one-time public key address and a blind signature method are used to record transactions with increased secrecy. The creator of a tag must be acknowledged as part of the tag's authority before the two tags may engage in any kind of interaction. Submit an authorization request to the organization, and after it receives the reader's request, the company will evaluate its trustworthiness based on the following criteria:

$$t(Q_{nq}) = \alpha t(Q_{adv}, \beta) + (1 - \alpha) t_f(\alpha_{pay})$$

After the cluster gateway is selected, the remaining mn nodes will be combined into one central location. This is a diagram illustrating how network latency and computational cost are linked to the distance from node 1 to gateway q.

$$Q_{adv} = t_f + \alpha Q_{mq}$$

where α is the pre-existing commitments of each transaction. Typically, node 1 will connect to the gateway P that has the least PAP. As a first step, it takes in all data on the autonomous clusters that are currently accessible. Assuming that node l belongs to an independent cluster B consisting of n nodes, with a delay of Q arriving at l of M_{ln} and the ability to process a message of length J being Q_m, node J may determine:

$$Q_{mq} = M_{jl} + M_{\lambda q} + Q_{mq}$$

The specific procedure is described in Figure 6.

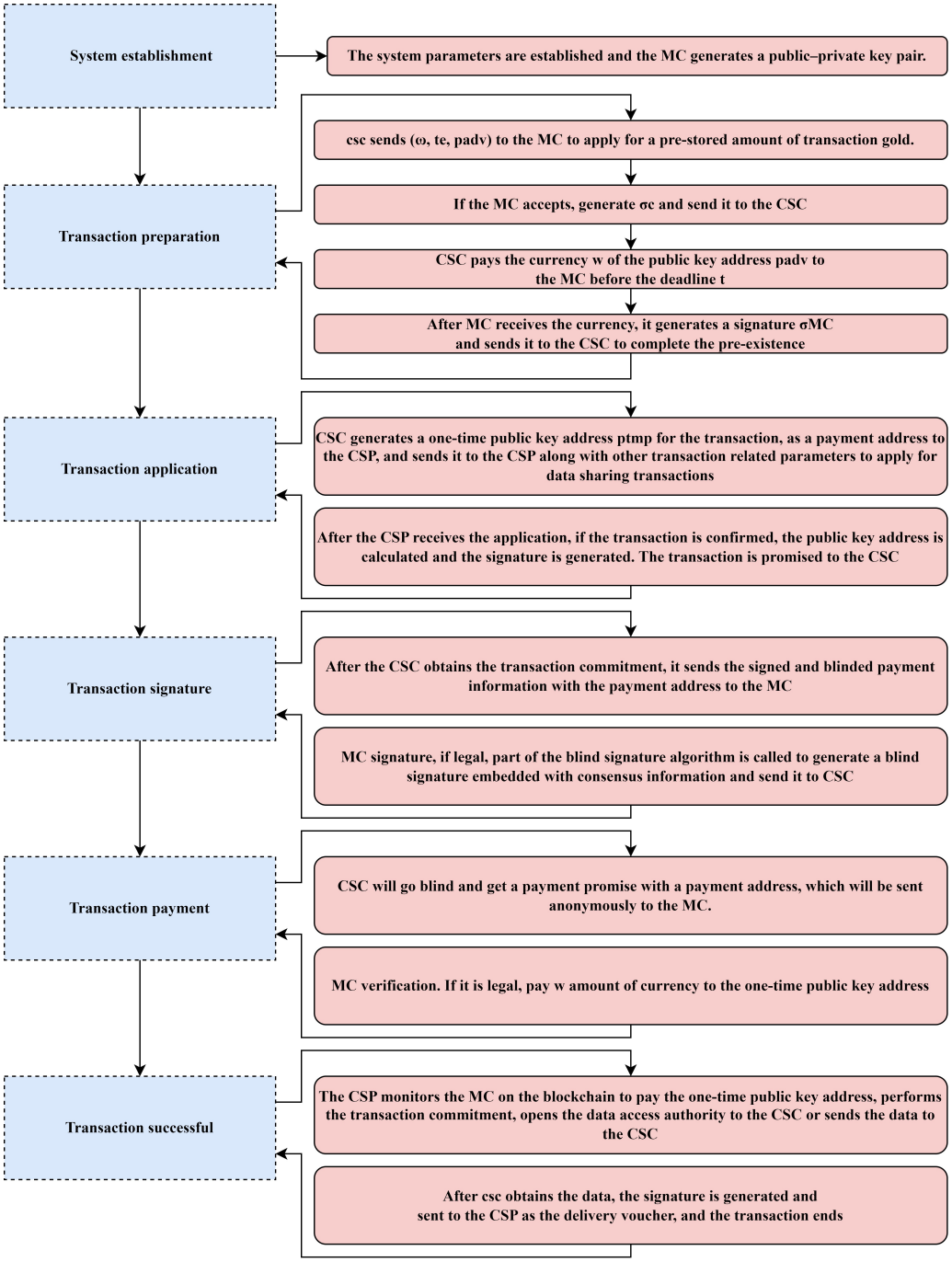

Figure 6. Specific steps of the proposed technique.

Table 5. Security technique to enhance consensus mechanism.

Step 1 : Initalize R = 0
Step 2 : If the Number of existing nodes is greater than 4,
Calculate speaker node p
Step 3 : If R = P, Then Accept the proposal,
Broadcast verified feedback message
Receive the correct number of feedback messages
Step 4: Else Verify Proposal,
Apply for change collection with Number of nodes applied to change set

4.2. Formulating Data Protection Technique

Encryption techniques, consensus processes, use scenarios, implementations, and systems play a role in BCT-IoT security. It is recommended to use a "structure + ontology + management" approach to address the many BCT-specific security issues that arise, including sub-domain protection, data security, application security, key security, security audit and early warning, and an emergency mechanism. To successfully respond to the development demands of future BCT-IoT information security sharing, the 7-dimensional protection system must simultaneously traverse the whole life cycle of the BCT IoT information system. The BCT system employs a mathematical technique for establishing trust and access rights between various nodes in the consensus mechanism of the BCT IoT information-sharing security protection system. BCT's fundamental determinants include encryption methods, consensus mechanisms, use cases, and information-sharing security protection system implementation and system.

1. *Stability of the structure:* When considering the significance of BCT bearer services, the breadth of subsystems, the level of openness of information systems, and the security of subsystems after the implementation of BCT technology in the future of the IoT, one can look at the experience of network security protection in the power industry. Firewalls and other access control devices at each communication border and fortified BCTs via virtual private networks are two ways to safeguard hosts and network devices in the BCT IoT system.
2. *Protection of Ontologies:* Before sending out transaction data to the whole network, the trading node in the BCT should evaluate its importance and security. The desensitization algorithm library should be developed in a targeted manner to anonymize transaction data between nodes, and a risk model of user privacy data leakage risk should be constructed to subjectively and quantitatively evaluate the threat of data leaking. The approval system for privacy data is combined with BCT's user authentication system, a rights management system, and a rights management system with varying degrees of protection of privacy data to actualize the data access mechanism based on the approval system. The upper-layer applications of a BCT IoT are not guaranteed to be secure by the security of the BCT IoT itself. Existing attack techniques for application systems are complex and often rely on exploiting pre-existing vulnerabilities or malicious code in the source code, weak authentication, and data transport in plaintext. To catch malicious code before it can cause any harm, it's best to use data mining and machine learning techniques, build malicious code feature extraction methods that take advantage of multi-dimensional features like the PE file header and the machine code byte sequence, and combine these with effective feature selection methods before putting the application system online. Furthermore, classifiers, which speed up the discovery of previously undiscovered dangerous code and boost its detection accuracy and generalizability. To actively investigate and patch the current flaws and prevent security risks, pre-built vulnerability mining is performed before the BCT IoT is launched using a variety of vulnerability mining methods such as fuzzing, binary comparison, static analysis, and dynamic analysis. Hackers may easily take control of a user's data or assets if they steal the user's private key, which is a security problem in the BCT IoT due to the storing and transfer of

keys. Private key replacement and management mechanisms are not included in the BCT, despite its centrality-eliminating design. Users may safeguard their private keys by using either a secret-sharing-based private key protection method or a hardware storage strategy based on physical security.

3. *Safety in Management:* All devices and systems on the BCT should be included in the audit, as should the reading and writing of data as well as any anomalous use of system resources. Consequently, multi-source logs, correlation analysis, fusion analysis, and situational factor analysis of multi-source logs are used to evaluate the networked network security status, and abnormal events and overall security postures in the system are sensed in time to make early warning and risk control measures. These are achieved through the application of data fusion and smart analysis techniques for network security. The BCT-IoT application scenarios need to be clarified to effectively avoid, promptly control, and mitigate the risks and repercussions of different forms of unexpected network security events including cyber attacks and malicious code infections. Take part in frequent emergency exercises, investigate the cause of network security issues and system vulnerabilities, fortify defenses, and forestall new attacks; these are different responsibilities as a network participant.

5. Experimental Results and Discussions

This section presents the experimental simulation of the proposed model. For the dataset, the online UCI repository is assessed. More than 12K instances were acquired for the bot data set. For simulation purposes, an i7 computing system with 16GB RAM and 2TB SSD was used. Data were cleaned and pre-processed using conventional techniques before experimental simulation. For experimentation, three phases were used. In the first phase, the proposed model assessed attack resistance against security attacks. In the second phase, BCT effectiveness is computed for the proposed model. Additionally, parameters of delay, data rate, and efficiency were used for overall performance assessment. In the final phase, the reliability and stability of the proposed model are analyzed for comprehensive performance assessment.

5.1. Defense against Attack

In this section, the security of the proposed BCT-based security architecture is assessed for IoT data exchange. Figure 7 details the distinct attacks on the IoT/BCT for risk assessment. The current study incorporats sufficient attack types that can lead to vulnerability in IoT security. Moreover, the completeness of the list can be justified in a manner that the included attacks vary from IoT node level to the storage level. Therefore, the proposed technique can compressively secure data in the IoT network. The effectiveness of the framework's defenses against different threats is defined by analytical criteria. It can be seen from Figure 7 that the framework is very secure against five attacks, very secure against three, and somewhat secure against one. The reasoning behind the analysis is that it is impossible to tell an attacking node apart from a normal node if it follows the process of registering the network and assigning public and private keys. This is the case unless the attacking node has additional attack behavior and the normal node has access to the private chain. There will be far less of a chance of it happening. This study lays the groundwork for the IoT by allowing nodes to communicate their feedback histories via various private chains (Private Block, chain, PrBCT).

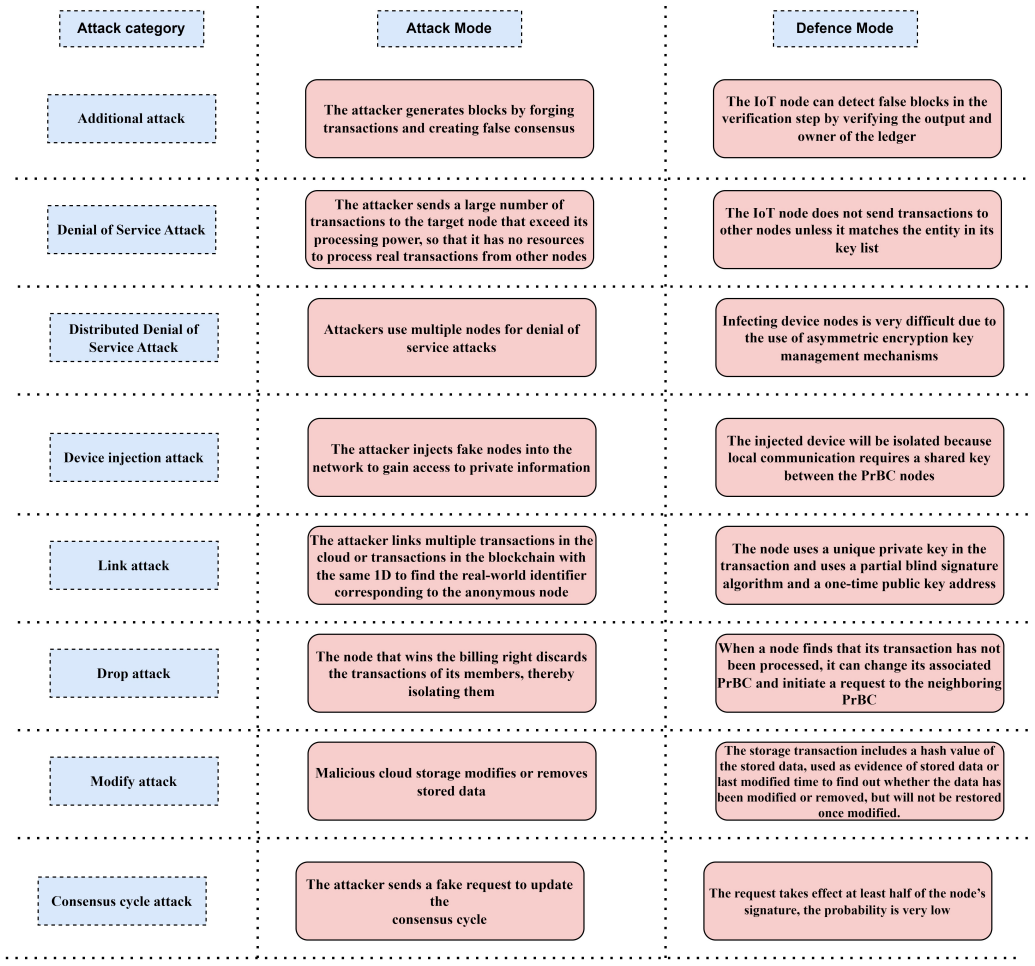

Figure 7. IoT/BCT attack analysis and response mechanism.

5.2. The Efficiency of Data BCTs

In this section, the data BCT's validity and practicability are tested by measuring its throughput and latency. The data BCT simulation system's experimental design may be broken down into two main parts: the data-generating module and the consensus module. The consensus module is tested for its log determination time and transaction throughput by a request sent from the data production module during a data-generating simulation. Matlab is the programming language behind the simulation system, which models data production on a single computer with 10 consensus procedures. The system environment consists of an Intel Core i7 Processor, 16GB of RAM, the Windows 11 operating system, and JDK 2.0. Constant requests from the data generator module are sent to the consensus module, which then runs the enhanced PBFT algorithm during the simulation experiment. After the agreement, the information is added to a new block and stored in the distributed ledger.

5.2.1. Transmission Rate

Data BCT transaction throughput is the number of data uploads, data digest requests, and data ledger writes per unit of time that a node processes. Tests were run for durations of 15 s, 25 s, 45 s, 65 s, and 95 s, with the average rate for each duration. The results demonstrate that the data BCT processes around 10,500 times/s of transaction volume.

5.2.2. Delay

Data BCT latency is the time it takes for a request to be broadcast, executed by the consensus algorithm, and acknowledged by the network before an account can be

considered confirmed. The average of all delays is calculated based on the last six blocks' worth of generation time, and the average correlation between book delays and block generation times is shown in Figure 8. The longer it takes to produce a block, the more time passes until it may be used. The study is based on the observation that when the block's generation time rises, the overall delay rises as well since more requests are received during that time, the broadcast and verification time is longer, and the block validated by the broadcast is bigger. The TPS block generation time delay, as seen in the throughput graph, is in milliseconds, which is acceptable for most IoT use cases.

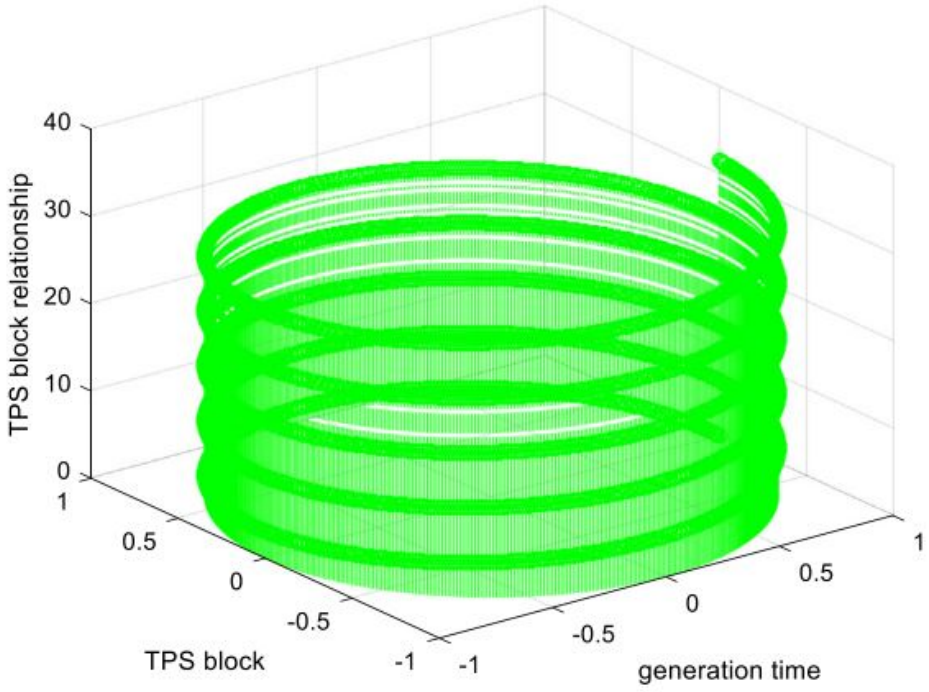

Figure 8. TPS block generation time.

5.2.3. BCT Trading Efficiency

BCT trading's primary time sinks are the creation of trades, signing of calculations, and confirmation of receipt. Confirmation of reception time is connected to the complexity of the smart contract involved in the supervision, while transaction creation time is an aggregate of initialization, message initiation and confirmation time, and the network communication state of the IoT. To reduce the overhead of signature calculations and speed up the ledger's processing time, this study employs a concise signature method that is simple to implement. The threshold short signature technique is used to simulate subscription delays and block creation times. There are 400 iterations and 150 bits in the signature. Parameter creation takes an average of 1.254 ms while signing takes about 4.487 ms. Compared to the Bitcoin method, which takes around 1.1 h to confirm the time, the transaction BCT formed under the proposed approach is more efficient. After confirming that it is possible to build a short path in an HS network under ideal circumstances, we investigate several aspects that impact the routing path and time overhead of the group route in the real world, as shown in Figure 9. Network and group topology are two major kinds of characteristics that significantly affect routing costs and success rates.

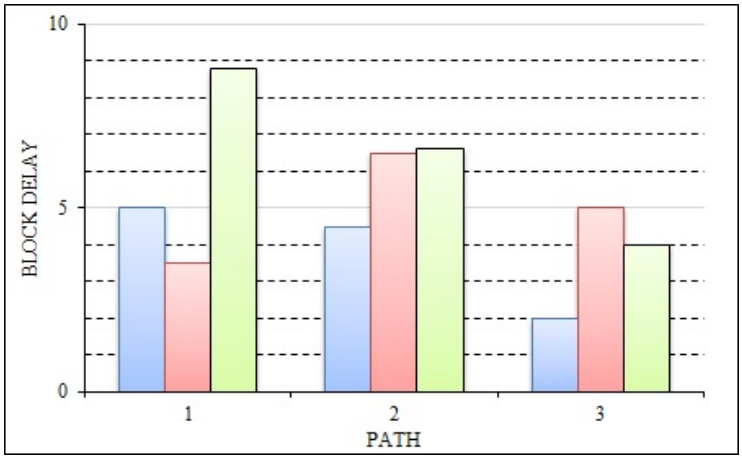

Figure 9. Log delay; (PATH indicate heterogeneous paths of the IoT network randomly chosen for data transmission. Block Delay is computed in seconds).

By examining these variables, we can assess how well the cluster-based routing algorithm performs and determine what values to use for various parameters in real-world applications. First, the node density, the motion node ratio, and the node speed are the primary parameters influencing the topology of an ad hoc network. The effect of node variables on typical journey times and success rates is shown. The network's connection grows as the average node speed grows. However, when the speed rises, the network architecture changes fast, the likelihood of the node vanishing along the routing route grows, the routing time lengthens, and the success rate drops. The impact of nodes is comparable to the effect of the percentage of mobile nodes. The addition of mobile nodes may boost network performance. Therefore, if there are too many mobile nodes, the network architecture will evolve more rapidly than it otherwise would. From a different angle, however, route success rates are increased by a factor of 4.4 due to increased node connection. The density of the figure's nodes is most clearly seen along the vertical axis. Figure 10 depicts how, in a typical IoT setting, the BCT IoT information security shared route adapts to varying densities of connected devices in different scenarios with variable node density. The number of hops required to access the information decreases steadily as the number of nodes grows. The pace at which packets evolve into common pathways will accelerate. This is because the source node may be buffered in the routing table if the dist is quite short. Therefore, the data packet is not sent to the neighboring cluster. Sending the path to the routing database increases the route success rate thanks to the path's redundancy. The route success rate drops as the dist rise because the path is less reliable due to the unstable topology.

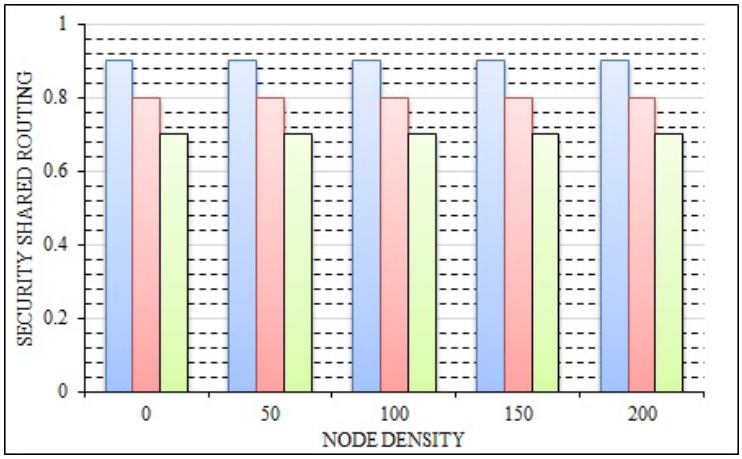

Figure 10. BCT IoT information security shared routing.

5.3. Reliability Efficiency

In addition to the aforementioned aspects, reliability is computed. Effectiveness requires the ability to make decisions. This necessitates evaluating how well reliability analysis is working going forward. It depicts the percentage of data attacks correctly detected by the proposed model as compared to the non-blockchain technique. The simulated results of the dependability evaluation may be shown in Figure 11. As more data sets are used in the experimental implementation of the offered model, higher efficiency values are recorded, nearing 93.67%. For extensive data sets, the proposed method seems to perform better.

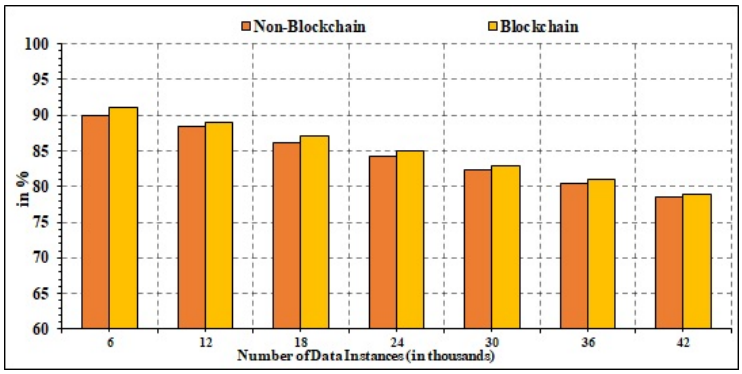

Figure 11. Reliability.

5.4. Stability Efficiency

Stability analysis is used to determine the durability of the proposed model over large data instances. In other words, the system's stability foretells general stabilization when it is deployed across large data sets for long-term assessment. Mean Absolute Shift is used to evaluate system stability. A MAS score of 0 indicates the least stable condition possible, and a MAS score of 1 indicates the most stable condition possible. The stability analysis of the proposed system is shown in Figure 12. It has been calculated that the proposed model has an overall range from 0.65 to 0.81, with an average of 0.62. The proposed method is robust and well-suited for detection.

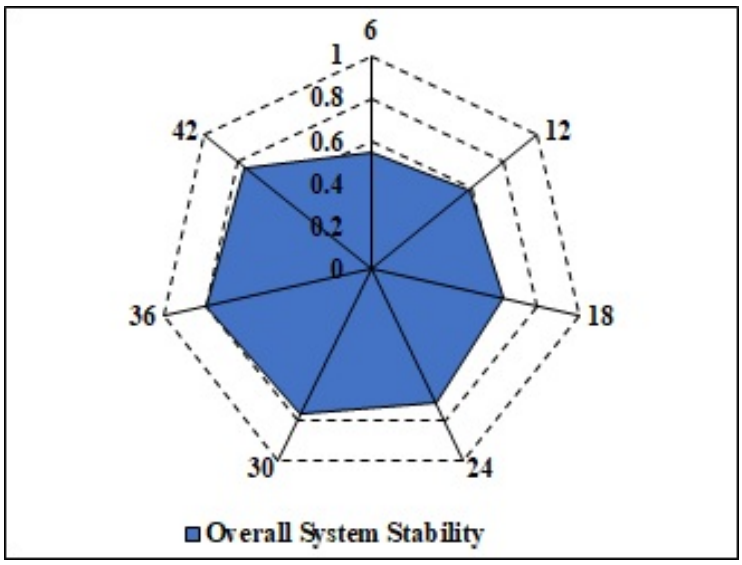

Figure 12. Stability.

5.5. Discussion

The presented methodology addressed several research challenges as compared to the conventional techniques. More than 90% efficiency is registered for the proposed model, which in comparison to the state-of-the-art techniques is better. This is because the proposed

model assesses the BCT technique of Data BCT and Transaction BCT within the IoT network, which is better than comparative techniques. Moreover, in terms of delay, the proposed model can determine attacks in less amount of time as compared to related techniques, which further enhances the effectiveness of the proposed model. Finally, elevated measures of reliability and stability further depict the efficacy of the proposed model.

6. Conclusions

Research on data decentralization is a major concern as no effective reliability assurance system is available for IoT information exchange. Henceforth, a lightweight security technique for exchanging information is proposed in the current work. Two BCT techniques are considered including Data BCT and Transaction BCT. Transaction BCT is a distributed ledger technology that is used to record and verify the exchange of information. In the current article, we focus on how BCT technology may be used to ensure the safety of data sent between IoT devices. Experimental simulations have been performed to validate the proposed model in terms of efficiency, delay, reliability and stability. For future work, we will next investigate ways to preserve the privacy of BCT data and process it with reduced delay. Additionally, future work on how BCT technology may be used to ensure the safety of data sent between IoT devices will be performed. Moreover, the blockchain-targeted attacks will be incorporated in the future work of the proposed technique.

Author Contributions: Conceptualization, A.A. and T.A.A.; Methodology, A.A. and T.A.A.; Formal analysis, A.A. and T.A.A.; Writing—original draft, T.A.A.; Writing—review & editing, T.A.A.; Supervision, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number IF2-PSAU-2023/01/23010.

Data Availability Statement: This article has no associated data.

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

References

1. Hasan, H.R.; Salah, K. Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts. *IEEE Access* **2018**, *6*, 65439–65448. [CrossRef]
2. Ajgaonkar, A.; Raghani, A.; Sheth, B.; Shukla, D.; Patel, D.; Shanbhag, S. A Blockchain Approach for Exchanging Machine Learning Solutions Over Smart Contracts. In Proceedings of the Science and Information Conference, Trier, Germany, 19–23 September 2022; Springer: Berlin, Germany, 2022; pp. 470–482.
3. Bommu, S.; Babburu, K.; Thalluri, L.N.; Gopalan, A.; Mallapati, P.; Guha, K.; Mohammad, H. Smart City IoT System Network Level Routing Analysis and Blockchain Security Based Implementation. *J. Electr. Eng. Technol.* **2023**, *18*, 1351–1368. [CrossRef]
4. Alshudukhi, K.; Khemakhem, M.; Eassa, F.; Jambi, K. An Interoperable Blockchain Security Frameworks Based on Microservices and Smart Contract in IoT Environment. *Electronics* **2023**, *12*, 776. [CrossRef]
5. Zhao, Y.; Li, Q.; Yi, W.; Xiong, H. Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain. *Agriculture* **2023**, *13*, 274. [CrossRef]
6. Sharadqh, A.; Hatamleh, H.; Alnaser, A.; Saloum, S.; Alawneh, T. Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-based Mitigation for Security Provisioning in Edge Assisted IoT Environment. *IEEE Access* **2023**, 11, 27433–27449. [CrossRef]
7. Kumar, S.; Vidhate, A. Issues and Future Trends in IoT Security using Blockchain: A Review. In Proceedings of the 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 5–7 January 2023; pp. 976–984. [CrossRef]
8. Abed, S.; Jaffal, R.; Mohd, B. A Review on Blockchain and IoT Integration from Energy, Security and Hardware Perspectives. *Wirel. Pers. Commun.* **2023**, 1–44. [CrossRef]
9. Lhore, H.; Bousselam, K.; Elissati, O.; Chami, M. Blockchain Technology as a Possible Solution to IoT Security Issues. *Int. J. Eng. Trends Technol.* **2023**, *71*, 152–163. [CrossRef]
10. Verma, R.; Dhanda, N.; Nagar, V. Analysing the Security Aspects of IoT using Blockchain and Cryptographic Algorithms. *Int. J. Recent Innov. Trends Comput. Commun.* **2023**, *11*, 13–22. [CrossRef]
11. Sureshkumar, T.; Sivaraj, R.; Vijayakumar, M. Design and implementation of a framework for blockchain based security using IoT. *J. Intell. Fuzzy Syst.* **2023**, *44*, 905–918. [CrossRef]

12. Prasanna Kumar, M.; Nalini, N. An Efficient Blockchain-Based Security Framework for PUF-Enabled IoT Devices in Smart Grid Infrastructure. *Lect. Notes Electr. Eng.* **2023**, *928*, 869–877. [CrossRef]
13. Ganesh Babu, R.; Yuvaraj, S.; Muthu Manjula, M.; Kaviyapriya, S.; Harini, R. Performance Analysis of Data Sharing Using Blockchain Technology in IoT Security Issues. *Lect. Notes Netw. Syst.* **2023**, *492*, 507–515. [CrossRef]
14. Pal, K. Security implications of IoT applications with cryptography and blockchain technology in healthcare digital twin design. In *Digital Twins and Healthcare: Trends, Techniques, and Challenges*; IGI Global: Hershey, PA, USA, 2022; pp. 229–252. [CrossRef]
15. Na, D.; Park, S. IoT-Chain and Monitoring-Chain Using Multilevel Blockchain for IoT Security. *Sensors* **2022**, *22*, 8271. [CrossRef] [PubMed]
16. Said, O. LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment. *Sensors* **2022**, *22*, 7948. [CrossRef] [PubMed]
17. Patan, R.; Manikandan, R.; Parameshwaran, R.; Perumal, S.; Daneshmand, M.; Gandomi, A. Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities. *IEEE Internet Things J.* **2022**, *9*, 19296–19306. [CrossRef]
18. Hewa, T.; Braeken, A.; Liyanage, M.; Ylianttila, M. Fog Computing and Blockchain-Based Security Service Architecture for 5G Industrial IoT-Enabled Cloud Manufacturing. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7174–7185. [CrossRef]
19. Qahtan, S.; Sharif, K.; Zaidan, A.; Alsattar, H.; Albahri, O.; Zaidan, B.; Zulzalil, H.; Osman, M.; Alamoodi, A.; Mohammed, R. Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6415–6423. [CrossRef]
20. Attkan, A.; Ranga, V. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex Intell. Syst.* **2022**, *8*, 3559–3591. [CrossRef]
21. Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2022**, *27*, 760–776. [CrossRef]
22. Janani, K.; Ramamoorthy, S. Defending IoT security infrastructure with the 6G network, and blockchain and intelligent learning models for the future research roadmap. In *Challenges and Risks Involved in Deploying 6G and NextGen Networks*; IGI Global: Hershey, PA, USA, 2022; pp. 177–203. [CrossRef]
23. Whig, P.; Velu, A.; Nadikattu, R. Blockchain platform to resolve security issues in IoT and smart networks. In *AI-Enabled Agile Internet of Things for Sustainable FinTech Ecosystems*; IGI Global: Hershey, PA, USA, 2022; pp. 46–65. [CrossRef]
24. Chen, B.; Liu, D.; Zhang, T. A Blockchain-Based Security Model for IoT Systems. *J. Inf. Knowl. Manag.* **2022**, *21*, 2250004. [CrossRef]
25. Liao, Z.; Pang, X.; Zhang, J.; Xiong, B.; Wang, J. Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1159–1175. [CrossRef]
26. Wang, C.; Tan, X.; Yao, C.; Gu, F.; Shi, F.; Cao, H. Trusted Blockchain-Driven IoT Security Consensus Mechanism. *Sustainability* **2022**, *14*, 5200. [CrossRef]
27. Xihua, Z.; Goyal, S. Security and Privacy Challenges using IoT-Blockchain Technology in a Smart City: Critical Analysis. *Int. J. Electr. Electron. Res.* **2022**, *10*, 190–195. [CrossRef]
28. Pratik, A.; Bhattacharjee, A.; Priyadarshini, R.; Divakar, S. An IoT and blockchain-based system for acute security check and analysis. In *The Role of IoT and Blockchain: Techniques and Applications*; CRC Press: Boca Raton, FL, USA, 2022; pp. 285–294.
29. Yu, Z.; Song, L.; Jiang, L.; Khold Sharafi, O. Systematic literature review on the security challenges of blockchain in IoT-based smart cities. *Kybernetes* **2022**, *51*, 323–347. [CrossRef]
30. Santra, S.; Sharma, S.; Deyasi, A. Enhanced Security and Privacy for IoT Based Locker System Operated at Low Frequency Spectrum Using Blockchain. *Commun. Comput. Inf. Sci.* **2022**, *1695*, 56–63. [CrossRef]
31. Rashid, M.; Choi, P.; Lee, S.H.; Kim, K.; Kwon, K.R. Utilizing Blockchain and Distributed Storage to Enhance Security and Privacy in the IoT Ecosystem. In Proceedings of the 2022 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Alamein New City, Egypt, 18–21 December 2022; pp. 160–165. [CrossRef]
32. Vikram, A.; Kumar, S.; Mohana. Blockchain Technology and its Impact on Future of Internet of Things (IoT) and Cyber Security. In Proceedings of the 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 1–3 December 2022; pp. 444–447. [CrossRef]
33. Alrubei, S.; Ball, E.; Rigelsford, J. Adding Hardware Security into IoT-Blockchain Platforms. In Proceedings of the 2022 IEEE Latin-American Conference on Communications (LATINCOM), Rio de Janeiro, Brazil, 30 November–2 December 2022 . [CrossRef]
34. Alzuabi, W.; Ismail, Y.; Elmedany, W. Privacy and Security Issues in Blockchain based IoT Systems: Challenges and Opportunities. In Proceedings of the 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, 20–21 November 2022; pp. 258–265. [CrossRef]
35. Parcha, A.; Mishra, S.; Bist, A.; Agarwal, R.; Gupta, S.; Sharma, S.; Sathyaraj, R. Implementing security in IoT systems via blockchain. *Int. J. Internet Technol. Secur. Trans.* **2022**, *13*, 85–104. [CrossRef]
36. Velayudham, P.; Nagaraju, V.; Masi, S.; Chandrasekaran, S.; Kulandaivel, R.; Ramachandran, M. Blockchain-Based Internet of Things (IoT) Security for Data Sharing in Smart City Environment. In *The Convergence of Artificial Intelligence and Blockchain Technologies*; World Scientific: Singapore, 2022; pp. 221–241. [CrossRef]
37. Sille, R.; Mahdi, H.; Choudhury, T.; Sahoo, S.; Kapoor, A.; Nanda, I.; Sharma, A. Review Study on Blockchain Frameworks for Security Issues in IoT Devices. In Proceedings of the 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 20–22 October 2022; pp. 876–881. [CrossRef]

38. Cabrera-Gutierrez, A.; Castillo, E.; Escobar-Molero, A.; Alvarez-Bermejo, J.; Morales, D.; Parrilla, L. Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks. *IEEE Access* **2022**, *10*, 114331–114345. [CrossRef]
39. Mathur, A.; Prakash, S. Review of Security Enhancement in IoT using Blockchain. In Proceedings of the 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 17–19 June 2022; pp. 396–402. [CrossRef]
40. Kumaresan, M.; Gopal, R.; Mathivanan, M.; Poongodi, T. Amalgamation of blockchain, IoT, and 5G to improve security and privacy of smart healthcare systems. In *Blockchain Applications for Healthcare Informatics*; Academic Press: Cambridge, MA, USA, 2022; pp. 283–312. [CrossRef]
41. Jain, N.; Wahid, N.; Al-Farhani, L.; Manideep, A.; Bhardwaj, V.; Sangeeth Kumar, M. A Blockchain Approach to IoT Security and Reliability Analysis. In Proceedings of the 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 27–29 April 2022; pp. 758–763. [CrossRef]
42. Samanta, S.; Sarkar, A.; Sharma, A.; Geman, O. Security and Challenges for Blockchain Integrated Fog-Enabled IoT Applications. *Lect. Notes Netw. Syst.* **2022**, *427*, 13–24. [CrossRef]
43. Chowdhury, N.; Alam, K.; Islam, M. Security and Privacy in IoT using Blockchain and Lightweight Cryptographic Protocol. In Proceedings of the 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2022. [CrossRef]
44. Bai, X.; Tu, S.; Waqas, M.; Wu, A.; Zhang, Y.; Yang, Y. Blockchain Enable IoT Using Deep Reinforcement Learning: A Novel Architecture to Ensure Security of Data Sharing and Storage. *Lect. Notes Comput. Sci.* **2022**, *13340*, 586–597. [CrossRef]
45. Psathas, A.; Iliadis, L.; Papaleonidas, A.; Bountas, D. An IoT Authentication Framework for Urban Infrastructure Security Using Blockchain and Deep Learning. *Commun. Comput. Inf. Sci.* **2022**, *1600*, 284–296. [CrossRef]
46. Maiti, M.; Barman, S.; Bhagat, D. LIVECHAIN: Lightweight Blockchain for IOT Devices and It's Security. *Lect. Notes Netw. Syst.* **2022**, *481*, 265–275. [CrossRef]
47. Ali, M.; Dhanaraj, R.; Sharma, V.; Balamurugan, B. IoT and Blockchain based Smart Agriculture Monitoring and Intelligence Security System. In Proceedings of the 2022 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 15–17 November 2022. [CrossRef]
48. Chen, Y.; Li, M.; Zhu, X.; Fang, K.; Ren, Q.; Guo, T.; Chen, X.; Li, C.; Zou, Z.; Deng, Y. An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain. *Inf. Process. Manag.* **2022**, *59*, 102884. [CrossRef]
49. Xu, X.; Zhu, D.; Yang, X.; Wang, S.; Qi, L.; Dou, W. Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain. *ACM Trans. Internet Technol.* **2021**, *21*, 1–17. [CrossRef]
50. Alfandi, O.; Otoum, S.; Jararweh, Y. Blockchain solution for iot-based critical infrastructures: Byzantine fault tolerance. In Proceedings of the NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 20–24 April 2020; pp. 1–4.
51. Li, W.; Feng, C.; Zhang, L.; Xu, H.; Cao, B.; Imran, M.A. A scalable multi-layer PBFT consensus for blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2020**, *32*, 1146–1160. [CrossRef]
52. Feng, L.; Zhang, H.; Chen, Y.; Lou, L. Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain. *Appl. Sci.* **2018**, *8*, 1919. [CrossRef]
53. Kumar, U.; Akancha; Nancy; Pathak, N. Security Amplification of IoT: Blockchain. *Lect. Notes Netw. Syst.* **2022**, *392*, 273–287. [CrossRef]
54. Fasila, K.; Mathew, S. Fast and Efficient Security Scheme for Blockchain-Based IoT Networks. *Comput. Mater. Contin.* **2022**, *73*, 2097–2114. [CrossRef]