buildings

MDPI

Article

A Classification-Based Blockchain Architecture for Smart Home with Hierarchical PoW Mechanism

Weilu Lv [1,2,†], Ning Wang [3,*,†], Xianwang Xie [4] and Zhen Hong [5,*]

[1] School of Art and Archaeology, Zhejiang University City College, Hangzhou 310015, China
[2] School of Architecture, Tsinghua University, Beijing 100084, China
[3] School of Spatial Planning and Design, Zhejiang University City College, Hangzhou 310015, China
[4] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 101408, China
[5] Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou 310023, China
* Correspondence: wangning@zucc.edu.cn (N.W.); zhong1983@zjut.edu.cn (Z.H.)
† These authors contributed equally to this work.

Abstract: Smart home, as a typical Internet of Things (IoT) application, provides people with a variety of conveniences. Unfortunately, it may suffer from security and privacy issues. Currently, blockchain theory is considered as one of the potential solutions to the IoT security problem. However, according to the rules of blockchain, it requires large storage to store distributed ledgers and undertakes long latency caused by proof of work (PoW), which cannot be performed by resource-constrained IoT devices. To address the issue, we propose a classification-based blockchain architecture with a hierarchical PoW mechanism, which can reduce the storage consumption and decrease the latency. In our architecture, we divide IoT devices into several child nodes by data classification and convert the data storage into partial network storage. Furthermore, we try to set the moderate-cost security grades (SG) to adjust the difficulty of PoW for reduction of latency. Finally, comparing the performance of our scheme with the traditional method and current technology, the proposed architecture not only takes up less storage (i.e., almost 90% reduction) but also increases efficiency (i.e., almost 50% running time saving) while ensuring safety.

Keywords: smart home; secure architecture; blockchain; storage efficiency; IoT

Citation: Lv, W.; Wang, N.; Xie, X.; Hong, Z. A Classification-Based Blockchain Architecture for Smart Home with Hierarchical PoW Mechanism. *Buildings* **2022**, *12*, 1321. https://doi.org/10.3390/buildings12091321

Academic Editors: Liyin Shen, Jorge Ochoa and Haijun Bao

Received: 30 June 2022
Accepted: 24 August 2022
Published: 29 August 2022

1. Introduction

The smart city refers to the use of various information technologies or innovative ideas to build and optimize the urban management framework [1,2]. It usually integrates the systems and services of the city to improve the efficiency of resource utilization and the quality of citizens' lives. In a sense, a smart city is the product of the rapid development of information technology, the high-quality and sustainable development of modern cities. As an important part of the smart city, the smart home, which is one of the applications filed on the Internet of Things (IoT), has brought a new modern concept of people living in recent years [3–5]. It integrates with a series of digital techniques that influence the daily life of individuals [6]. As millions of devices are continuously being linked to the IoT networks, how to keep IoT systems secure and avoid various kinds of malicious attacks is an open issue and a matter of great concern [7–9]. Currently, a highly centralized security framework is widely used for IoT due to its easy control. However, it is incompletely suitable for IoT since a single central control node may be vulnerable by attackers [10].

One effective solution to protect the IoT network is to employ blockchain technology [11–16]. Usually, blockchain is an open distributed digital ledger that maintains a growing list of blocks one after another within a chain. Each block is added to the ledger after mining, which is verified by the participating nodes. To mine a block, some specific nodes called miners try to solve a time-consuming cryptographic problem known as proof of work (PoW) [17]. This is how blockchain eliminates the need for trusted third parties

through the distributed record preservation and verification system. Currently, blockchain-based technology is widely used in various fields, such as smart education [18], smart healthcare [19], smart home [12], etc.

Recently, there has been much research regarding secure IoT systems [20–23]. Dorri et al. [24] propose a blockchain-based architecture for IoT devices that supports security and privacy. However, it is not fully built on a distributed architecture due to the use of a central cloud storage. Furthermore, they try to reduce the latency by removing the PoW consensus mechanism, but cannot prove whether it would withstand attacks performed by compromised nodes [25]. Similarly, to eliminate the PoW mechanism, a blockchain-enabled architecture of software-defined networking (SDN) controllers using a cluster structure with a new routing protocol is proposed for resource-constrained IoT device scenarios [26]. It actually uses public and private blockchains for peer to peer (P2P) communication between IoT devices and SDN controllers. In order to improve the architecture (or features, e.g., structure, verification, storage) of the original blockchain, as shown in Table 1, Qu et al. [27] propose a hypergraph-based blockchain model to reduce data storage, but cannot deal with the long latency caused by PoW. Mohanty et al. [28] develop an integrated blockchain model that includes a lightweight consensus algorithm, certificateless cryptography, and distributed throughput management scheme. It generates an overlay network to assign higher resources to a public blockchain to guarantee the dedicated security and privacy. But this scheme seems a bit complex for smart home scenarios. We can see the existing blockchain-based architecture for smart home devices face the challenge of imbalanced security and efficiency [29]. It exposes the traditional highly centralized architecture to huge security risks and vulnerabilities. Therefore, it is necessary to design a decentralized, safe, and efficient blockchain-based smart home architecture for human living.

Table 1. Comparison of blockchain models.

Features	Description	
	Original Blockchain	**Hypergraph-Based Blockchain**
Structure	One chain	Several subchains
Verification	By node itself	By other nodes
Storage	One node one copy	Partial nodes have a copy
Miners' function	PoW	PoW and linear independence matrix

In this paper, we propose a classification-based blockchain architecture for smart homes with a hierarchy-based PoW mechanism. In our architecture, we focus on reducing storage for IoT devices while decreasing the latency caused by PoW in the condition of acceptable security risks. The major contributions of this paper can be summarized as follows.

- To replace the high-risk centralized frameworks, we propose a classification-based blockchain architecture for smart homes that stores data in a fully decentralized way. In the architecture, we divide IoT devices into several child nodes by data classification and convert the data storage into the partial network storage. It not only helps decrease risks such as single point failure but also reduces almost 90% storage for resource-constrained IoT devices.
- We design a moderate-cost hierarchical PoW mechanism, i.e., set different security grades according to the security requirements, which can reduce the latency and the security risks to an acceptable level. By experimenting, the proposed architecture can help reduce running time by almost 50%.

The rest of this paper is organized as follows. Section 2 discusses the current problem associated with centralized blockchain-based architectures. In Section 3, we design and propose a new improved blockchain-based architecture that is a typically distributed mode. Furthermore, we propose a hierarchical PoW mechanism to balance the performance of security and computational complexity in Section 4. Experiments are conducted to further

analyze the proposed scheme on storage, security, and latency in Section 5. Finally, we conclude this paper in Section 6.

2. Problem Statement

In the traditional smart home, as shown in Figure 1, the architecture is so highly centralized that the key node (i.e., control center) is located at the center of the IoT network to control all the devices. However, it cannot always guarantee services availability because it is vulnerable to a single point of failure and malicious attacks such as Sybil and DDoS attacks [30]. Furthermore, the control center acts as the data switching station and the interactive information is prone to eavesdropping under the transmission process. In order to protect user privacy, we try to design a blockchain-based decentralized architecture for the smart home.

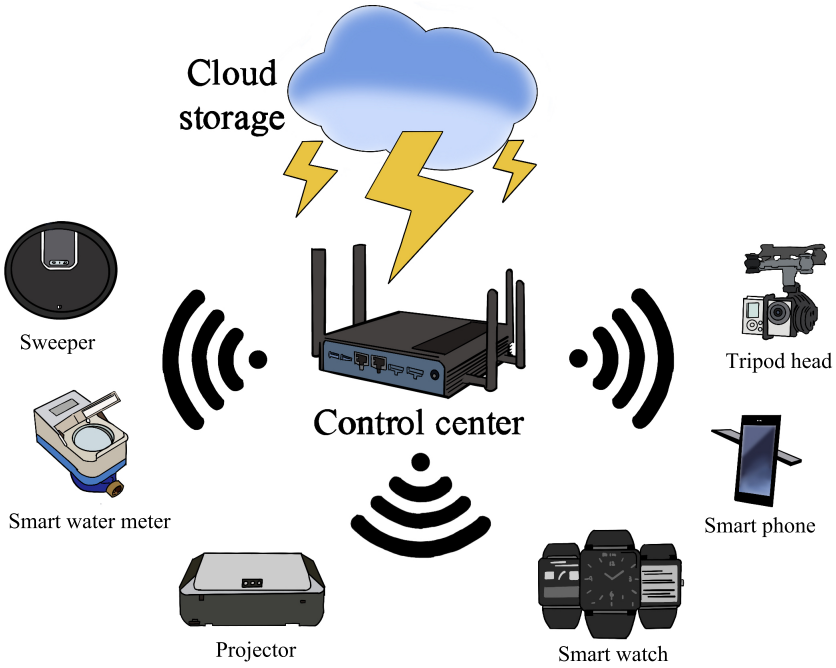

Figure 1. The traditional highly centralized smart home architecture.

The distributed ledger of the blockchain requires a full network accounting model. All nodes in the blockchain retain a ledger that contains all transaction data, and update it to maintain integrity if a new transaction is available. When a transaction occurs, all of the participant nodes would verify it during the mining process which may cause long latency according to the PoW mechanism. The higher the difficulty of the PoW mechanism, the more secure the transaction data, and the greater the latency. Once the transaction is verified and added to the blockchain, it will be stored in all nodes and cannot be tampered unless the attacker can simultaneously control more than 51% of the nodes in the system.

Consequently, it is not always necessary for all nodes to store all of the transaction records in the blockchain network. Actually, there is no need to set the same high level of security for all categories of transaction data. For one transaction record, it is enough to guarantee that it is stored by a sufficient number of nodes and it only needs to ensure that each kind of transaction is at an acceptable security level. When a new transaction occurs, only the associated nodes will verify and store the transaction record.

3. System Architecture

3.1. Architecture Overview

To address the above problem, we design an improved blockchain-based architecture. Firstly, we introduce the main objects within the architecture that are described as follows.

- **Node**: a device with storage in a blockchain. Each node contains several child nodes (CNs), and it belongs to at least one vertex set.
- **Miners**: are devices used to calculate encryption block hash keys in the blockchain.
- **Vertex set (VS)**: contains a number of CNs that are involved in different devices and store the same category of transaction data. Each VS maintains a sub-blockchain.

Figure 2 shows an example of the proposed blockchain-based architecture. In Figure 2, our blockchain network contains 7 devices ($Node_1$ to $Node_7$), 19 CNs (CN_1 to CN_{19}), 2 miners ($Miner_1$ and $Miner_2$), and 2 local networks (LN_1 and LN_2). Moreover,we classify CNs which record the same category of data to the same VS, and they are divided into five sets (VS_1 to VS_5) that are represented as connected blocks of the same color. Here, a device can be involved in two or more VSs at the same time. For example, $Node_4$ belongs to VS_1 and also belongs to VS_5. In addition, devices belonging to the same VSs may or may not be in the same local network.

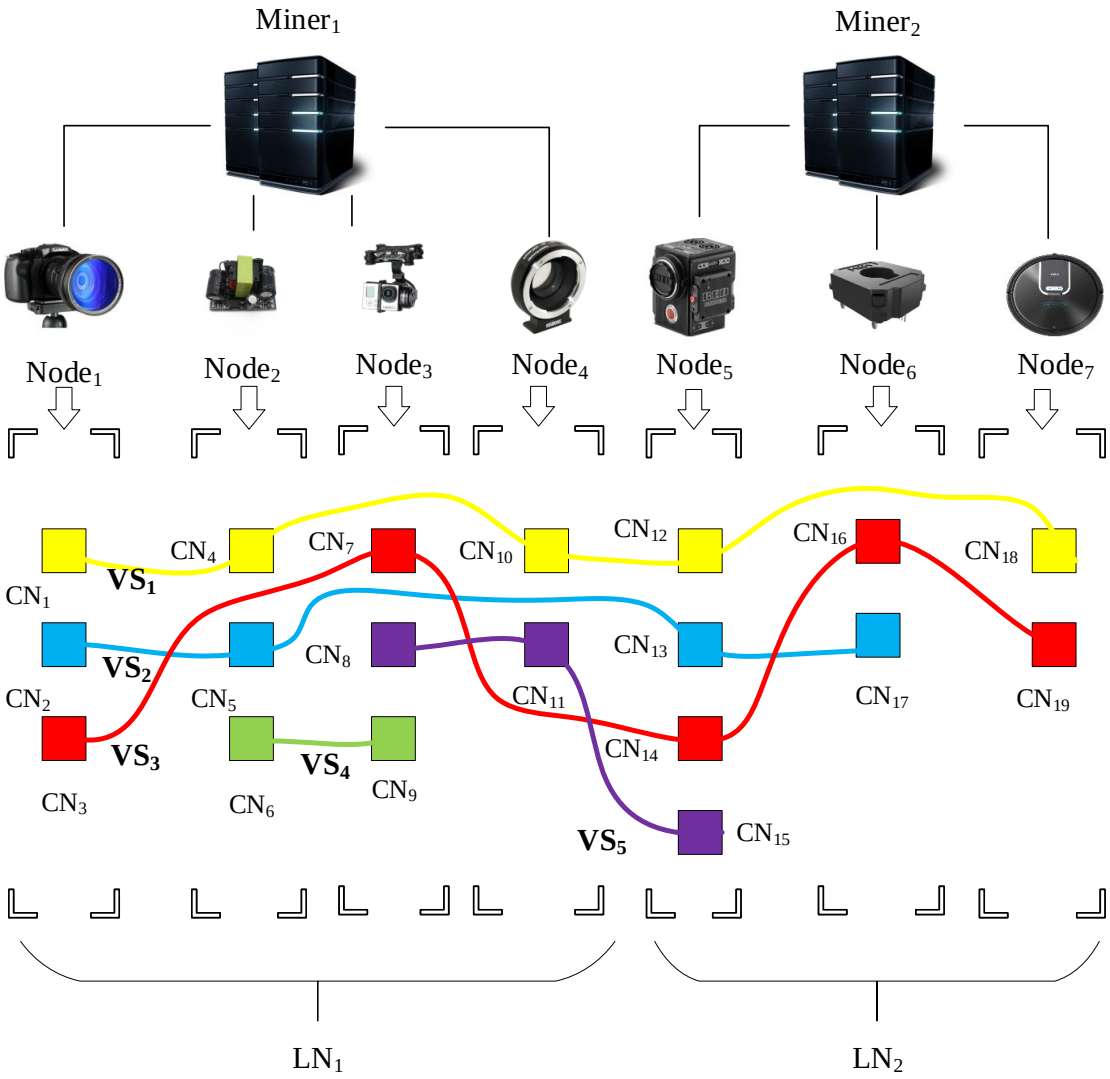

Figure 2. A classification-based blockchain decentralized architecture.

In the proposed architecture, a CN can only belong to one VS. The CNs in the same VS must be synchronized in the storage process. In order to balance the storage distribution and avoid the phenomenon that some CNs in the largest VS store too much data, we define the maximum and minimum size of a VS as $maxn$, $minn$, respectively, where $minn = maxn/4$.

3.2. The Data Structure of Nodes

Since a node in the blockchain must contain all transaction data related to the device, it involves the categories of transaction data generated from both itself and other devices. Meanwhile, the node must store the synchronized transaction data in different VSs. However, the original working mechanism of blockchain cannot reach the requirements due to its structure. Therefore, we designed a data structure for each node.

As shown in Figure 3, the storage structure designed for each node includes three parts: the blockchain-list, sub-blockchain, and relation vector. The blockchain-list involves several indexes of sub-blockchains that store synchronous transaction data related to the device, which means each VS maintains a sub-blockchain. Specifically, the total number of indexes is equal to the number of categories of data associated with the device in the whole blockchain. Each sub-blockchain is stored in the CNs of the device, and the data category between sub-blockchains are different from each other. The relation vector is a vector that records all the indexes of CNs related to this device, where r_k represents the indexes of CNs related to CN_k.

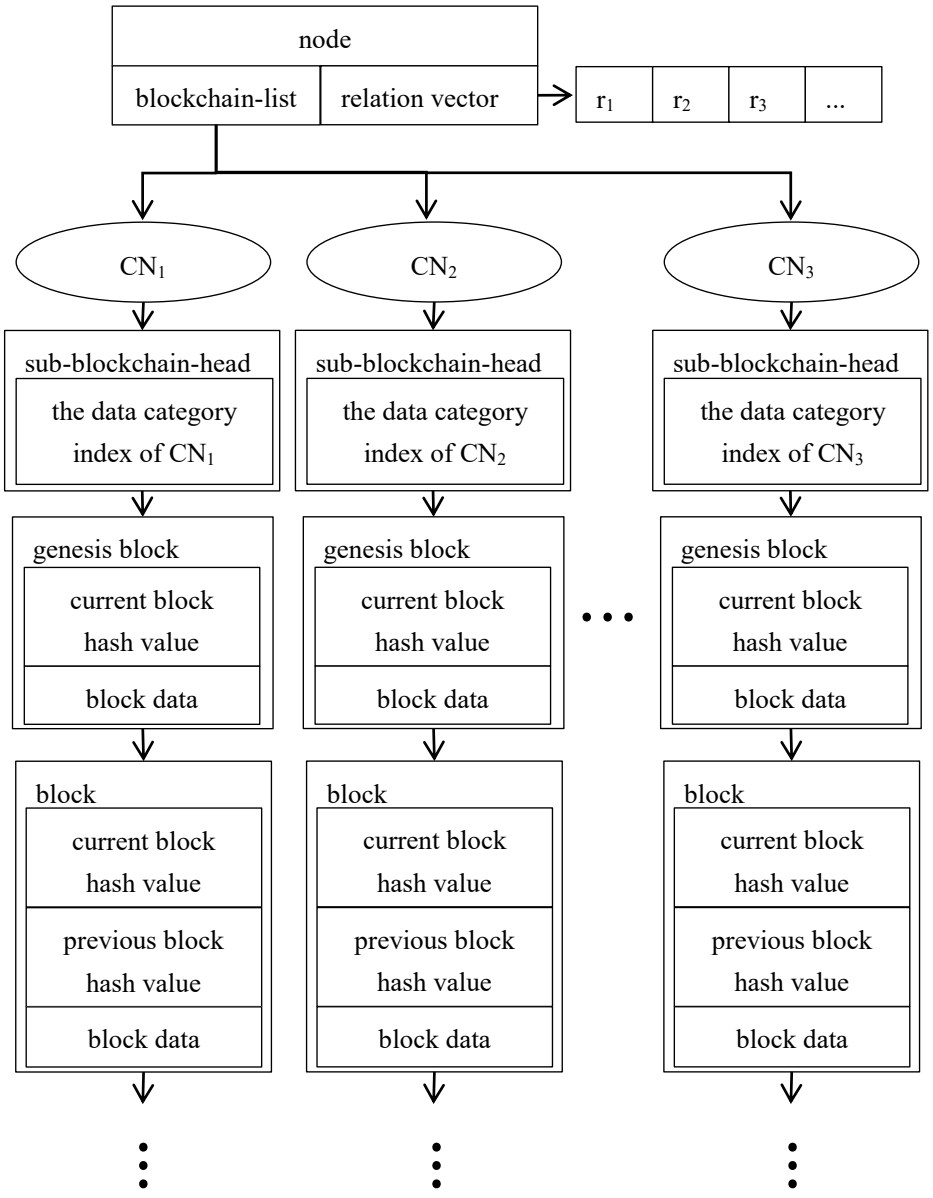

Figure 3. The data structure of nodes.

4. Hierarchical PoW Mechanism

As far as we know, PoW is the most widely used consensus algorithm in the blockchain which can effectively defend against various malicious attacks [17,22]. However, it is overloaded for power-constrained IoT devices. We cannot eliminate PoW since it may cause system vulnerabilities and threats. To address the above problem, we propose a moderate-cost hierarchical PoW mechanism for such power-constrained IoT devices to make the trade-off between efficiency and security.

In our architecture, we use small-scale private blockchain and each sub-blockchain only records the same category of data. According to the security requirements, we define that a data category has a security grade (SG), i.e., the SG of each data category must be positively related to its security requirement and cannot be much higher to make the IoT device overload. On the other hand, each CN also has the same security grade as a data category. The difficulty of PoW is self-adaptive according to the SG of each CN. The higher the SG, the longer it takes to run the PoW mechanism. Thus, this mechanism allows the CNs that store the data category with low-security requirements to consume fewer resources. However, letting the miners know the SG of the transaction data and run a PoW of corresponding difficulty when a transaction is released is a key problem.

We built a blockchain between miners to record the mapping of all the categories of data in the blockchain system to SGs that have been initialized. When a transaction occurs, the source CN constructs a record that includes information such as timestamp, the index of the category of transaction data, transaction content. The miners read the index from the constructed records and obtain the security grade through the mapping. Then, they run the PoW with corresponding difficulty for verification. If the transaction is verified to be legal, the record is added to the current block of the sub-blockchain with the same index of transaction data category.

When the current block in a sub-blockchain of a CN is full, according to the working principle of blockchain, the data in the current full block, the hash value of previous block and other information will be published to the whole sub-blockchain network. Miners receive this data and competitively calculate the cryptographic hash value. Once a miner settles down the puzzle, it will publish to the sub-blockchain for verification. If the verified result is acceptable, the block will be encrypted and stored, otherwise, it will be discarded and the above process will be repeated.

In addition to setting the security grade, the number of CNs in each VS must be sufficient to reach the security requirements. To avoid the construction of a VS with only a few CNs (e.g., some CNs are deleted from the blockchain), we designed a series of algorithms to manage the process of node joining (i.e., connect to network) and deletion (disconnection).

When a new node is connected to the network, each of its CNs is added to the VS that contains its other associated CNs and stores the same data category. If there is no VS associated with the new node in the network, its CNs will be randomly added to a VS in which the stored data category is the same as the corresponding CNs. On the other hand, if the number of CNs in a VS is greater than $maxn$, then the VS is split into two sets, one of which has a number of $minn$ CNs and the other is $(maxn\text{-}minn)$. Specifically, there is no association for CNs in these two VSs. Here we can assume that the number of interconnected devices is less than $minn$ since there are not many associated devices in the context of the smart home. The process for node addition is shown in Algorithm 1. In contrast, when a node is deleted from the network, i.e., disconnected from the network, it may cause the number of CNs in a VS to be less than $minn$. At this time, we merge this VS and the other VS whose number of child nodes does not exceed $(maxn\text{-}minn)$. The process of node deletion is given in Algorithm 2.

Algorithm 1 Node Addition

for each CN **in** $NewAddSet$ **do**
  $k \leftarrow$ index($NewAddSet$, CN)
  if $RelationVector[k] \neq$ null **then**
    $r_k \leftarrow RelationVector[k]$
  else
    $r_k \leftarrow random()$
  end if
  $j \leftarrow$ index(VS, r_k)
  $VS[j] \leftarrow VS[j] \cup CN$
  if size($VS[j]$) $> maxn$ **then**
    split $minn$ CNs in $VS[j]$ to a new VS
  end if
end for

Algorithm 2 Node Deletion

for each CN **in** deletedSet **do**
  $i \leftarrow$ index(VS, CN)
  $VS[i] \leftarrow VS[i] - CN$
  if size($VS[i]$) $< minn$ **then**
    select $VS[j]$ whose $size < (maxn - minn)$
    $VS[j] \leftarrow VS[i] \cup VS[j]$
  end if
end for

5. Performance Evaluations

To evaluate the proposed architecture, in this paper, one real smart home scenario ($maxn$ = 5, the number of categories is 100) is conducted for emulation and verification. Specifically, as shown in Figure 4, we designed a small testbed with the self-design IoT devices (nodes) to emulate the scenario of the smart home. In our testbed, we used PCs as miners and used Raspberry Pi Model 3B with 1 GB memory as a normal node which is integrated with various physical sensors.

Figure 4. The IoT device.

For a given N IoT nodes in the network, we try to calculate the average storage of each node and the running time of generating a certain amount of blocks. Furthermore, we try to find the relationship among the $maxn$ of VS, the average storage of each node, and the security. Here we define the safety factor for security evaluation as the maximum number of malicious CNs that the system can tolerate. In order to prove the advantage of our classification-based blockchain architecture, we compare with original blockchain

and hypergraph-based blockchain [27] on the performance of total used memory capacity and running time of generating a certain amount of blocks, respectively. All the analysis is verified under the average results of multiple experiments, since the evaluation may have random factors.

5.1. Storage Used Analysis

Figure 5 shows the used memory comparison between three architectures in a real smart home scenario. As shown in Figure 5, we can easily find each node in an original blockchain architecture consumes more memory than that in the other two architectures. This is because every node stores a copy of all records (all transaction data), and the used memory capacity of the entire network is proportional to the number of categories of data in each node. In contrast, our architecture and the hypergraph-based blockchain architecture require much smaller storage consumption because both schemes use multiple blockchains to store data. On the other hand, our architecture has almost the same result as the hypergraph-based blockchain architecture in memory consumption but is a little better in some scenarios. Specifically, the number of CNs in each VS which maintains a sub-blockchain is limited in our architecture, thus the average storage of each node and the transaction data for synchronization are also limited to a certain range. In our experiments, it can save up to 90% of storage space when the network is large with many nodes/devices. Thus, our scheme needs less storage through experiments analysis while comparing with the same type of methods.

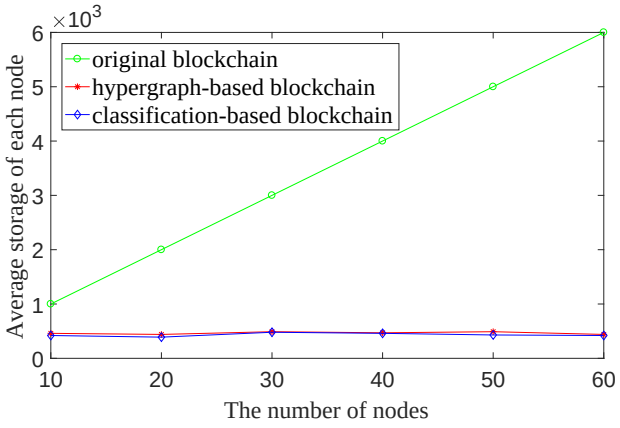

Figure 5. The used memory comparison among three architectures in real smart home scenario.

5.2. Latency and Security Evaluation

In this section, we evaluate the performance of the hierarchical PoW mechanism while comparing it with the traditional PoW. Generally, the running time of PoW is a linear positive correlation with the difficulty. Both the original and hypergraph-based blockchain architecture use traditional PoW so that they can only set one kind of difficulty for all data categories. In order to ensure safety, they have to set all categories of data to the highest difficulty. However, our architecture with hierarchical PoW mechanism can set the appropriate difficulty to each data category. As shown in Table 2, we compare the running time of generating a certain amount of blocks among three architectures. The results reflect the running time of ours is almost 50% less than other architectures, due to our proposed hierarchical PoW mechanism. That means our scheme has less latency than the others. Moreover, in our experimental test, the difficulty of each security grade is not high, and the average block time of all security grades is only about 3 s.

Table 2. Comparison of the running time of generating certain number of blocks among three architectures.

Number of Blocks	Running Time(s)		
	Original Blockchain	Hypergraph-Based Blockchain	Classification-Based Blockchain
1	5.7	5.1	2.8
2	10.8	10.4	5.6
3	16.9	16.2	7.9
4	21.5	21.2	10.6
5	27.5	27.1	14.1
6	32.9	32.5	17.4
7	37.2	36.8	19.8
8	44.3	43.9	22.7

To further evaluate our safety performance, we conducted several attacks on the system, tampering with data with malicious nodes to affect integrity. As shown in Figure 6, in our experiment, both the safety factor and average storage of each node are proportional to the *maxn* of a VS (i.e., the maximum number of participated devices in a sub-network). Obviously, the security level is determined by the maximum size of the VS. The greater the *maxn* of a VS is, the higher the security, and vice versa. In other words, the specific number of participating devices determines the safety factor of the system. Since smart homes usually contain dozens of devices, the systems have a high safety factor, and the cost of hacking is quite high. Consequently, the safety factor can be improved by increasing the number of participating devices depending on the specific scenarios. In summary, our scheme has a good integrity performance.

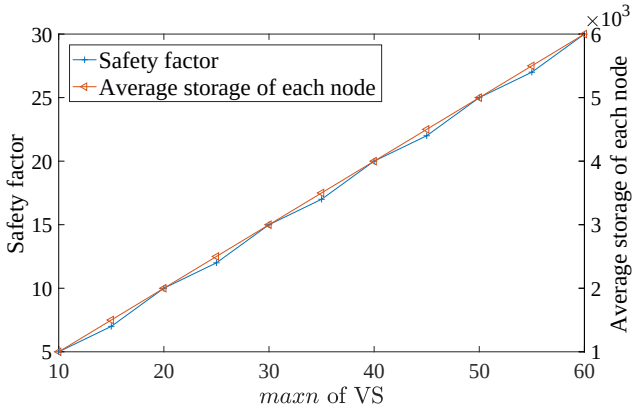

Figure 6. The relationship among the *maxn* of VS, the average storage of each node, and the security.

6. Conclusions

In this paper, we propose a classification-based blockchain architecture with hierarchical PoW mechanism in the smart home to address security challenges for resource-constrained IoT. With the proposed scheme, the experimental results show that it decreases risks to a certain degree, and reduces storage by almost 90%. Meanwhile, our moderate-cost hierarchical PoW mechanism balances the security and performance to an acceptable level so that it can reduce the running time by almost 50%.

As we know, the PoW-based mechanism always needs to consume a lot of device resources for the blockchain calculation. Although we use a moderate-cost strategy to reduce the resource consumption in our proposed architecture, unfortunately, the efficiency of the system is still not enough. Consequently, our next work will focus on further improving the efficiency of the system. The possible research direction may use a more lightweight approach to replace the PoW-based scheme.

Author Contributions: Conceptualization, W.L., N.W., X.X. and Z.H.; methodology, N.W. and Z.H.; software, X.X.; validation, W.L. and X.X.; formal analysis, W.L., N.W. and X.X.; investigation, W.L. and N.W.; writing—original draft preparation, W.L., N.W. and X.X.; writing—review and editing, Z.H.; visualization, X.X.; funding acquisition, Z.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under Grant No. 62072408, Zhejiang Provincial Natural Science Foundation of China under Grant No. LY20F020030, and New Century 151 Talent Project of Zhejiang Province.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank all of the anonymous reviewers who spent their own time to review this article and provide suggestions.

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

References

1. Camero, A.; Alba, E. Smart city and information technology: A review. *Cities* **2019**, *93*, 84–94. [CrossRef]
2. Laufs, J.; Borrion, H.; Bradford, B. Security and the smart city: A systematic review. *Sustain. Cities Soc.* **2020**, *55*, 102023. [CrossRef]
3. Dattana, V.; Kumar, A.; Kush, A.; Kazmi, S.I.A. Manet for Stable Data flow in Smart home and Smart city. In Proceedings of the 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 January 2019; pp. 1–4.
4. Almusaylim, Z.A.; Zaman, N. A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT). *Wirel. Netw.* **2019**, *25*, 3193–3204. [CrossRef]
5. Sovacool, B.K.; Del Rio, D.D.F. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renew. Sustain. Energy Rev.* **2020**, *120*, 109663. [CrossRef]
6. Scuotto, V.; Ferraris, A.; Bresciani, S. Internet of Things: Applications and challenges in smart cities: A case study of IBM smart city projects. *Bus. Process Manag. J.* **2016**, *22*, 357–367. [CrossRef]
7. Hoque, M.A.; Davidson, C. Design and Implementation of an IoT-Based Smart Home Security System. *Int. J. Netw. Distrib. Comput.* **2019**, *7*, 85–92. [CrossRef]
8. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: Challenges, issues and solutions at different IoT layers. *J. Supercomput.* **2021**, *77*, 14053–14089. [CrossRef]
9. Yu, R.; Zhang, X.; Zhang, M. Smart home security analysis system based on the internet of things. In Proceedings of the IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Nanchang, China, 26–28 March 2021; pp. 596–599.
10. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
11. Song, J.C.; Demir, M.A.; Prevost, J.J.; Rad, P. Blockchain Design for Trusted Decentralized IoT Networks. In Proceedings of the 2018 13th Annual Conference on System of Systems Engineering (SoSE), Paris, France, 19–22 June 2018; pp. 169–174.
12. Moniruzzaman, M.; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for smart homes: Review of current trends and research challenges. *Comput. Electr. Eng.* **2020**, *83*, 106585. [CrossRef]
13. Arif, S.; Khan, M.A.; Rehman, S.U.; Kabir, M.A.; Imran, M. Investigating smart home security: Is blockchain the answer? *IEEE Access* **2020**, *8*, 117802–117816. [CrossRef]
14. Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Ali, A. A machine learning approach for blockchain-based smart home networks security. *IEEE Netw.* **2020**, *35*, 223–229. [CrossRef]
15. Baucas, M.J.; Gadsden, S.A.; Spachos, P. IoT-based smart home device monitor using private blockchain technology and localization. *IEEE Netw. Lett.* **2021**, *3*, 52–55. [CrossRef]
16. Giannoutakis, K.M.; Spathoulas, G.; Filelis-Papadopoulos, C.K.; Collen, A.; Anagnostopoulos, M.; Votis, K.; Nijdam, N.A. A blockchain solution for enhancing cybersecurity defence of IoT. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 490–495.
17. King, S. Primecoin: Cryptocurrency with Prime Number Proof-of-Work. 2013. Available online: http://primecoin.io/bin/primecoin-paper.pdf (accessed on 7 July 2013).
18. Khan, A.A.; Laghari, A.A.; Shaikh, A.A.; Bourouis, S.; Mamlouk, A.M.; Alshazly, H. Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission. *Appl. Sci.* **2021**, *11*, 10917. [CrossRef]
19. Khan, A.A.; Shaikh, Z.A.; Baitenova, L.; Mutaliyeva, L.; Moiseev, N.; Mikhaylov, A.; Laghari, A.A.; Idris, S.A.; Alshazly, H. QoS-ledger: Smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. *Electronics* **2021**, *10*, 3083. [CrossRef]

20. Suchaad, S.A.L.; Mashiko, K.; Ismail, N.B.; Abidin, M.H.Z. Blockchain use in home automation for children incentives in parental control. In Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence, Hanoi, Vietnam, 28–30 September 2018; pp. 50–53.
21. Tantidham, T.; Aung, Y.N. Emergency service for smart home system using ethereum blockchain: System and architecture. In Proceedings of the 2019 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 888–893.
22. Saxena, U.; Sodhi, J.S.; Tanwar, R. Augmenting smart home network security using blockchain technology. *Int. J. Electron. Secur. Digit. Forensics* **2020**, *12*, 99–117. [CrossRef]
23. Qashlan, A.; Nanda, P.; He, X. Security and privacy implementation in smart home: Attributes based access control and smart contracts. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2021; pp. 951–958.
24. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: Challenges and Solutions. *arXiv* **2016**, arXiv:1608.05187.
25. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an Optimized BlockChain for IoT. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
26. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.K.R. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [CrossRef]
27. Qu, C.; Tao, M.; Yuan, R. A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes. *Sensors* **2018**, *18*, 2784. [CrossRef] [PubMed]
28. Mohanty, S.N.; Ramya, K.C.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.K.; Khanna, A. An efficient Lightweight integrated blockchain (ELIB) model for IoT security and privacy. *Future Gener. Comput. Syst.* **2020**, *102*, 1027–1037. [CrossRef]
29. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Karizno, S.R. SLPoW: Secure and low latency proof of work protocol for blockchain in green IoT networks. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5.
30. Yu, H.; Gibbons, P.B.; Kaminsky, M.; Xiao, F. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (S&P 2008), Oakland, CA, USA, 18–22 May 2008; pp. 3–17.