
Electronic Thesis and Dissertation Repository

11-28-2019 11:00 AM

Blockchain-Based Distributed Network Architecture for Internet of Things

Min Li

The University of Western Ontario

Supervisor

Wang, Xianbin

The University of Western Ontario

Graduate Program in Electrical and Computer Engineering

A thesis submitted in partial fulfillment of the requirements for the degree in Master of Engineering Science

© Min Li 2019

Follow this and additional works at: <https://ir.lib.uwo.ca/etd>



Part of the [Systems and Communications Commons](#)

Recommended Citation

Li, Min, "Blockchain-Based Distributed Network Architecture for Internet of Things" (2019). *Electronic Thesis and Dissertation Repository*. 6768.

<https://ir.lib.uwo.ca/etd/6768>

This Dissertation/Thesis is brought to you for free and open access by Scholarship@Western. It has been accepted for inclusion in Electronic Thesis and Dissertation Repository by an authorized administrator of Scholarship@Western. For more information, please contact wlsadmin@uwo.ca.

Abstract

IoT networks have already been widely deployed for its convenience and low-cost advantage. However, due to the lack of self-protection mechanisms and the imperfect network architectures, many IoT devices are very vulnerable for malicious cyber-attacks, which will further threaten the availability and security of information. Therefore, securing the network infrastructure while protecting data from malicious or unauthorized devices/users become a vital aspect of communication network design. In the thesis, two types of IoT scenario are mainly investigated, namely, IoT routing protection and smart community device authentication.

In IoT routing network, misbehaving routers affect the availability of the networks by dropping packets selectively and rejecting data forwarding services. By adopting the distributed consensus mechanism, we propose a blockchain-based reputation management system in IoT networks to overcome the limitation of centralized router RM systems. The proposed solution utilizes the blockchain technique as a decentralized database to store router reports for calculating reputation of each router. With the proposed reputation calculation mechanism, the reliability of each router would be evaluated, and the malicious misbehaving routers with low reputations will be blacklisted and get isolated. More importantly, we develop an efficient group mining process for blockchain technique in order to improve the efficiency of block generation and reduce the resource consumption.

In a smart community, current authentication approaches suffer from numerous challenges, such as poor authentication efficiency, inflexible authentication approach and insecure information sharing server. We propose a novel sidechain structure via optimized two-way peg protocol for device authentication in the smart community in order to overcome the limitations of existing approaches. The proposed sidechain structure requires the mainchain mining nodes to only store the local mainchain blocks without downloading or updating the entire mainchain after each block generation. By using Simplified Payment Verification (SPV) consensus mechanism, the existence of the target authentication information could be proved. Moreover, we propose an optimized two-way peg protocol in the proposed sidechain system in order to prevent the worthless information attack during the information sharing procedure.

Keywords: IoT, routing protection, smart community, blockchain, sidechain, two-way protocol, reputation management, device authentication, information sharing.

Summary for Lay Audience

With the emergence of wireless communications and smart devices, lots of progress have been made in the field of Internet of Things (IoT). IoT networks have already been widely deployed for its convenience and low-cost advantage. However, due to the lack of self-protection mechanisms and the imperfect network architectures, many IoT devices are very vulnerable for malicious cyber-attacks, which will further threaten the availability and security of information. Therefore, securing the network infrastructure while protecting data from malicious or unauthorized devices/users become a vital aspect of communication network design.

The emerging blockchain technology, with the inherent decentralized consensus mechanism, provides a promising method to maintain a secure peer-to-peer network. By adopting the distributed consensus mechanism of blockchain, i.e. Proof of Work (PoW), trust relationships can be established among its members, even some of the entities may not be fully trusted. In the thesis, two types of IoT scenario are mainly investigated, namely, IoT routing protection and smart community device authentication. For IoT routing protection, we propose a blockchain-based reputation management system in IoT networks to overcome the limitation of centralized router RM systems. More importantly, we develop an optimized group mining process for blockchain technique in order to improve the efficiency of block generation and reduce the resource consumption. The simulation results validate the distributed blockchain-based RM system in terms of attacks detection and system convergence performance, and the comparison result of the proposed group mining process with existing blockchain models illustrates the applicability and feasibility of the proposed works.

For smart community device authentication, we propose a novel sidechain-based authentication scheme for a smart community in order to overcome the limitations of existing approaches. To prevent the worthless information injection attack during the information sharing procedure, we also propose an optimized two-way peg protocol. Consequently, the simulation results prove the superiority of the proposed scheme in terms of reducing authentication time, improving information management efficiency and decreasing storage consumption as compared to existing works, and the applicability and feasibility of the optimized two-way peg protocol have been approved.

Acknowledgments

I would like to express my deepest gratitude to my supervisor, Dr. Xianbin Wang, for his patient guidance and selfless supports in developing my research. He encouraged me to explore a novel research area and focus on the latest technique problems. That is why I jumped out my comfort zone and worked on the blockchain-related area. He taught me how to do research studies and how to be a qualified engineer. It was a wonderful experience to learn from him during these two years.

I would like to thank everyone in our research group for their professional suggestions and advice during each research group meeting. Especially, I want to thank to Dr. He Fang, Dr. Fuad Shamieh and Dr. Tianqi Yu for forming a blockchain research group with me and sharing their understandings of the technical details. I cannot make such rapid progress without regular meetings and discussions with them.

Also, I would like to say thank you to every course supervisor I have met in University of Ontario during these two years for their professional guidance and help.

Last but not least, I would like to thank my parents, Shangjun Li and Hongxia Zhang, for their endless support and encouragement. Studying abroad is not a easy thing. It is their love that helped me to overcome lots of difficulties in these two years.

Finally, I would like to say thank you to the Department of Electrical and Computer Engineering at Western University for the excellent facilities, administrative staff, and resources available to graduate students.

Contents

Abstract	i
Summary for Lay Audience	ii
Acknowledgments	iii
List of Figures	vii
List of Tables	ix
List of Abbreviations	x
1 Introduction	1
1.1 Overview of IoT Networks	1
1.2 Thesis Motivations and Objectives	3
1.2.1 Routing Process in IoT Networks	3
1.2.2 IoT Smart Community	4
1.3 Contributions of the Thesis	5
1.4 Thesis Outline	7
2 Security Challenges in IoT Networks and Existing Solutions	9
2.1 Routing Process in IoT Networks	10
2.1.1 Security Challenges in IoT Routing Process	10
2.1.2 Existing Solutions	11
2.1.2.1 Routing Protocol for Low Power and Lossy Networks	11
2.1.2.2 Reputation Management Systems	13
2.1.3 Analysis	16
2.2 IoT Smart Community	17
2.2.1 Existing Challenges in IoT Smart Community	17
2.2.2 Existing Solutions	18
2.2.2.1 Centralized Information Sharing Server	18
2.2.2.2 Decentralized Information Sharing Server	19
2.2.3 Analysis	21
2.3 Chapter Summary	22
3 Blockchain Technology and Its Applications	23
3.1 Overview of Blockchain Technique	24

3.1.1	Key Pair and Signature Creation	24
3.1.2	Signature Verification	25
3.1.3	Mining Process	26
3.2	Type of Blockchain Technology	29
3.2.1	Public Blockchain	29
3.2.2	Private Blockchain	29
3.3	Sidechain Technology	30
3.3.1	Sidechain Structure	30
3.3.2	Two-way Peg Protocol	31
	3.3.2.1 Confirmation Period	33
	3.3.2.2 Contest Period	33
3.3.3	Sidechain vs. Blockchain	34
3.4	Applications of Blockchain Technique	35
3.4.1	Crypto-currency	35
3.4.2	Internet of Things (IoT)	35
3.4.3	Data Security and Data Sharing	36
3.4.4	Identity Management	36
3.4.5	Medical Applications	37
3.5	Analysis of Advantages and Disadvantages	37
3.5.1	Advantages of Blockchain Technology	37
3.5.2	Disadvantages of Blockchain Technique	38
3.6	Chapter Summary	39

4 Blockchain-based Distributed Reputation Management System for IoT Routing Protection **40**

4.1	Introduction	40
4.2	System Model	41
4.3	Proposed Scheme	42
4.3.1	Blockchain-based Reputation Management System	42
4.3.2	Efficient Group Mining Process	44
4.4	Model Analysis	48
4.4.1	Technology Comparison	48
4.4.2	Overhead Analysis	49
	4.4.2.1 Computation Requirements	49
	4.4.2.2 Communication Overhead	50
	4.4.2.3 Storage Overhead	51
4.5	Performance Evaluation	52
4.5.1	Simulation Settings	52
4.5.2	Analysis of Experimental Results	53
	4.5.2.1 Attack Detection Performance	53
	4.5.2.2 System Convergence Performance	55
	4.5.2.3 Robustness and Efficiency Performance	57
4.6	Chapter Summary	61

5	A Sidechain-based Decentralized Authentication Scheme via Optimized Two-way Peg Protocol for Smart Community	63
5.1	Introduction	63
5.2	System Model	64
5.2.1	Local Authentication Procedure at Private Side Blockchains	65
5.2.1.1	Registration Phase	66
5.2.1.2	Authentication Phase	67
5.2.2	Authentication Information Sharing at Public Mainchain	68
5.3	Technology Comparison	71
5.4	Simulation Experiment and Result Analysis	71
5.4.1	Authentication Time Consumption Analysis	72
5.4.1.1	Simulation Settings	73
5.4.1.2	Authentication Time Consumption Against PSK Character Lengths	73
5.4.1.3	Authentication Time Consumption Against Blockchain Parameters	74
5.4.2	Performance Analysis of the Proposed Optimized Two-way Peg Protocol	76
5.4.2.1	Simulation Settings	76
5.4.2.2	Optimized Two-way Peg Protocol Performance	77
5.4.3	Performance Analysis of the Information Management Efficiency	78
5.4.3.1	Simulation Settings	78
5.4.3.2	Information Management Efficiency Performance	79
5.4.4	Storage Consumption Comparison	80
5.5	Chapter Summary	81
6	Conclusion and Future Work	83
6.1	Conclusion	83
6.2	Future Work	85
6.2.1	The Proposed Blockchain-based Reputation Management System	85
6.2.2	The Proposed Sidechain-based device Authentication Scheme	86
	Bibliography	88
	Curriculum Vitae	94

List of Figures

1.1	Typical applications of IoT networks.	2
2.1	Basic model of IoT routing process. The model consists of three layers: cloud server layer, routing layer and end-user device layer.	10
2.2	RPL path construction using DODAG method.	13
2.3	Centralized reputation management system model. The IoT devices upload the reputation reports to the central reputation management server, and the sever sends the blacklist back to them.	14
2.4	Model for cooperative mining process.	15
2.5	A smart home model where the gateway handles the local registration and authentication processes for each IoT device.	18
2.6	An IoT smart community where each smart system is centrally managed by a gateway, and all the systems rely on a third-party server for sharing information within the community.	19
2.7	A Blockchain-based method for authentication process in IoT smart community.	20
3.1	Basic structure of blockchain.	24
3.2	Procedure of the data encryption and broadcast.	25
3.3	Procedure of the signature verification.	26
3.4	Detailed block contents and structure.	26
3.5	Example of PoW consensus mechanism.	27
3.6	Flowchart of Proof of Work (PoW) mining process.	28
3.7	Structure of sidechain technology. The sidechain structure consists of a main-chain and several side blockchains. The crypto-currency used in each sidechain can be various.	31
3.8	Procedure of the two-way peg protocol in sidechain technology.	32
4.1	Adversarial blockchain-based reputation management system in IoT networks. The data link between the users and cloud server suffers from malicious routers.	42
4.2	Model of proposed group mining process, in which edge devices with high computational power will be required to group to edge devices with low computational power.	45
4.3	Flowchart of the proposed group mining process.	47
4.4	Packet dropping attacks detection for different malicious levels.	54
4.5	Selfish behavior detection for different malicious levels.	55
4.6	Convergence of the proposed reputation system for different malicious levels. .	56
4.7	Convergence of the proposed reputation system for different network sizes. . . .	56

4.8	Global reputation value performance detection for different malicious levels. . .	58
4.9	Comparing the proposed RM system with other existing trust models in terms of average STR against malicious percentage.	59
4.10	Comparison results of our blockchain model with other existing blockchain models in terms of processing time for creating one new block.	60
5.1	Proposed sidechain-based authentication model. The proposed model consists of a public mainchain and private side blockchains.	65
5.2	Structure and content of the private side blockchain.	66
5.3	Procedure of the proposed authentication process at private side blockchain. . .	67
5.4	Model of authentication information sharing at the public mainchain. Both PoW consensus mechanism and the proposed optimized two-way peg protocol have been applied for safe operation of the proposed sidechain-based smart community system.	68
5.5	Authentication time comparison among three methods with different PSK character lengths.	74
5.6	Authentication time comparison of three block positions with different blockchain lengths.	75
5.7	Performance evaluation for optimized two-way peg protocol with using certificates as the authentication method.	77
5.8	Information management efficiency comparison among the proposed sidechain-based method, traditional sidechain method and existing blockchain-based method.	79
5.9	Storage consumption comparison between conventional method, blockchain-based method, traditional sidechain and proposed sidechain model.	80

List of Tables

3.1	Comparison Results Between Blockchain Technology and Sidechain Technology.	34
4.1	Comparison Results Between The Traditional Blockchain Technology, Existing Blockchain Model and the Proposed Blockchain Model.	49
4.2	Memory Size for Each Block Component of a Blockchain.	51
4.3	System Settings Comparison and Parameter Settings.	52
5.1	The Technology Comparison Between the Traditional Blockchain Technology, the Traditional Sidechain Technology and the Proposed Sidechain Model. . . .	72
5.2	Environment Features of Authentication Process.	73
5.3	Parameter Configurations for Testing the Proposed Trust Scheme.	76
5.4	Parameter Configurations for Analyzing the Implementation Cost.	78

List of Abbreviations

CH	Cluster head
CO	Communication Overhead
CV	Centrality value
DAO	Destination Advertisement Object
DIO	DAG Information Object
DIS	DAG Information Solicitation
DODAG	Destination-Oriented Directed Acyclic Graph
ETX	Expected transmission times
GHz	Gigahertz
IoT	Internet of Things
LAN	Local Area Network
LLNs	Low power and Lossy Networks
LQL	Link quality level
LSB	Lightweight Scalable Blockchain
MP2P	Multipoint-to-point traffic
OF	Objective Function
PDR	Packet Delivery Ratio
PLC	Power Line Communication networks
PoW	Proof of Work
PSK	Pre-Shared Key
OTP	One Time Password
P2P	Point-to-point
P2P	Peer-to-Peer
P2MP	Point-to-multipoint traffic

QoS	Quality of Service
RM	Reputation Management
RPL	Routing Protocol for Low Power and Lossy Networks
SHA	Secure hash algorithm
STR	Successful Transaction Rate
WPANs	Wireless Personal Area Networks
WSNs	Wireless Sensor Networks

Chapter 1

Introduction

1.1 Overview of IoT Networks

With the proliferation of Internet-enabled smart devices, Internet of Things (IoT) networks have attracted significant attention of both academics and industry professionals [1]. IoT network is the network that allows different types of smart devices to connect and exchange data in order to realize the demands of "Smart Life" [2]. Compared to the traditional Internet, IoT network has strong inclusiveness towards the categories of end-user devices (IoT devices). For instance, it does not limit its Internet connectivity to standard devices, such as computers, smartphones and tablets. Any range of physical devices and everyday objects embedded with IoT technology can communicate and interact with others through the Internet, and they can be remotely monitored and controlled. For example, the temperature in a smart home can be adjusted remotely by IoT networks.

With these IoT-enabled intelligent devices, IoT networks have played a fundamental role in many different scenarios [3]. Fig. 1.1 shows some typical applications of IoT networks, including medical and health care, smart home and transportation. Taking health care as an example, the patient's blood pressure and heart rate can be monitored and analyzed according to IoT health monitoring devices readings collected. Moreover, connecting in-home monitoring devices to hospital-based systems can be implemented to ensure an accurate health protection with IoT networks. With millions of IoT devices being deployed every day, an enormous amount of data and information will be generated and analyzed every day, which will totally

redefine the way people live [4].

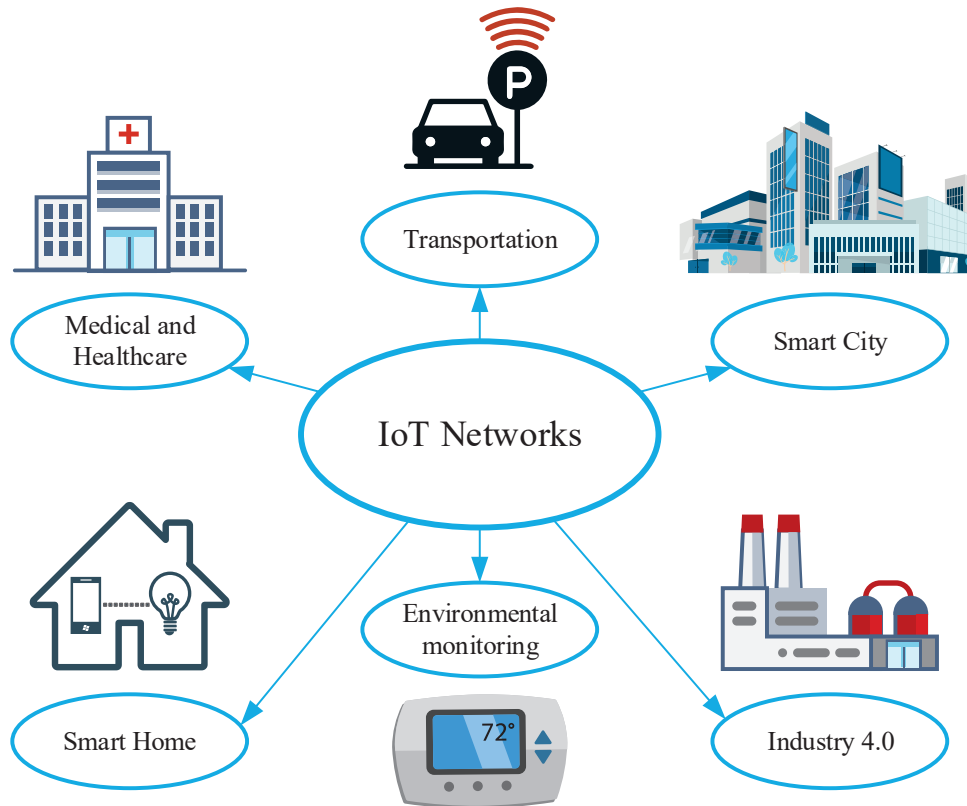


Figure 1.1: Typical applications of IoT networks.

The generation of IoT networks precisely meets the needs of automation and intelligent applications. However, both memory capacities and energy resources of IoT devices are quite limited, due to the constraints of low manufacturing and application costs. These immanent restrictions will cause several challenges when implementing the IoT networks.

The first challenge is the security concern of the personal data [3]. Personal data collected by end-user devices is uploaded to the cloud server through IoT smart devices for the purpose of monitoring and data analysis. Due to the computational and hardware related constraints, IoT devices could be compromised by attackers to act maliciously. For instance, due to the lack of self-protection mechanisms, IoT devices are very vulnerable for different malicious cyber-attacks, such as information stealing, selfish attacks and identity usurpation. Especially in large-scale IoT networks with enormous amounts of smart devices, the effects of misbehaving devices are more remarkable regarding to the data transmission accuracy and information

security.

Another challenge is the imperfection of the existing network security structure in IoT networks [5]. Owing to the decentralized nature of IoT networks, collaborative environments can be achieved among IoT devices for the improvement of energy efficiency and data accuracy. However, the existing IoT network security system structure still relies on the traditional centralized model and the reliability of the third party, which violates the purpose of designing IoT networks. Therefore, how to design a decentralized IoT network security system structure while providing excellent performance in attack defense needs to be investigated.

Additionally, efficiency improvement is also critical in IoT networks due to the limited resources [6]. If the designed works increase too much additional burden to the smart devices, the network could suffer from bottleneck communications and large processing latencies, which limit the system Quality of Service (QoS) performance. Thus, it is necessary to develop a decentralized platform in IoT networks for stringent QoS provisioning required by IoT applications.

In conclusion, IoT networks play an irreplaceable role in providing services for residents with both public city infrastructure and private smart devices. Whereas, there are still several challenges that need to overcome.

1.2 Thesis Motivations and Objectives

As we mentioned above, IoT networks have been applied to many different applications, and there are still many severe challenges needed to be resolved. In this thesis, we mainly focus on two scenarios: routing process in IoT networks and device authentication process in IoT smart community.

1.2.1 Routing Process in IoT Networks

Since a large amount of valuable data collected by end-user devices will be transmitted to the cloud server through the IoT routing layer in IoT networks, protecting the routing process is vital for data security and privacy-preservation.

Attack Detection: IoT networks are normally applied in both private and public networks for data exchanging and data analysis. Since IoT devices have constrained resources, self-protection mechanisms can hardly be achieved among IoT routers in the routing layer. Once attackers capture a routing node, the cryptography information can be extracted and utilized for working legally in the network. As a result, the whole network is threatened by cyber attackers and different malicious routing behaviors. Thus, the research objective is securing the IoT routing process by detecting the misbehaving devices while mitigating the resource restriction.

Security Framework Enhancement: A security management system is required in order to monitor the misbehaving IoT routers. Although the centralized security system model can provide a reasonable detecting performance, centralized framework is not suitable for the decentralized nature of IoT networks. In addition, with the number of IoT devices dramatically increasing in the network, the centralized security center cannot properly manage the information for the whole system. Therefore, our specific objective is designing a decentralized security management system for IoT routing protection.

System Efficiency Improvement: During the detection process of the security management system, certain calculation schemes would be applied in order to rank the trust of each router in the IoT routing layer. Considering the limited energy resources of each IoT router, a reasonable light-weighted calculating scheme should be used to improve the system efficiency and detection performance. Hence, improving the efficiency of security system for IoT routing protection is another research object.

1.2.2 IoT Smart Community

Smart community is a virtual environment composed of different IoT systems, such as smart homes, smart health, and smart public buildings [7]. Personal data are collected and processed in each system by smart devices, and then get shared among the community in order to improve community safety, home security, healthcare quality, and emergency response abilities [8]. Both device authentication process in each smart system and information sharing process within sub-systems are the major obstacles for privacy protection in smart community due to

imperfect mechanisms and the resource-constrained nature of IoT devices [9].

Authentication Efficiency Improvement: Most of the existing IoT smart systems rely on a gateway device to manage the local device authentication process. With the number of IoT devices increasing in the system, the burden of the centralized server will increase dramatically. In this case, the system will undergo bottleneck communications and large processing latencies, which limit the system Quality of Service (QoS) performance. Thus, the research objective is improving the device authentication efficiency in each system of the smart community.

Adaptive Authentication Methods: There are many authentication methods existing for smart devices with different computational powers and scenarios, such as One Time Password (OTP), Pre-Shared Key (PSK) and Certificates [10] [11] [12]. However, all the smart devices in the same system can only use one authentication method regardless of different computational powers. Therefore, an adaptive authentication mechanism that can apply various authentication methods in the same system should be proposed in order to ensure a more flexible and resilient security for each device.

Information Sharing Server Enhancement: In a smart community with many assembled smart systems, it is normal to have IoT devices that move from one system to another. In this case, the authentication information should be transferred among different systems. Existing solutions involve a centralized third-party server to handle the shared information by assuming it is fully trustworthy. However, the whole system will suffer from the risk of one-point failure, and the security of personal data will be threatened. Hence, designing a decentralized information sharing structure for smart community is another research objective.

1.3 Contributions of the Thesis

The main contributions of this thesis are summarized as follows:

- A comprehensive description of blockchain technology is presented in order to show the benefits of applying this technology into the IoT environments. In particular, both struc-

ture and operation procedure of the blockchain technique are introduced. Proof of work (PoW), as the core technology of the blockchain technique, has been summarized with a flowchart. Additionally, several blockchain related concepts are also presented, as they are the basis of the proposed models in the later chapters. Sidechain technology, as an extended technology of blockchain, is introduced in details and compared the technical aspects with the blockchain technology. After that, several promising research areas for blockchain technology have been outlined, and some representative works are also summarized. In the end, an objective appraisal towards blockchain technology is also given for the purpose of an in-depth study of blockchain.

- A blockchain-based reputation management system for IoT routing protection in IoT networks is proposed in this thesis. The contribution of this work is twofold. **Firstly**, we proposed a 4-steps blockchain-based reputation management system in order to evaluate the reliability of each route. As a result, the malicious misbehaving routers with low reputations will be blacklisted and get isolated. **Secondly**, in order to introduce the blockchain technology into the IoT environment, an efficient group mining technique has been proposed. The efficient group mining simplifies the mining procedure by setting mining nodes into group to mine the same block. The nonce value range of each mined block has been calculated and distributed to each group members. The computational powers of each group has been balanced in order to prevent 51% attack.
- A sidechain-based authentication scheme via optimized two-way peg protocol for smart community is proposed in order to overcome the challenges caused by existing blockchain-based method. The contribution of this work is twofold. **Firstly**, we propose an optimized sidechain structure for device authentication in the IoT smart community. Instead of downloading and updating the entire mainchain after each block generation process as traditional sidechain technology, the proposed structure save a reference mainchain block at local memory and use SPV proof to prove the existence of the information. The proposed structure consumes less storage consumption, and gets more efficient when searching the target information. **Secondly**, in order to protect the smart community from the worthless information injection attack and ensure the normal operation of sidechain tech-

nology in the IoT environment, an optimized two-way peg protocol has been proposed based on dynamically analyzing the trust value of the target device.

1.4 Thesis Outline

The rest of the thesis is organized as follows:

In Chapter 2, security challenges are briefly introduced for each IoT scenario (IoT routing process and smart community). Followed by this, existing technical solutions are summarized and analyzed according to the different categories. In IoT routing protection, both Routing Protocol for Low power and Lossy Networks (RPL) based solutions and reputation management based solutions are illustrated. For authentication process in smart community, both traditional centralized model and decentralized model are analyzed and compared. After that, a particular solution analysis for each IoT scenario is suggested.

In Chapter 3, a detailed overview of blockchain technique is firstly introduced, including the whole procedure of the block generation, the concept of Proof of Work (PoW) and other blockchain related knowledge. Then, a detailed demonstration of sidechain technology has been given, including its structure, the two-way peg protocol and its comparison results with blockchain technology. After that, the applications of blockchain technique are categorized based on different application fields, such as IoT, data security and medical applications. Finally, both advantages and disadvantages of the blockchain technique are summarized for future research.

In Chapter 4, a blockchain-based reputation management system for routing process protection in IoT networks is proposed. In the system model section, the proposed RM has been divided into four steps: 1) distributed information collection from neighboring routers; 2) routing service evaluation; 3) router reputation calculation; 4) misbehaving router blacklisting. To improve the implement efficiency of blockchain, an efficient group mining technique has been proposed. Then, the technology comparison and overhead analysis are given. Finally, some experiments have been conducted in MATLAB in order to evaluate the proposed blockchain-based RM model in terms of attack detection, system convergence performance and efficiency performance.

In Chapter 5, we proposed a sidechain-based authentication scheme via optimized two-way peg protocol for smart community. In the system model section, the local authentication procedure achieved at private side blockchains has been illustrated into registration phase and authentication phase. Then, the authentication information sharing procedure at the optimized mainchain is presented. More importantly, to enhance the information security of the community, an optimized two-way peg protocol has been proposed by dynamically evaluating the trustworthiness of each smart device based on the authentication method, previous authentication information sharing history and local authentication results. Then, the technology comparison is given. The simulation results prove that the proposed scheme has advantages compared with existing works in terms of reducing authentication time, improving information management efficiency and decreasing storage burden. The applicability and feasibility of the proposed optimized two-way peg protocol have also been approved.

Finally, all the contributions of this thesis are concluded in Chapter 6. The future research plan and suggestion are discussed in Chapter 6 as well.

Chapter 2

Security Challenges in IoT Networks and Existing Solutions

As we mentioned in the previous chapter, IoT network suffers from different types of malicious behaviors and attacks due to the limited resources and memory space constraints. In this chapter, we mainly focus on investigating the security challenges in IoT routing process protection and device authentication process in IoT smart community. For each scenario, after introducing the background of security problems, the existing solutions will be summarized and compared.

The remainder of this chapter is organized as follows. Section 2.1 introduces the IoT routing process. Some basic components of IoT routing layer are also presented, namely, end-user devices, IoT routers and cloud server. Then, existing solutions are divided into two categories: Routing Protocol for Low Power and Lossy Networks (RPL) based solutions and reputation management based solutions. The scenario of device authentication process smart community is discussed in Section 2.2. We firstly introduce the typical components of the smart system in the community. Then, we point out the existing challenges in the smart community. After comparing the centralized model with the decentralized model, we analyze the situation of the smart community and give our suggestions. Finally, a chapter summary is drawn in Section 2.3.

2.1 Routing Process in IoT Networks

2.1.1 Security Challenges in IoT Routing Process

With the increasing popularity of Internet of Thing (IoT) devices, massive amounts of IoT data have been generated and collected on a continuous basis for data analysis and monitoring, leading to increased requirements on communication and data security. The objective of IoT routing layer is to forward the data packet collected to the destination.

The following Fig. 2.1 presents the basic components of IoT routing process, namely, end-user device layer, routing layer and cloud server. In end-user device layer, different IoT devices collect the target data and then transmit the data through the routing layer to the cloud server for the purpose of storage and data analysis. The routing transmission can be one-hop or multi-hop, which increases the difficulty of malicious behaving detection [13].

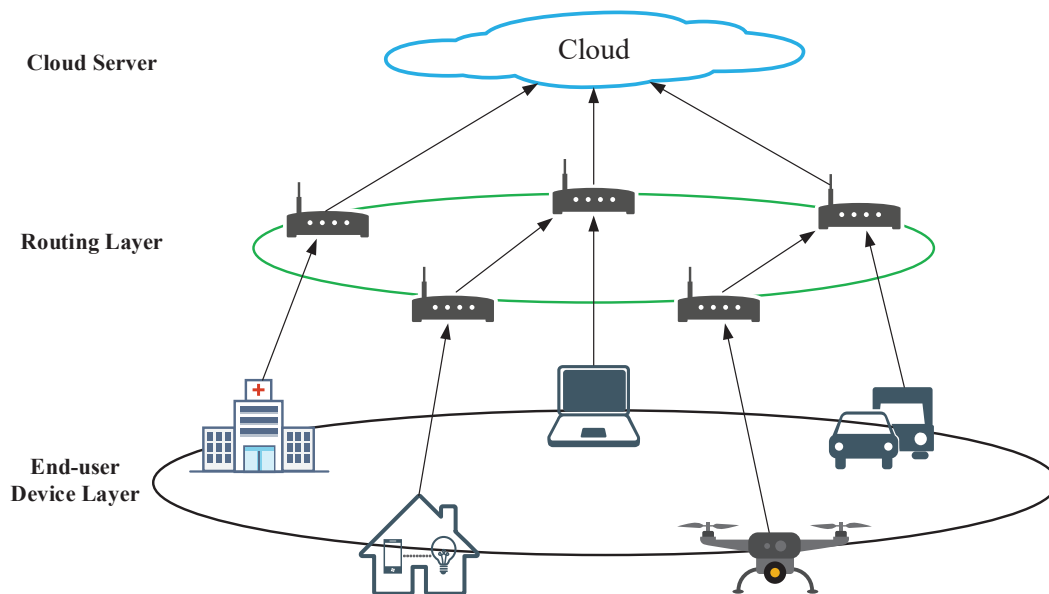


Figure 2.1: Basic model of IoT routing process. The model consists of three layers: cloud server layer, routing layer and end-user device layer.

Due to the computational and hardware related constraints, IoT routers do not have complete self-protection mechanisms for malicious cyber-attacks, which makes IoT routing layer one of weakest portions in the IoT data forwarding process [13]. In order to ensure the Quality of Service (QoS) required by IoT applications and secure the personal data required by

users, IoT routing protection is critical. Thus, how to mitigate the limitation of IoT routers and establish a trusted attack detection system is strongly needed in IoT networks.

2.1.2 Existing Solutions

To resolve the abovementioned security issues in routing process, many research have been done in the wireless networks, such as mobile ad-hoc networks and wireless sensor networks. Existing workable methods for routing protection can be classified into two categories, e.g. Routing Protocol for Low power and Lossy Networks (RPL) based and reputation management based.

2.1.2.1 Routing Protocol for Low Power and Lossy Networks

IoT network is one of the implementations of Low power and Lossy Networks (LLNs), in which low-power Power Line Communication networks (PLC), Wireless Personal Area Networks (WPANs) and Wireless Sensor Networks (WSNs) are all included. LLNs devices have highly resource constrained in terms of memory, battery life and processing power, which generates lots of security concerns during the routing process [14].

With these constraints, existing Internet protocols are unsuited for LLNs. Attackers can capture the routing node and extract the data packet for illegal purposes. Thus, the Routing Protocol for Low power and Lossy Networks (RPL) is designed aiming to avoid the insecure router and minimize the packet forwarding cost [15]. RPL supports three basic traffic flows: point-to-point (P2P) traffic, point-to-multipoint traffic (P2MP) and multipoint-to-point traffic (MP2P) [16]. Best routing path in RPL is determined by its parent selection process using the Objective Function (OF) and the Destination-Oriented Directed Acyclic Graph (DODAG) process [17] [18]. Here, we will briefly explain these two main procedures of RPL.

Objective Function (OF) and Ranking Process: Objective Function (OF) is the core technique in RPL by determining the rule of parent selection and forwarding decision. OF construction relies on four basic components: (i.) computing the path cost, (ii.) the rules for choosing parents (including time, number of parents and identity of parents), (iii.) the rules for ranking all the parents, (iv.) the way of advertising the path cost.

Base on the evaluation of Objective Function (OF), all the nodes in RPL will be ranked and the nodes with least rank will be chosen as the candidate parent nodes. Among the candidate parents list, the best parent node can be found by applying different routing metrics, such as throughput, link quality level (LQL) and expected transmission times (ETX) [19]. To apply RPL to different optimization scenario, the routing metrics can be changed.

Destination-Oriented Directed Acyclic Graph (DODAG) Process: Destination-Oriented Directed Acyclic Graph (DODAG) is the built graph in RPL that shows all the available paths of root node and leaf nodes. In such tree topology of RPL, root node is the destination node for all other devices. For example, a gateway in the smart home can be viewed as a root node, and the rest devices are leaf nodes. With DODAG and OF, all the rank results can be shown in the graph.

DODAG is consist of three basic ICMPv6 messages (i.) DAG Information Object (DIO), (ii.) DAG Information Solicitation (DIS) and (iii.) Destination Advertisement Object (DAO). The root node will send the DIO message to its neighbors and the neighbors will be required to send the acknowledgment back. The neighbor who sends the acknowledgment will be allowed to forward the DIO message to its own neighbors [20]. If the node outside the network wants to join in, they will need to send a DIS message to require a DIO message. DAO messages are sent by child nodes to the selected parent nodes after the DIO message received [21]. The following Fig. 2.2 shows the RPL path construction by using DODAG process.

It was proved that the RPL protocol performed well in defending the external attackers [22]. However, when IoT routers are compromised to become internal attackers, the protocol can hardly detect the malicious ones due to the insufficient computational capacity and resource constraints [23]. For instance, RPL has strict rules for managing routing path selection and optimized state. Once one router is attacked for illegal purposes, attackers can implement malicious code inside in order to break routing operation rules of RPL. As a result, the whole topology will be broken.

In order to enhance the security of RPL, many researches have been done and large amounts of RPL-expanded technologies were proposed. In [24], a Fuzzy logic reasoning was applied to RPL to transform heterogeneous routing metrics into one evaluation criterion. A two-stage

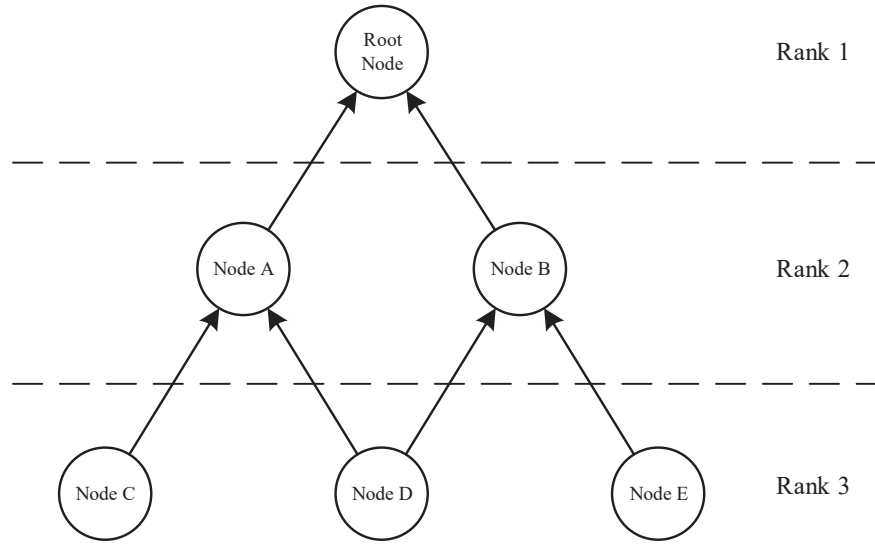


Figure 2.2: RPL path construction using DODAG method.

fuzzification engine was proposed in their work: both expected transmission times (ETX) and device energy are measured in order to increase the accuracy of path selection. The stability of the system is achieved by decreasing the possibility of parents change.

A trust-based RPL model was proposed for enhancing the ability of the internal attack detection [25]. By calculating the trustworthiness of each router, routing path decision can be made by using both trust directly available and trust indirectly from other routers. However, the calculation of direct and indirect trust requires significant amounts of memory for recording the history of both internal and external interactions among routers [26] [27]. These requirements on computational and energy resource directly limit the application of RPL based routing protecting in resource-constrained IoT systems. Additionally, trust calculation based on RPL can only be applied to limited neighboring routers due to its high resource requirements [28] [29].

2.1.2.2 Reputation Management Systems

The other category of routing protection is achieved through Reputation Management (RM) by recording the previous behaviors of each router. By analyzing previous behaviors reported by each router, the corresponding reputation of each router can be evaluated [30]. The routers with high reputation values are considered as trustworthy, while those with low reputation values are viewed as misbehaved ones [23].

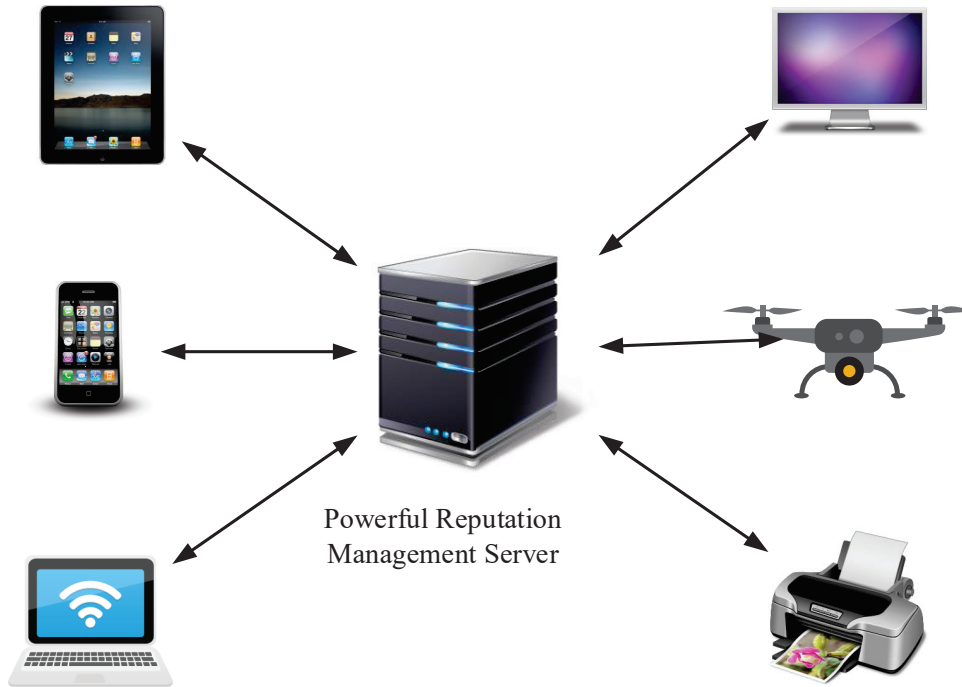


Figure 2.3: Centralized reputation management system model. The IoT devices upload the reputation reports to the central reputation management server, and the sever sends the blacklist back to them.

As presented in Fig. 2.3, most of the existing reputation management methods follow a centralized model where a powerful RM center collects, stores and analyses the reputation of all routers. However, the centralized nature of the RM center has the risk of one-point failure, which limits its application in IoT systems due to the stringent QoS requirement [31]. In addressing this challenge, a hierarchical trust management architecture was proposed for wireless sensor networks with decentralized third parties involved for collecting the trust information of all nodes [32]. Nevertheless, this method failed to consider the trustworthiness of the third parties used by assuming complete trust of third parties, and any entity of the third parties has the power to manipulate the data without detection.

A blockchain-based reputation system was proposed in order to mitigate the risk of malicious third party [33]. This scheme showed high reliability in attack defense by involving external nodes for monitoring all routers' behaviors. By applying the distributed consensus mechanism of blockchain, i.e. Proof of Work (PoW), trust relationships can be established among its members, even some of the entities may not be fully trusted [34]. In order to sim-

plify the PoW process, they proposed a cooperative mining process among all the mining nodes of the blockchain. As shown in Fig. 2.4, the target task of generating one new block has been divided by all mining nodes for decreasing the time consumption and energy waste. The head miner will firstly work on collecting all the reputation reports from the routers. Then, miner 2 will generate a genesis block, which is a block without header information. Miner 3 will calculate the nonce value and send to miner 4 for verification. After verifying at the miner 4, then block will be created and get broadcast to all the miners. Their experiment results proved the proposed model in terms of improving the packet delivery ratio and decreasing communication overhead by providing a decentralized reputation system [33].

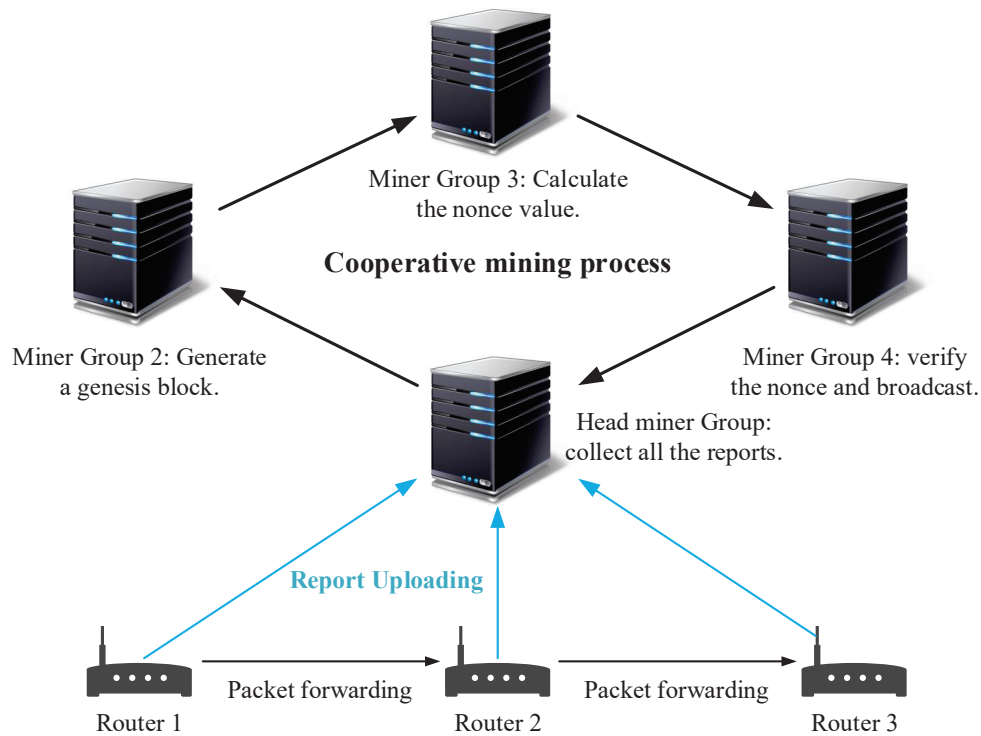


Figure 2.4: Model for cooperative mining process.

However, this proposed work did not specify the way of defining the trust among the routers, and the relationship between the mining nodes and the external routing nodes. Moreover, the cooperative mining process assigned the mining task to four miner groups without balancing the computational powers and information verification process are inside the miner groups. There is certain caused risk that one of the malicious miner groups has much more computational powers than other groups to dominate the blockchain and create fake transac-

tions and it will threat the whole system, which is called 51 percent attack in blockchain [35].

2.1.3 Analysis

Based on these two categories of alternative solutions for IoT routing protection, reputation management system is strongly suggested for its global decision scheme and high security performance. However, there are two main issues existing in the reputation management system that need to be fixed.

Firstly, a decentralized reputation management for IoT networks is needed. Most existing reputation systems are using a centralized powerful third party to collect all the reputation reports from routers and assuming all the routers can communicate with the center, which is not suitable for a decentralized IoT network. In addition, the centralized IoT reputation systems have a certain inherent vulnerability which is the one-point failure.

Secondly, a reputation mechanism which clearly define the trust of the routers in the IoT environment is needed. There are many works on reputation mechanism in ad-hoc network, and most accepted mechanisms utilize direct trust and indirect trust to calculate the reputation for an entity. Each entity has its own judged results for other entities so that it can make a wise decision when communicate with others, which means that every entity needs to calculate the reputation for others. The calculation consists of two folds: direct trust value and indirect trust value, and they are gained respectively based on the previous local reports which are saved in its own memory and the judged results that are received from others. This requirement costs lots of energy and recourses, which is clearly not suitable for IoT environment. Moreover, the built trust relationship is partial among several devices due to the large resources requirement, while the reputation management for IoT systems should have a global view to calculate the reputation values for each entity. Thus, a decentralized reputation management for IoT routing protection is in demand.

2.2 IoT Smart Community

2.2.1 Existing Challenges in IoT Smart Community

IoT smart community is an IoT application scenario where different IoT systems are combined, such as smart homes, smart health, and smart agriculture. In a smart community, personal data are collected and processed in each system by smart devices, and then get shared with other systems [8]. In order to protect the security of personal information, it is vital to make sure that only the registered and authenticated devices can make use of the system and share information. Otherwise, it will result in numerous potential security risks such as information stealing, data tampering and identity usurpation [36]. Both local authentication process in each smart system and information sharing process within sub-systems are the major obstacles for privacy protection in IoT smart community due to imperfect mechanisms and the resource-constrained nature of IoT devices [37].

In numerous IoT smart systems, the architecture still relies on a centralized model to handle the local registration and authentication processes [38]. Fig. 2.5 presents a smart home system where each device accomplishes the local registration and authentication processes through the gateway. When the number of IoT devices increases, the communication burden of gateway will be increased. Plus, it also increases the probability of one-point failure for the whole system. Thus, how to design a decentralized communication structure for local registration and authentication processes in smart system is worthy to investigate.

In smart community, information sharing among different IoT systems is often required [39]. Especially, for the smart device with mobility features, its authentication information is always required to be shared with other systems. Since there is no previous authorization information existing in the new smart system, the device information should be uploaded to the new system in order to get authorization again, which costs lots of time and energy. Moreover, in a smart community, the data safety cannot be guaranteed if the resource system sends the information to the target system directly since there is no uniform standard to judge the level of trust. Therefore, a information sharing center should be designed in the smart community for securing the personal data and the smart systems.

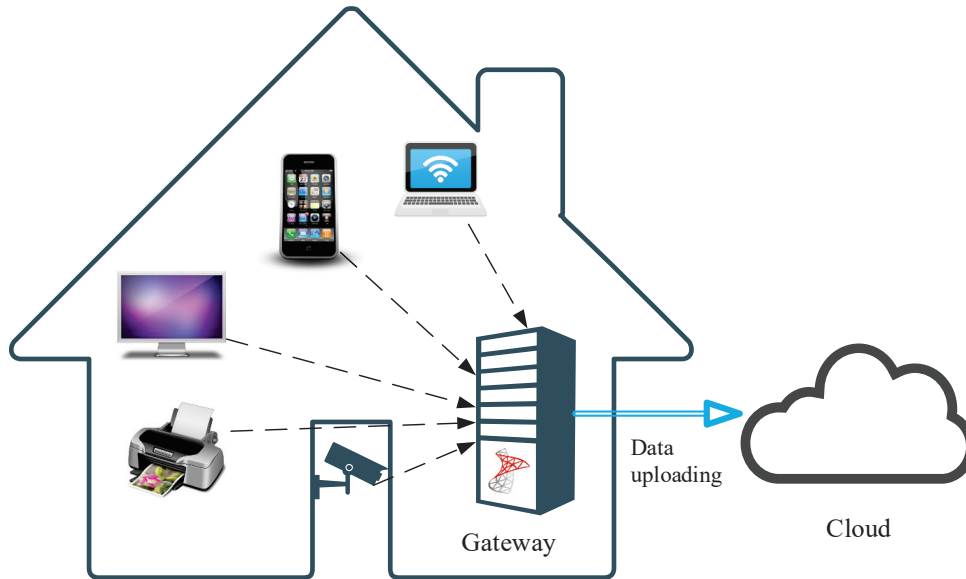


Figure 2.5: A smart home model where the gateway handles the local registration and authentication processes for each IoT device.

2.2.2 Existing Solutions

To solve the abovementioned authentication issues in IoT smart community, many studies have been investigated. The existing models for authentication process in smart community can be mainly classified into two categories, e.g. centralized model and decentralized model.

2.2.2.1 Centralized Information Sharing Server

Most of the existing structures in the real smart communities are using the traditional centralized model for the effective and efficient communication performance.

The typical smart community structure is usually composed of several smart sub-systems and a centralized information sharing server. Each smart sub-system provides the direct interaction with the local IoT devices through the gateway device, and the information sharing server is responsible for realizing information sharing among the sub-systems. The local IoT devices are connected to a gateway device by WiFi to form a Local Area Network (LAN), and the sub-system communicate with other systems through the gateway device by common TCP/IP Protocol.

Fig. 2.6 displays an existing centralized structure of an IoT smart community, where all

sub-systems rely on a powerful third party server to realize the information sharing service. The central third-party sever usually has high computational powers to handle all the information from the smart community, and the structure shows high efficiency in processing the data exchange and data analysis. A centralized model was proposed for IoT smart health scenario, in which the information of patients will be shared among different sub-system [40]. In each sub-system, a gateway is utilized for data analyzing and data forwarding to the information sharing center. The centralized information server is used for efficient information sharing and reaction. However, the centralized server could make the system under the risk of one-point failure [41]. If the center has been compromised, the security of personal data is threatened. More importantly, the centralized server could suffer from bottleneck communication when the number of shared information significantly increase.

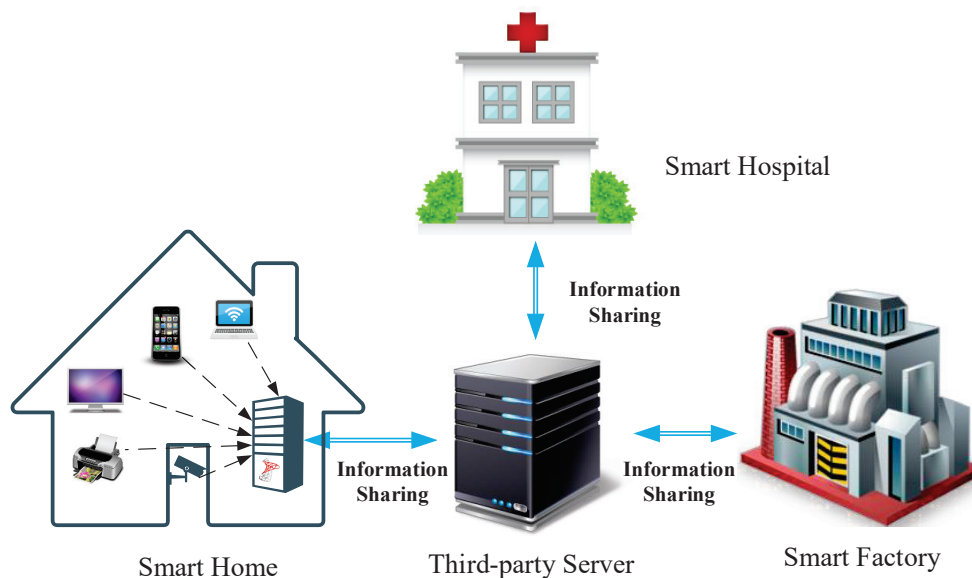


Figure 2.6: An IoT smart community where each smart system is centrally managed by a gateway, and all the systems rely on a third-party server for sharing information within the community.

2.2.2.2 Decentralized Information Sharing Server

The other category of authentication structure in IoT smart community is achieved through a decentralized model.

Although decentralized models were proposed for preventing the shortcomings caused by

centralized models, lacking of inside consensus mechanism will lead to malicious attacks among internal servers [42]. By reaching a consensus mechanism at each entity, a blockchain-based method proposed in [43] has been viewed as an alternative solution for solving these issues. Through establishing a blockchain in each gateway in smart systems, the blockchain-based method distributively manages authentication information and realize the authentication information sharing function. Fig. 2.7 presents the basic structure of this proposed blockchain-based method, in which each gateway are viewed as the mining nodes for the blockchain. In this way, the authentication information could be distributively saved and transferred among different systems. With the PoW consensus mechanism, a trusted relationship among each gateway from different sub-system can be built and the information shared can be trusted.

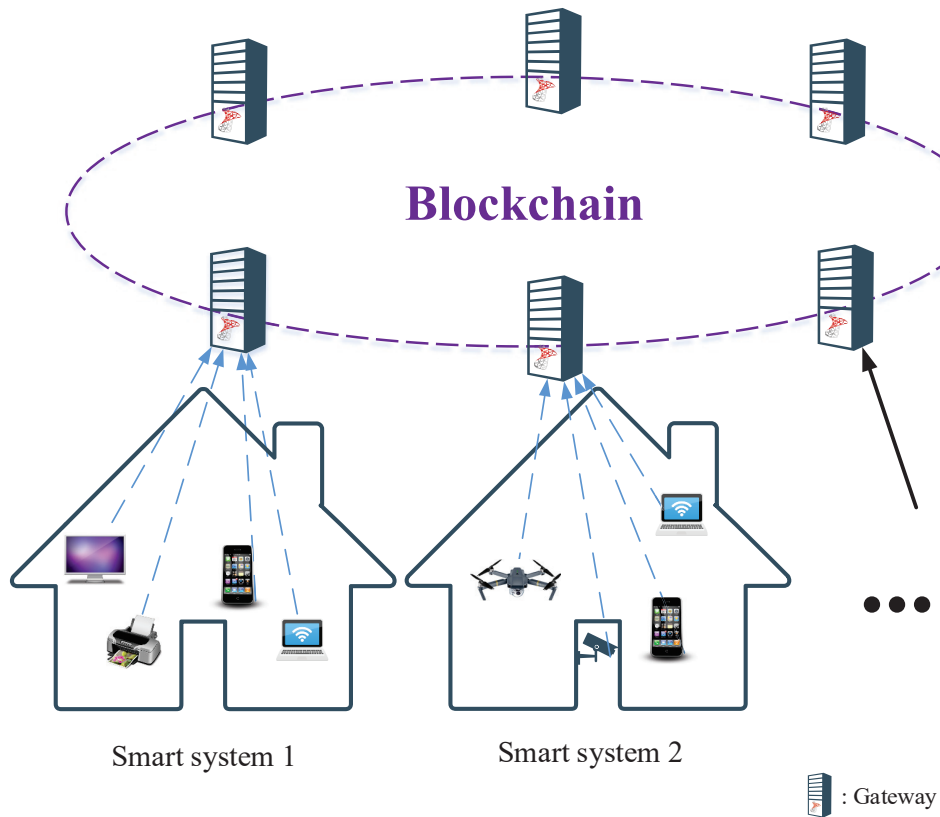


Figure 2.7: A Blockchain-based method for authentication process in IoT smart community.

Although this proposed structure makes the whole community as a decentralized peer-to-peer database for sharing information, each smart IoT system is still centralized for local authentication management. Instead of decreasing the burden of the gateway in each smart system, the overload of each gateway has been increased by processing additional information

caused by blockchain, which contains the authentication information from other smart systems in the community [43]. This centralized nature of gateways has a risk of one-point failure, which limits its application in IoT smart community due to the stringent QoS requirement. Moreover, there is a chance that the successfully registered device has been attacked to become a malicious device. In this case, the authentication information should not be shared with other systems due to the concern of information security. The proposed blockchain-based authentication method cannot prevent this risk because they did not provide a suitable evaluation for the information that is saved in the blockchain.

2.2.3 Analysis

Based on the analysis of these two categories of device authentication models in smart community, the decentralized authentication method with consensus mechanism is recommended due to its high security performance. However, there are two main issues that should to be handled.

Firstly, the burden of the gateway in each sub-system should be decreased for a better communication performance. The most promising solution is applying local blockchains at each smart system. Instead of implementing a blockchain which contains all the authentication information of all smart systems, the local blockchain only saves local device authentication information and processes local device authentication. A decentralized trustworthy database can be built among local mining nodes in each local blockchain which is guaranteed by the PoW consensus mechanism [44]. Thus, with using the local blockchain, the personal information in each sub-system can be securely managed and the overload of each gateway can be significantly decreased.

Secondly, there should be a suitable information evaluation criterion to judge if the required authentication information should be shared with other systems or not. It is normal in the smart community to have some IoT devices with mobility features, such as drones and community service robots. In this case, the authentication information should be allowed to be shared with other sub-systems. However, if the target device has already been attacked to become a malicious one, sharing its authentication information with other systems will threaten the information security of other systems by giving the direct writing and reading authorities to the

malicious device.

2.3 Chapter Summary

In this chapter, we mainly analyze the challenges and alternative solutions in IoT routing protection and device authentication process in IoT smart community.

For IoT routing protection, the IoT routing scenario has been fully introduced. Two main types of existing solutions are demonstrated: RPL based solutions and RM based solutions. Based on the comparison between these two methods, we recommended using RM method for IoT routing protection and then summarize two issues existing in RM method that should be further investigated. For the device authentication process in smart community, we firstly introduce the typical components of the smart system in the community and summarize the existing challenges. Then, two types of smart community models have been presented, which are traditional centralized model and decentralized model. After the presentation and comparison, we proposed to use decentralized model to overcome the challenges in device authentication process in smart community. Two main problems of existing decentralized model have been pointed out for further study.

Chapter 3

Blockchain Technology and Its Applications

As we previously mentioned in Chapter 2, with the increase of Internet of Things (IoT) devices, existing centralized networks can hardly manage the data security by presenting a single point of failure, a threat of data tampering. A peer-to-peer decentralized network is strongly needed in IoT, which can provide a symmetric relationship between the users and service providers.

Blockchain, as a decentralized database, offers a secure Peer-to-Peer (P2P) system in which distributed entities collaboratively verify and confirm all the transaction histories [45]. As an alternative to traditional centralized systems, blockchain has won the eyes of fields from both academics and industry professionals.

In this chapter, we provide a detailed review of blockchain component, namely transaction encryption, decryption and verification, and mining process. Two types of blockchain technology are then introduced, namely public blockchain and private blockchain. We also present the sidechain technology, an extended technology of blockchain, and compare with blockchain in terms of technical details and security performance. Furthermore, various promising applications that blockchain technology has been applied to are well demonstrated, including Internet of Things (IoT), data security and data sharing, identity management and medical applications, along with many other emerging applications. Finally, we mention several benefits and challenges in blockchain implementation for a wide range of practical applications.

The organization of this chapter is listed as follows. Section 3.1 introduces the overview

of blockchain technique. The detailed procedure and fundamental components of blockchain are presented. In section 3.2, both public blockchain and private blockchain have been investigated. Then, we introduced the sidechain technology in Section 3.3, including its structure and protocol. In Section 3.4, several promising fields for blockchain applications are summarized, such as crypto-currency, Internet of Things (IoT), and data security. After that, a pros and cons analysis of blockchain technique is presented in Section 3.5. Finally, conclusions are obtained in Section 3.6.

3.1 Overview of Blockchain Technique

Blockchain technology is a distributed database which shares transactions among all the members and nodes in its network with certain consensus mechanism [42]. Each block is linked to the prior one by the hash value of the block, which is shown as Fig. 3.1.

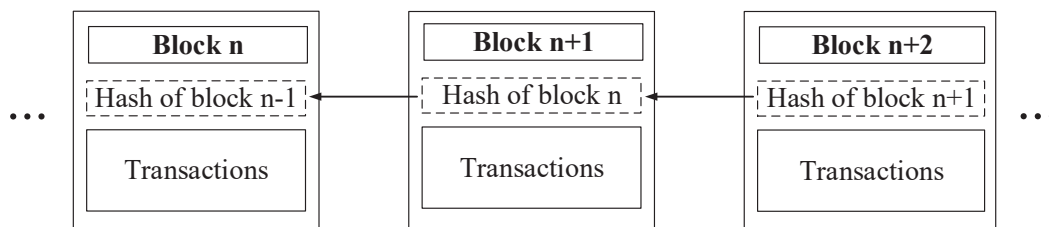


Figure 3.1: Basic structure of blockchain.

3.1.1 Key Pair and Signature Creation

For each entity in the blockchain network, it has a unique key pair of private key and a public key for identity use [46]. The private key is the key that entity needs to store by itself without letting anyone knows, while the public key is the key that is publicized to all users in the network.

When a new transaction is generated between two entities, a secure hash algorithm (SHA) will be applied to transfer the transaction into a message digest, which is the hash value that connects the blocks. Then, the message digest will be encrypted by its private key to form a digital signature, which can only be decrypted and validated by its public key. After that, the

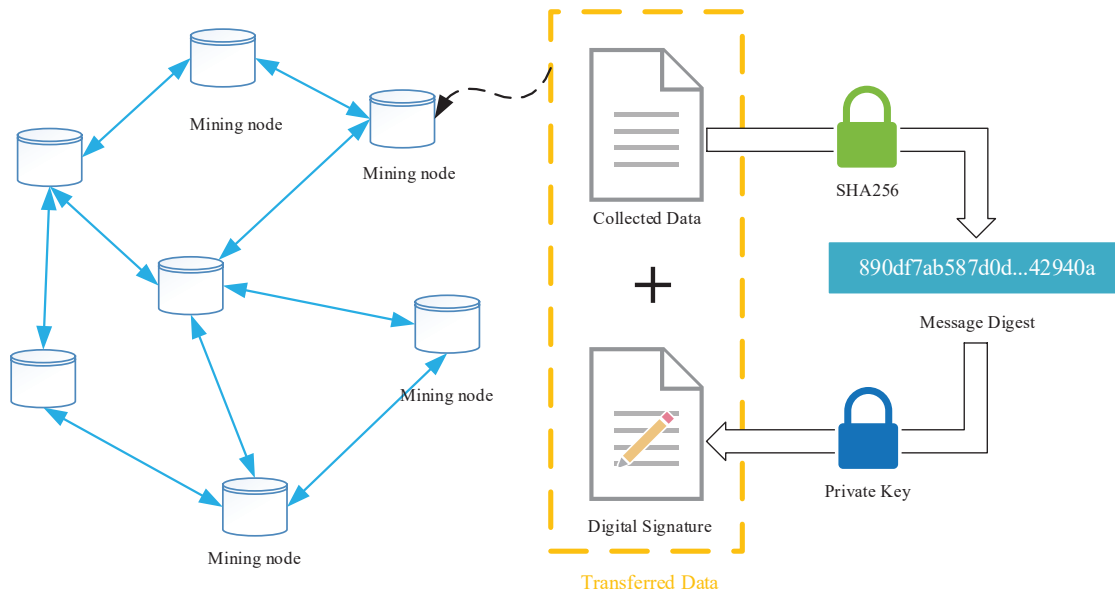


Figure 3.2: Procedure of the data encryption and broadcast.

transaction will be broadcast to all the blockchain members along with the signature waiting to be verified. The procedure of the transaction encryption is shown in Fig. 3.2.

3.1.2 Signature Verification

When other blockchain entities receive the broadcast information, they need to do the transaction decryption and signature verification to verify the information, as shown in Fig. 3.3.

The received transaction will be firstly hashed into message digest 1 and use the public key of the sender which they have already stored in the local database to decrypt the signature and get another message digest 2. If these two message digests are the same, this message is verified successfully. During the verification, only when more than 50 percent of the devices in this IoT network valid this transaction, this transaction is accepted [44]. Otherwise, this proposed one will be discarded [47]. Then, the verified transaction will be required to be mined for a certain period to be packaged into a new block and connect to the previous ledger.

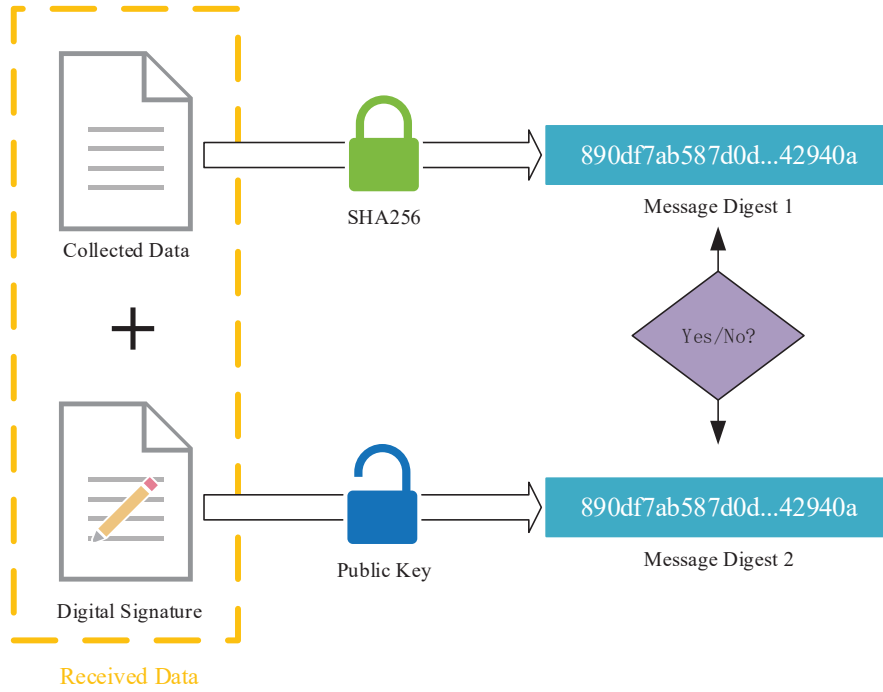


Figure 3.3: Procedure of the signature verification.

3.1.3 Mining Process

After several transactions have been verified by the whole network, a new block with five parts contained will be generated by miners, namely, the hash of previous, transactions, nonce value, timestamp and current hash. The following Fig. 3.4 shows the block contents. Miners are the entities who create and update the block to the whole network with high computational powers [44].

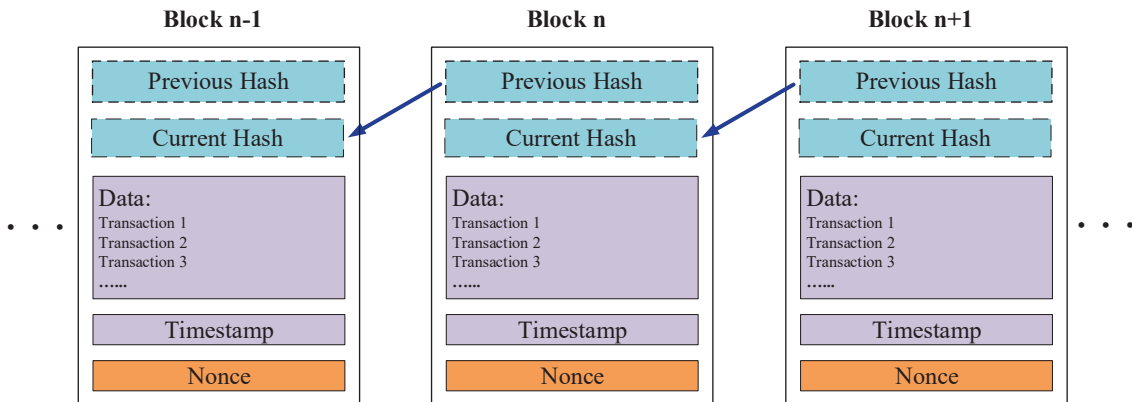



Figure 3.4: Detailed block contents and structure.

In this process, a consensus mechanism called Proof of Work (POW) has been applied to create a trusted relationship among all the users, which is the crucial element of the blockchain technology [48]. The concept of POW was firstly mentioned by Cynthia Dwork and Moni Naor in 1993. In 2008, Nakamoto Satoshi adopted the PoW method in Bitcoin systems to increase its security, and this makes the PoW method popular [49]. The purpose of POW is to prove the validity of the transaction of the new block. In the mining process, the miner needs to figure out a puzzle problem to provide a proof for the current block, as shown below:

$$\text{HashValue} = \text{hash}(\text{SHA256}, \text{hash}(\text{SHA256}, M)) \quad (3.1)$$

where M represents the data of this block, which includes transactions, timestamp, previous hash, current hash and nonce value. This equation presents that the total content of the block will be hashed twice, and the final hash value should meet the block difficulty requirement.

000000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb



The image shows a hexadecimal hash value: 000000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb. A blue bracket is drawn under the first 16 zeros (000000000000000000), with a vertical line pointing down to the text 'Block difficulty'.

Figure 3.5: Example of PoW consensus mechanism.

Fig. 3.5 shows an example of hash value, and the number of zeros in the beginning is the difficulty of the block generation. The puzzle problem is to find the correct nonce value for the current block to make sure that the final hash value can meet the block difficulty [49]. All the blockchain members will work individually to find the correct nonce by inserting input values one by one starting with 1. It should be noticed that the traditional mining process is a competition among all miners in the system, and the miner who gets the correct nonce value first will win the writing access for the blockchain. The whole procedure of PoW is shown in Fig. 3.6.

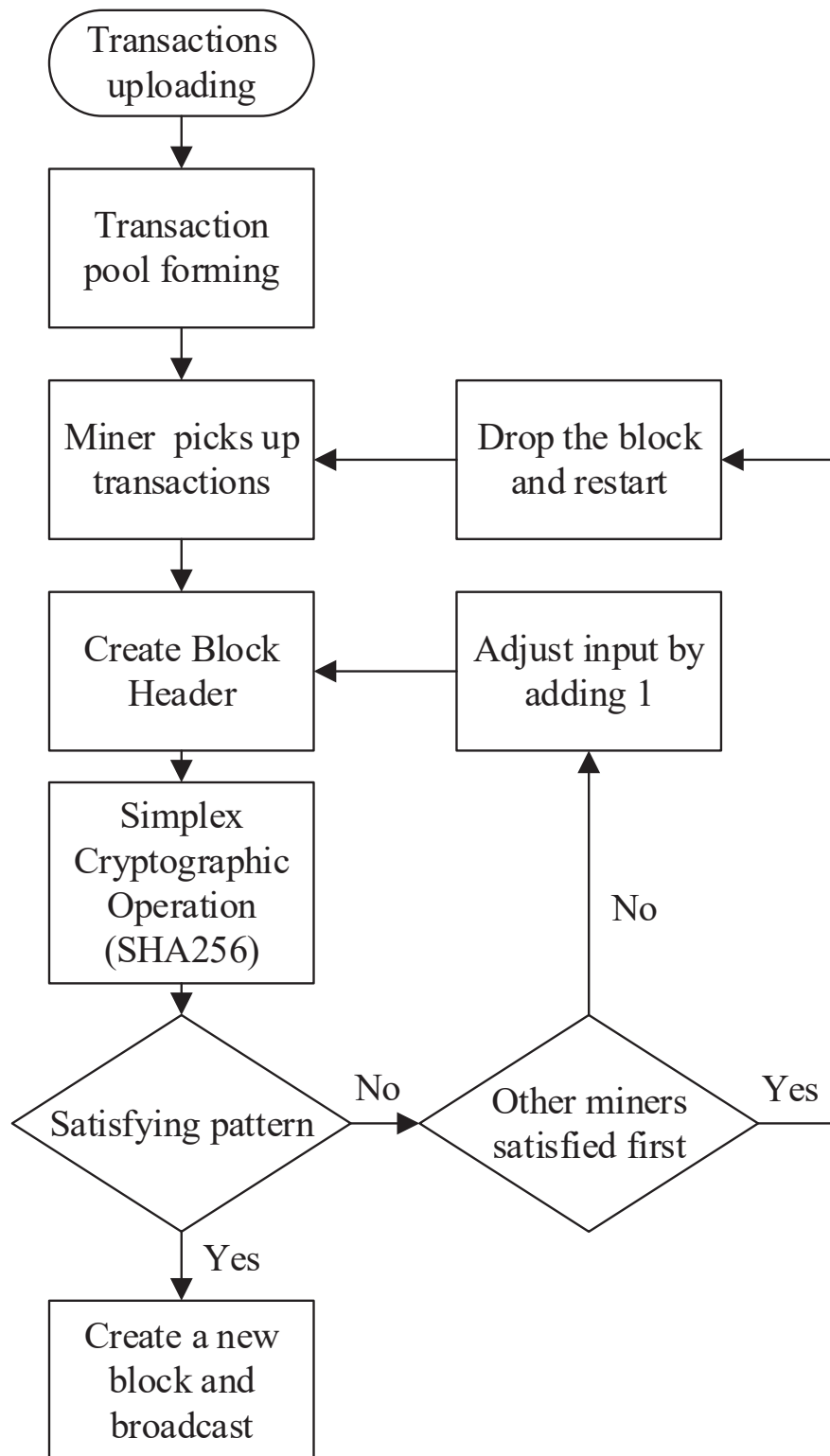


Figure 3.6: Flowchart of Proof of Work (PoW) mining process.

3.2 Type of Blockchain Technology

There are mainly two types of blockchain technology, namely, public blockchain and private blockchain [46].

3.2.1 Public Blockchain

The public blockchains are open source to all the entities of the network. This blockchain type allows anyone entity to participate as its user, miner or developer. All the transactions that saved on the public blockchains are fully transparent to every entity, which means every entity can read and write to the blockchain, such as Bitcoin and Ethereum. The benefits of the public blockchain are summarized as follows.

Decentralized Database: The public blockchain is designed to be a fully decentralized database. All the entity of the blockchain has the same authority to read and write the validated transactions.

Transparency and Immutability: The transactions on the public blockchain are transparent to all the users and the transactions cannot be changed or manipulated by any entity.

High Security Protection: 51 percent attack is one of the most typical blockchain attacks [35]. If the attackers can control more than 50% of computational powers in a Blockchain network, the attacker will have the ability to manipulate any data without the consensus of the community. The public blockchains usually have massive amounts of miners, which means it is impossible for attackers to control more than 50% of miners at the same time.

3.2.2 Private Blockchain

The private blockchains are closed source to a certain group of entities in the network, such as Ripple (XRP) and Hyperledger. In a private blockchain, a group of entities will be chosen to be the miners and only miners have the read and write authorities to the blockchain. For the rest users, they cannot read or write directly to the blockchain. They can only provide transactions

and get the instructions from the miners. The benefits of the private blockchain as summarized as follows.

Privacy Benefits: Since the transactions on the blockchain can only be viewed by the certain miners, the data privacy is selectively protected.

Efficient Services: The private blockchain is more centralized than the public blockchain. Due to a certain mining group in the network, the transaction processing is more efficient.

Energy Saving: Since the regular users in the private blockchain do not save or update the blockchain database, the energy could be saved for other communication.

3.3 Sidechain Technology

Sidechain technology, as an extended technology of blockchain, was firstly defined in 2014 for enabling bitcoin and other crypto-currencies to transfer money among multiple blockchains [50].

The structure of sidechain consists of a main blockchain with multiple small side blockchains. The main functions of sidechain are allowing the key information to transfer from one chain to others and reducing the burden of the main chain, which help the system to gain both agility and freedom of using multiple networks [51].

3.3.1 Sidechain Structure

The following Fig. 3.7 presents the basic structure of the sidechain structure. The sidechain structure consists of a mainchain and several side blockchains with different types of cryptocurrency used.

Both mainchain and side blockchains still flow the basic structure of blockchain technology, including the block structure, PoW consensus mechanism and new block generation procedure. However, in order to make transaction between mainchain and side blockchains, a

universal protocol should be applied for ensuring the operation of the system. In the following subsection, we will present this protocol of sidechain technology.

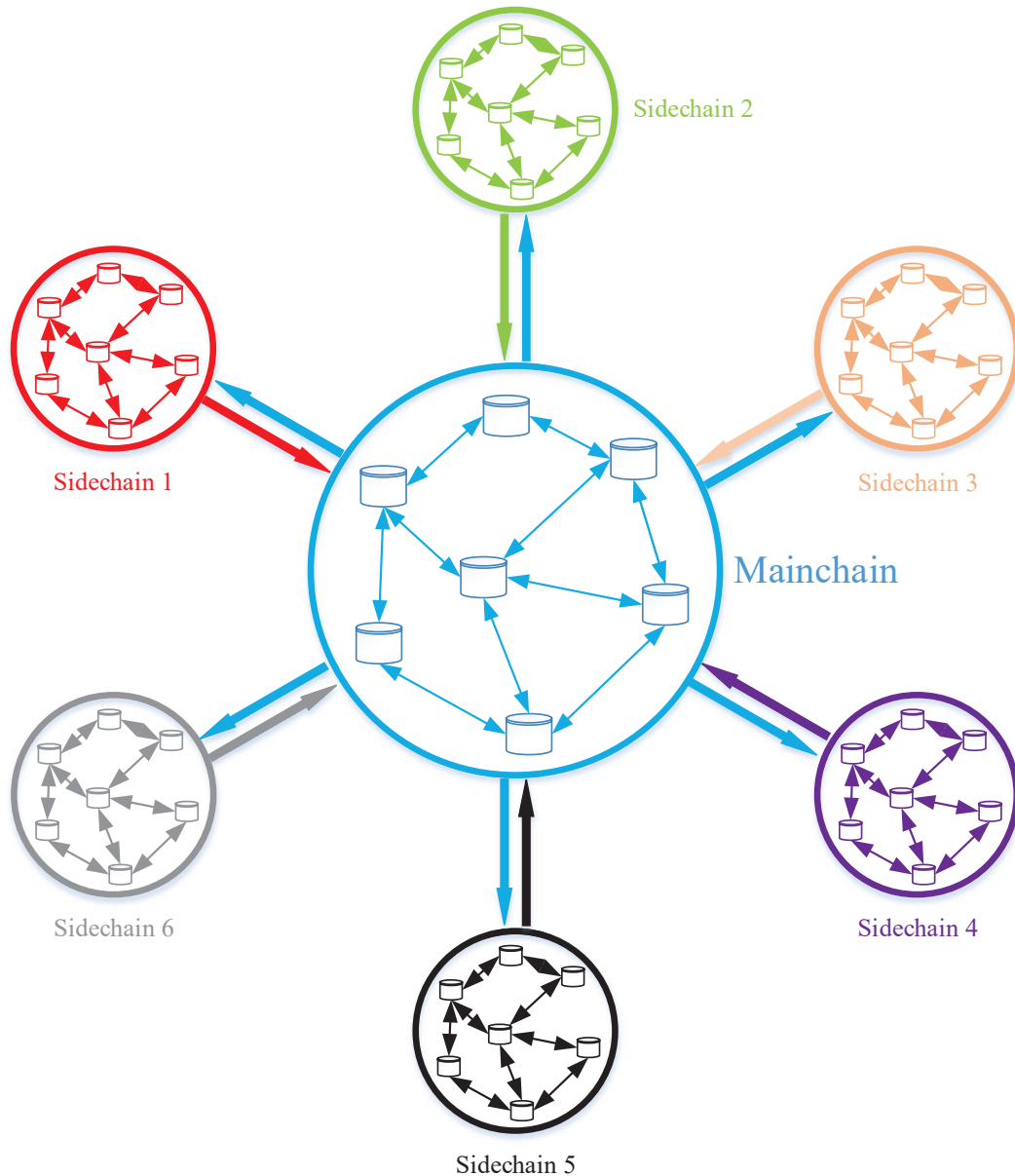


Figure 3.7: Structure of sidechain technology. The sidechain structure consists of a mainchain and several side blockchains. The crypto-currency used in each sidechain can be various.

3.3.2 Two-way Peg Protocol

Besides Proof of Work (PoW) consensus mechanism, a two-way peg protocol has been applied during crypto-currencies transfer between main blockchain and side blockchains for preventing

money double spending attack [52].

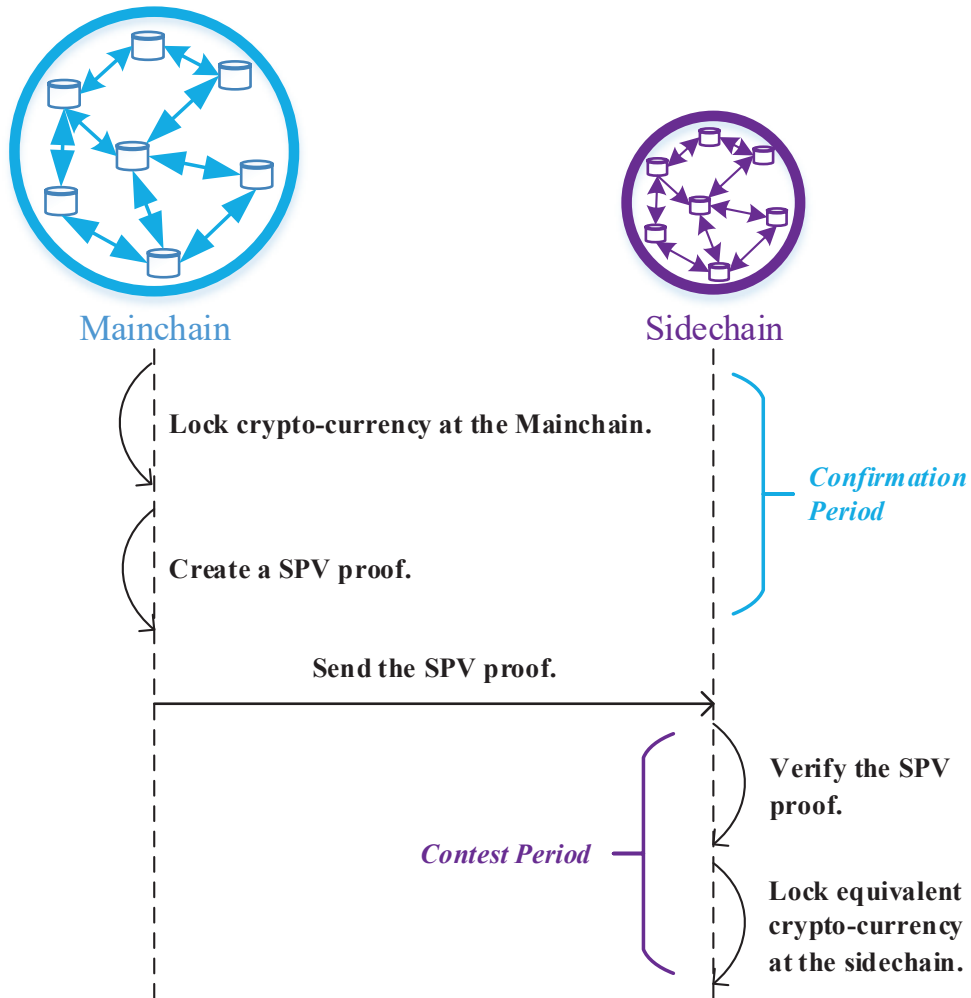


Figure 3.8: Procedure of the two-way peg protocol in sidechain technology.

The two-way peg protocol is used when a transaction happens between the mainchain and side blockchains [51]. The following Fig. 3.8 presents the protocol when mainchain needs to transfer crypto-currency to the sidechain. Like PoW in bitcoin, a Simplified Payment Verification (SPV) proof has been applied as the consensus mechanism for this procedure to prove that the message/ required crypto-currency has been locked. The SPV was firstly described in Satoshi Nakamoto’s paper [49]. Essentially, an SPV proof is composed of (a) transaction ID, (b) transaction ID list and (c) a list of block headers demonstrating PoW [50]. The SPV consensus mechanism allows the lightweight verifiers to check that some amount of work has been committed to the existence of an output without downloading the entire blockchain. Since

the SPV consensus mechanism only needs to download the block headers instead of the whole blockchain, it can provide an efficient tracking service in sidechain systems.

When the mainchain is required to transfer money to the sidechain, the coins of the main chain will be locked in a specific address and generate an SPV proof. Then the proof will be sent to the sidechain. Based on the verified proof, the corresponding crypto-currency will be unlocked in the sidechain. To synchronize these two chains, two waiting periods are defined: Confirmation Period and Contest Period [50].

3.3.2.1 Confirmation Period

The Confirmation Period of a transfer between mainchain and side blockchains is a duration for crypto-currency to be locked on the mainchain before it can be transferred to the sidechain. During this period, an SPV proof will be created and sent to the sidechain.

The aim of this period is to prevent the double spending attack at the mainchain. The Confirmation Period is a per-sidechain security parameter, which trades cross-chain transfer speed for security [50].

3.3.2.2 Contest Period

The Contest Period is the waiting period designed for the sidechain side, and in this duration, the newly-transferred coin cannot be spent on the sidechain until the Contest Period is finished.

The purpose of a Contest Period is to prevent double spending attack at the sidechain. In this period, the received SPV proof will be verified by the sidechain and corresponding crypto-currency will be unlocked to the receivers.

When a user wants to transfer coins from the sidechain back to the mainchain, they will follow the same two-way peg protocol as the original transfer: send the coins on the sidechain to an SPV-locked output, produce a sufficient SPV proof to the mainchain, and use the proof to unlock a number of previously-locked outputs with equal denomination on the mainchain.

Table 3.1: Comparison Results Between Blockchain Technology and Sidechain Technology.

	Blockchain Technology	Sidechain Technology
Purpose	Create a secure decentralized database	Transfer crypto-currencies between different systems
Technology Structure	One single chain broadcast to all the mining nodes	one mainchain and multiple side blockchains
Connection Method	Using hash function to connect blocks	Using the two-way peg protocol to connect the mainchain with the side blockchains
Consensus Mechanism	Proof of Work (PoW)	Proof of Work (PoW) Simplified Payment Verification (SPV)
Connection Speed	Calculating the nonce value during PoW	Confirmation Period and Contest Period
Fault Tolerance	System fails when more than 50% of mining nodes are compromised	Security faults on sidechain will not affect the security of mainchain.
Specific Attacks	51% Attack	Double Spending Attack Worthless Information Attack

3.3.3 Sidechain vs. Blockchain

In this subsection, we compare the sidechain technology with the blockchain technology in terms of the technical details and security performance. Table 3.1 illustrates the comparison results between blockchain technology and sidechain technology.

Based on the comparison result, it can be concluded that sidechain is a promising method for handling multiple networks in IoT environment. However, there are still some technical mechanisms that should be further adjusted for applying into the IoT network scenarios [53]. It should be also noted that there is a certain risk in sidechain technology that side blockchains keep sharing worthless information with the mainchain in order to disturb system operation. This attack will cause constantly increase of the system load, while the existing two-way peg cannot detect this attack[50]. If a mining node of sidechain has been compromised and performed worthless information attack by uploading authentication information of malicious devices to the mainchain, the security of the whole system will be seriously affected. Therefore, an optimized two-way peg protocol with information evaluation scheme is strongly needed in

order to apply sidechain technology into the IoT scenario.

3.4 Applications of Blockchain Technique

In this section, we introduce some promising applications of blockchain technology. Due to the increasing demands of decentralized network structures and decentralized security, blockchain application researches can be subdivided into several categories, namely crypto-currency, Internet of Things (IoT), Data Security and Data sharing, Identity Management, Medical Applications and others.

3.4.1 Crypto-currency

Blockchain technology was first designed to record transactions for securing crypto-currency in the financial industry in 2008 [49]. By using the PoW consensus mechanism, the blockchain technology provides a new thought of protecting the crypto-currency from the electronic fraud and double spending attack. Bitcoin, as one of the most famous applications of blockchain, has got a lot of attentions from Businessmen and scholars to deeply analyze the blockchain.

With the idea of sidechain coming out in 2014, different types of crypto-currencies could be efficiently transferred with each other. The appearance of sidechain technology promotes various forms of crypto-currencies and financial transactions. Now, people are still using blockchain technology and sidechain technology to redefine the crypto-currency and making profits on it.

3.4.2 Internet of Things (IoT)

As the number of IoT devices increasing, IoT networks call for both decentralized structure and secure environment, which blockchain technology is designed for. Due to the fact that most IoT devices have low computational powers and limited resources, the way of applying blockchain into IoT network should to be further considered.

The authors in [54] proposed a blockchain-based framework for IoT smart homes, and the system consisted of three parts, namely smart home, cloud storage, and overlay. Inside

the smart home, they proposed to implement a local blockchain to manage the security of local storage, local IoT devices and other local components. Paper [55] proposed a novel way of intrusion detection systems in IoT network called Lightweight Scalable Blockchain (LSB), which uses a distributed trust algorithm, to overcome the limitation of resources of IoT devices. They firstly divided IoT devices into clusters and each cluster has a cluster head (CH). In each cluster, only the CH has the right to manage blockchain and all the other nodes will be allowed to store one block for the CH to achieve a distributed database saving work. This method satisfied the purpose of decentralized database and the purpose of collaborating distributed works among nodes and sensors.

3.4.3 Data Security and Data Sharing

Considering the blockchain has the ability to secure the data with encryption technique and share data within its members, this technology has several applications in data management.

A new application of blockchain for the data encryptions was introduced in [56]. The authors came up with a distributed solution by combining the blockchain technology with traditional cloud server. Instead of registering drone itself to the blockchain, each hashed data would be collected from drone to the blockchain and then a blockchain receipt would be uploaded to the cloud server to reduce the burden of computation and improve the security of data collection. In [57], the authors demonstrated a novel way of using blockchain to protect the security of data sharing. The blockchain they designed accepted two types of transactions: (a) access control management transaction and (b) data storage and retrieval transaction. The users/ end devices are no long need to trust the third-parties to analyze the data since they have direct access to query the data through the off-blockchain storage solution.

3.4.4 Identity Management

Identity access control is a vital area for network security and data protection. The cryptographically secure identity of blockchain can be used to further enhance the identity check by using decentralized PoW consensus mechanism and transactions verification process.

A blockchain-based identity framework for IoT network was proposed in [58] called BIFIT,

which is an autonomous identity management system for IoT devices. They work utilized a global blockchain to obtain the signature of each device with both offline keys and online keys, which create subject appliance identities and establish devices owner identities. They also simulated a smart home testbed, and used the offline key pair to train the model and the online key pair to test the model.

3.4.5 Medical Applications

Since the medical history of each patient is private and sensitive, securing medical service data is crucial. By using blockchain technology, only the entity with the authorized key would be allowed to get access to the certain medical history, and only the medical history that validated by the authorized doctor will take effect in the medical blockchain database.

A blockchain-based framework for data protection during the health information exchange was presented in [59]. They assigned three cryptographic keys to each user/patient during the registration process, namely transaction private key, transaction public key and membership key. By applying the smart contract, the system can monitor the connection between the database layer and the user layer by setting the timers.

3.5 Analysis of Advantages and Disadvantages

Based on the blockchain process and its applications above mentioned, this technology does have advantages that could be utilized for enhancing the existing network structure. However, it still has disadvantages that should be mitigated in the designing stage [45] [46] [53]. In this section, we will analyze the pros and cons of blockchain technology.

3.5.1 Advantages of Blockchain Technology

Here, we summarize the three typical advantages of blockchain technology, namely, distributed architecture, transaction immutability and transaction transparency.

Distributed Architecture: For each authorized blockchain user, the position and right of managing the blockchain are equal, and no priority is existing. Thus, by applying PoW consensus mechanism, the blockchain technology can provide a secure P2P architecture, which is a distributed framework.

Transaction Immutability: Transaction immutability is the core function of the blockchain technology. Once the data has been validated and saved in blockchain, the information cannot be erased or modified due to the nature of blockchain design. In other words, the data saved in blockchain is irreversible. Therefore, when it comes to protecting the truthfulness of information, blockchain technology is an appropriate choice.

Transaction Transparency: Transaction transparency is another significant feature of the blockchain technology. Due to the fact that all the blockchain members share the same ledger and get updated after each block verification process, the transactions in each block are transparent and can be extracted by each entity for checking purpose.

3.5.2 Disadvantages of Blockchain Technique

Blockchain technology is not a perfect technology because it still has some drawbacks to address in order to be applied in other networks. Here, we mention two main disadvantages, namely, transaction delays and security vulnerabilities.

Transaction Delays One of the biggest drawbacks of the blockchain technique is the time relay during the process of traditional PoW consensus mechanism in new block generation. In order to overcome this issue and apply the blockchain technology into the IoT environment, suitable changes to the traditional PoW consensus mechanism are needed.

Security Vulnerabilities There have plenty of security attacks for blockchain technology, such as 51 percent attack and double spending attack. For the 51 percent attack, the attackers could manipulate any transaction without the any consensus mechanism if they can control more than 50% of computational powers, which will totally threaten the data reliability of the

system. For the double spending attack, the business thieves steal the crypto-currency after they take control the blockchain. They would create a copy of the currency transaction to make it look legitimate, or might erase the transaction altogether. This type of attack usually happen at token-used blockchain system. Therefore, avoiding certain blockchain attacks is necessary when designing the blockchain-related networks.

3.6 Chapter Summary

The new thought of decentralized network by using blockchain technology is getting more mature and well implemented in the real-world day by day. The trust relationships can be established among untrusted entities in blockchain through the PoW consensus mechanism, which can provide more security protections for the decentralized database. However, in order to fit different network environments and performance requirements, the principle and framework of blockchain should be further studied and designed. In this chapter, we introduced the basic components of blockchain technology and showed the details of new block generation process. Both public blockchain and private blockchain are summarized and compared. We then presented the sidechain technology, including its network structure, two-way peg protocol and comparison results with blockchain. After that, we presented several popular areas where blockchain technology has been applied on. Finally, we mentioned some benefits and challenges of the blockchain technology. We hope that this comprehensive literature review of blockchain technology can provide a roadmap for blockchain-based application developments, and aid researchers in considering directions for valuable research in the future.

Chapter 4

Blockchain-based Distributed Reputation Management System for IoT Routing Protection

4.1 Introduction

With the proliferation of IoT devices, many emerging industrial and consumer-related applications are relying on massive amounts of IoT data on a continuous basis, leading to increasing requirements on communication and data security [60]. Due to the computational and hardware related constraints, IoT communication devices and network facilities have many security vulnerabilities [61]. Specifically, due to the lack of self-protection mechanisms, many IoT routers are very vulnerable for malicious cyber-attacks. Thus, routing process protection in IoT networks is critical for stringent Quality of Service (QoS) provisioning required by IoT applications, especially data security and privacy-preservation [62]. A compromised router in an IoT network could act maliciously by selectively dropping packets and rejecting data forwarding services. Although existing Reputation Management (RM) systems are useful in identifying misbehaving routers, the centralized nature of the RM center has the risk of one-point failure.

Several workable existing solutions have been summarized in chapter 2 and they did not achieve a secure protection for IoT routing. The emerging blockchain technology, with the

inherent decentralized consensus mechanism, provides a promising method to reduce this one-point failure risk. Thus, we propose a blockchain-based distributed reputation management system for routing protection in IoT networks to overcome the abovementioned challenges. The proposed scheme utilizes the blockchain technique as a decentralized database to store router reports for calculating reputation of each router. A corresponding reputation calculation method in IoT environments is developed to evaluate the trustworthiness of each router. The proposed scheme also adopts two criteria of evaluating the centrality of routers for misbehaving router detection. To apply the proposed RM scheme in IoT networks, an efficient group mining process is designed for reducing the complexity of blockchain technique.

The rest of this chapter is organized as follows. In section 4.2, the adversarial model is first defined. The proposed blockchain-based distributed RM scheme and efficient group mining process are then demonstrated in section 4.3. The model analysis is presented in section 4.4. In section 4.5, the simulation results of the proposed scheme are presented. Finally, the chapter is concluded in section 4.6.

4.2 System Model

An adversarial blockchain-based reputation management system in IoT system is shown in Fig. 4.1. In assisting the subsequent analysis, the IoT network system considered in this chapter consists of four layers, namely, end-user device layer, routing layer, edge server layer and cloud server layer. The proposed RM model is designed for medium and large routing networks, and the network should have enough router number to provide routing reports for each data forwarding service.

The model in Fig. 4.1 illustrates an adversarial routing process in an IoT network, where the end-user devices try to upload data to the cloud server through the routing layer in the presence of a malicious router. Specifically, the malicious router attempts to provide the routing service for the data uploading process with data packet dropping/selfish behavior in order to disrupt the IoT network. By applying the blockchain technique at the edge layer, the malicious router can be detected and isolated.

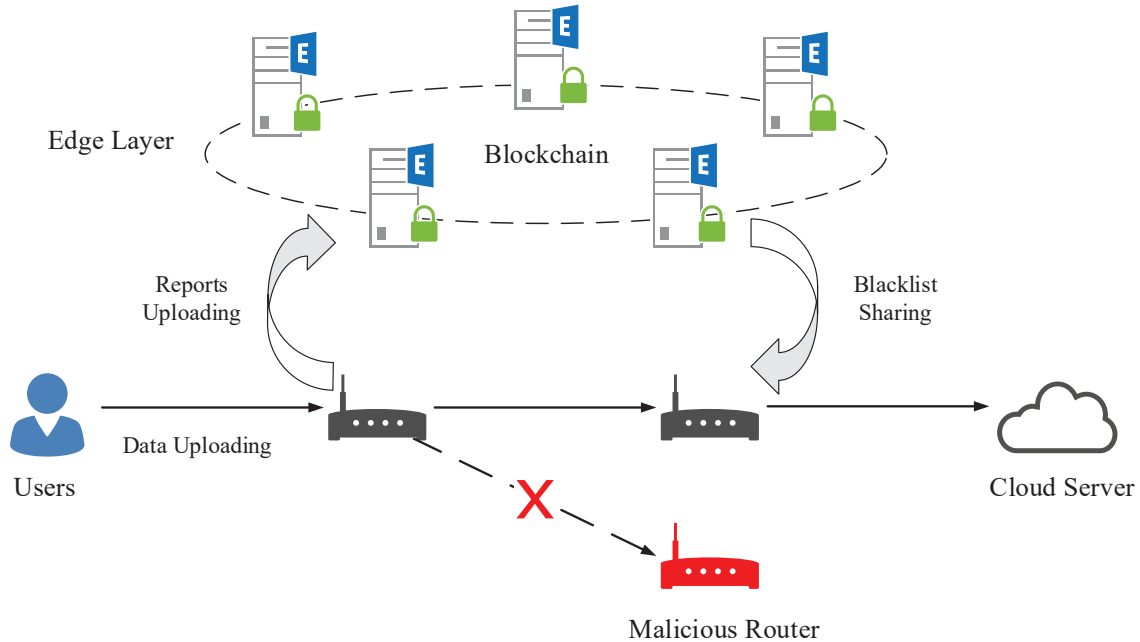


Figure 4.1: Adversarial blockchain-based reputation management system in IoT networks. The data link between the users and cloud server suffers from malicious routers.

4.3 Proposed Scheme

4.3.1 Blockchain-based Reputation Management System

Considering the low latency of edge server and the low latency tolerance of reputation management, we deploy the proposed blockchain-based RM system at the edge server [63] [64]. The computational requirements, communication overhead and storage overhead will be analyzed in the next subsection.

The proposed reputation management scheme consists of the 4 steps as follows:

Distributed Information Collection from Neighboring Routers: When a router helps forwarding the data packets, its neighboring routers will be required to report to the nearest edge server for the purpose of reputation management. In achieving this goal, the report will consist of the report router ID (the router which uploads the report), the reported router ID (the target router), number of requested packets, and number of forwarded packets.

Routing Service Evaluation: The reports collected from distributed routers will be viewed as transactions for the blockchain ledger and will be verified before appending to a new block in the blockchain. Based on these reports, the packet delivery ratio (PDR) will be calculated by the edge server based on equation (4.1).

$$PDR = \frac{\text{Number of forwarded packets}}{\text{Number of requested packets}} \quad (4.1)$$

By setting a successful delivery ratio threshold, this routing service will be identified as cooperative or uncooperative. We set 1 to represent for cooperative feedback and -1 for uncooperative feedback. The transactions will then wait for the block verification process.

Router Reputation Calculation: Once a new block has been verified and added into the blockchain ledger, the reputation value corresponding to relative routers will be calculated based on the following formulas. Here we employ centrality value (CV) to indicate the importance of a target router under evaluation to an evaluating router and the whole system. For instance, the routers which provided a large amount of services or have frequently interacted with other routers are viewed as central roles with high centrality value in this network. We defined two kind of centrality values: $CV(a, b)$ is the centrality value of the target router b to an evaluating router a , which can be used to prevent the malicious routers from building up many relationships with other routers with high trust; $CV(b)$ is the centrality value of the target router b to the whole system, which can ensure the reports from central routers weight more than others.

These two centrality values used in this model can be computed using the following equation (4.2) and (4.3):

$$CV(a, b) = \frac{N_{a,b}}{N_a}, \quad (4.2)$$

where $N_{a,b}$ is the total number of reports uploaded from router a regarding the previous routing behavior of router b . N_a is the total number of reports that router a has uploaded.

$$CV(b) = \frac{S_r + S_s}{2 * N_r}, \quad (4.3)$$

where S_r is the total number of times that router b has been reported when router b is providing a routing service. S_s is the total number of times that router b has acted as a routing evaluator to report other routers' behavior to the edge server. N_r is the total number of current received reports.

When a new report has been appended into the ledger, the reputation value for the associated router will be updated. Let $R_i(b)$ represent the reputation value for router b , and the reputation update function is shown as the following equation (4.4).

$$R_i(b) = R_{i-1}(b) + (f(i) - R_{i-1}(b)) * R_a * (\alpha * CV(a, b) + \beta * CV(b)), \quad (4.4)$$

where $f(i)$ is the feedback value calculated based on the reporting router a uploaded. $R_{i-1}(b)$ is the previous reputation value of the target router b . R_a is the reputation value of evaluating router a . Both α and β are weight factors to balance these two centrality values.

Misbehaving Router Blacklisting: With the proposed distributed RM scheme, the router's reputation value will keep gradually increasing when it acts cooperatively during the routing process. On the contrary, if the router behaves maliciously, its reputation value will decrease dramatically. When its reputation value falls below a certain threshold, its router ID will be blacklisted by the blockchain-based edge server, and the blacklist will be broadcast to the routing layer to isolate this router.

4.3.2 Efficient Group Mining Process

As previously mentioned in Section 3, Proof of work (PoW) is the most important method of the blockchain technology, which ensures high security of the decentralized database.

During the PoW mining process, the miners (mining nodes) need to figure out a puzzle for validating the current block they are working on [44]. The puzzle is shown as following:

$$HashValue = hash(SHA256, hash(SHA256, M)) \quad (4.5)$$

and

$$\text{HashValue} \leq D, \quad (4.6)$$

where M represents the message of this block, which includes transactions, timestamp, previous hash, current hash and nonce value. D is the difficulty of creating one block.

The puzzle in equation (4.5) and (4.6) is to find the correct nonce value to make sure that the final hash is less than the given target D , which is the difficulty for making a new block [18]. All the blockchain members will work individually to find the correct nonce by inserting input values one by one starting with 1. It should be noticed that the traditional mining process is a competition among all miners in the system, and the miner who gets the correct nonce value first will win the writing access for the blockchain. The winner mining node will add the new block to the blockchain and update the blockchain to every mining node of the blockchain system.

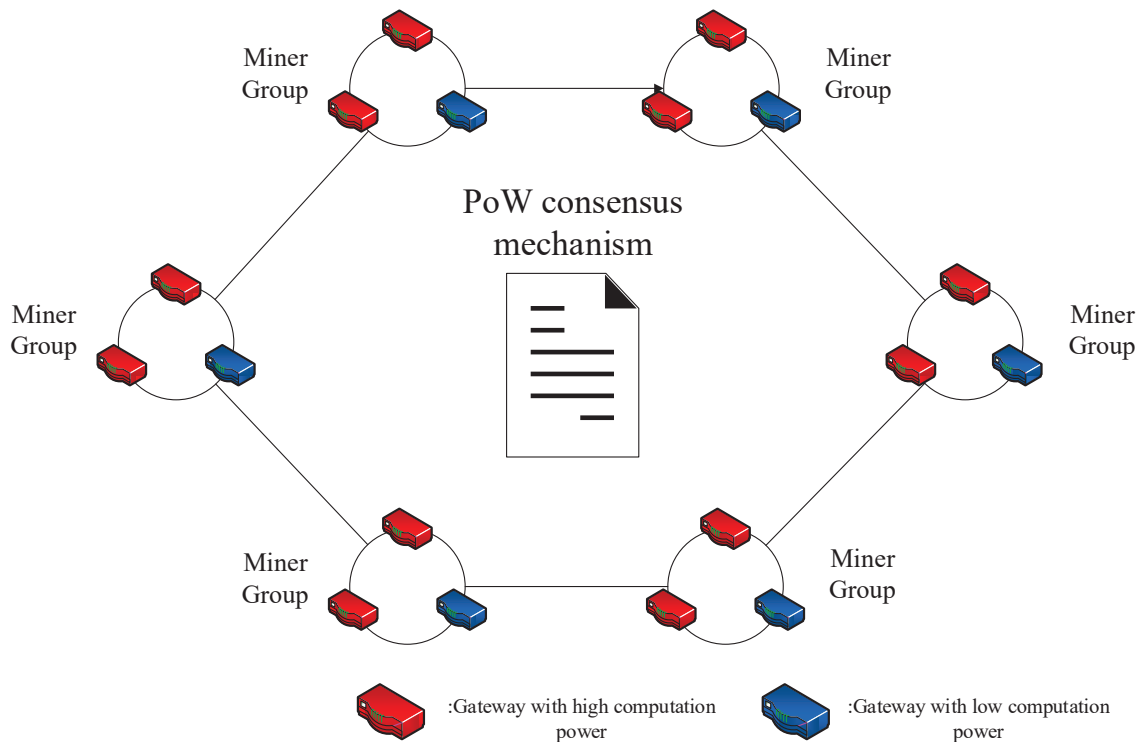


Figure 4.2: Model of proposed group mining process, in which edge devices with high computational power will be required to group to edge devices with low computational power.

Due to the limited resources of IoT devices, it is hard to achieve the traditional PoW process among IoT devices. In order to fix this issue, we propose an efficient group mining for

blockchain, which is shown in Fig. 4.2. Instead every miner working on their own block, all miners will be separated into several groups based on their heterogeneous computational powers and their locations. The miners with high computational powers will be required to group with members with low computational powers so that the average computational power for each group is balanced and the mining competition is fair for each group and device. The purpose of balancing the computational power is to prevent the 51 percent attack [35]. For instance, there will not be a case where a powerful mining group can control more than 50% of computational powers and manipulate the content of the blockchain.

In the proposed group mining process, all mining groups will share the same blockchain and use the hash of the latest block as a reference to create a new block. Inside each group, a group leader will be chosen each round, which will lead the group to mine the block each time. As shown in Fig. 4.3, the group leader will pick transactions from the transaction pool and generate a genesis block. The genesis block only includes the picked transactions, previous hash, and leaves the rest elements empty (current hash, timestamp and nonce). This genesis block will then be multicast within its group so that every group member will have the same task working on. Each group member will be assigned a certain part of nonce range by the group leader each time based on their different computational power. The way of calculating the total nonce value range of a new block is presented in equation (4.7) [65].

$$n \leq \frac{2^{256}}{H_d}, \quad (4.7)$$

where n is the nonce value range and H_d is the difficulty of creating one block.

Then, starting from the lowest value within their allocated nonce value range, each group miner will search for the correct nonce value. If the input nonce value does not satisfy the equation (4.5) and (4.6) after applying the SHA256, the input value will be added by 1 and re-input. This procedure will continue until the miner finds the correct nonce or reaches the end of allocated range.

When a mining node in this group succeeds in its mining process, the correct nonce value will be multicast within the group and all group members will verify the nonce value by checking the SHA values. If the received nonce value is correct, the new block will be multicast to

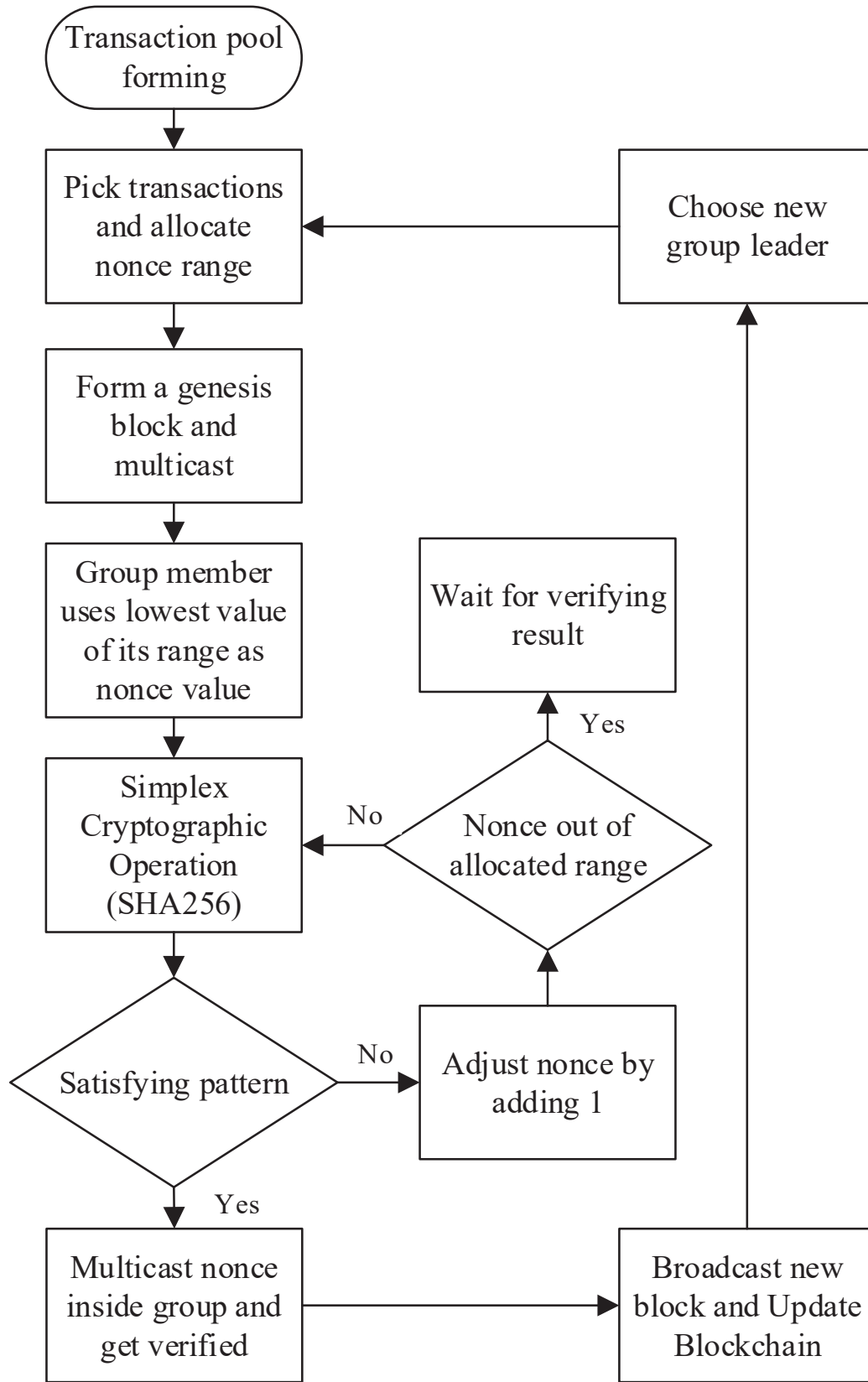


Figure 4.3: Flowchart of the proposed group mining process.

other mining groups and all groups will update the blockchain with the new block. Then, the one which finds the correct nonce value will be chosen as the new group leader for the next round, and the rest group leaders will not be replaced. The initialized group leader for each mining group will be the device with the highest computational power in that group.

4.4 Model Analysis

In this section, we prove the applicability and realizability of the proposed Blockchain-based RM system by comparing the technical details with existing models and analyzing the system overhead.

In order to express the benefits of the proposed model, we compare the proposed group mining blockchain model with the traditional blockchain technology used in Bitcoin system, and an existing blockchain model mentioned in paper [33].

4.4.1 Technology Comparison

The following Table 4.1 presents the technology comparison results among abovementioned three blockchain-based models in terms of technical details and security vulnerabilities. As we can see from the table, the traditional blockchain technology is designed for crypto-currency and it suffers from double spending attack due to the nature of token-used systems. Whereas, the existing blockchain model and the proposed model are both non token-used systems and are aimed to simplify the mining procedure in order to apply in the IoT networks. Compared with the existing cooperative mining blockchain model, the proposed model in this chapter has less possibility of suffering from the 51% attack due to the computational powers balance rule of the group mining process. Moreover, it has a more efficient mining task allocation scheme to ensure the efficiency of block generation. Therefore, the proposed blockchain model shows its superiority in efficient mining process and attack defense ability compared with other two models.

Table 4.1: Comparison Results Between The Traditional Blockchain Technology, Existing Blockchain Model and the Proposed Blockchain Model.

	Traditional Blockchain Technology in Bitcoin System	Existing Blockchain Technology in IoT Networks	Proposed Blockchain Technology in This Chapter
Member Permissions	Public Blockchain (Every entity can read and write)	Private Blockchain (Only mining nodes can read and write)	Private Blockchain (Only mining nodes can read and write)
Transaction Content	Crypto-currency	Collected data	Collected data
Transaction Relationship	Continuously; Related	Independent; Unrelated	Independent; Unrelated
Consensus Mechanism	PoW	Cooperative Mining Pow Process	Group Mining PoW Process
Reward to Mining Nodes When Succeed in Mining	Certain mining fees will be paid to miners	No	The mining node will be chosen as the group lead of the mining group
Double Spending Attack	Yes	No	No
51% Attack	Less possible	High possible	Less possible

4.4.2 Overhead Analysis

In this section, the overhead analysis of the proposed blockchain-based RM system has been studied from three aspects: computation requirements, communication overhead and storage overhead.

4.4.2.1 Computation Requirements

In the proposed work, most of the computation is required at the mining node for 1) mining process; 2) reputation calculation for each router. For the mining process, we conduct the blockchain onto the edge server for faster transaction verification speed and higher throughput of data. More importantly, following the group mining rule, we set mining nodes into groups to mine a same block for reducing the computational overhead at each node. Thus, the computational overhead should not be a factor limiting the application of the proposed blockchain-based

RM model. In order to detect the malicious routers in the network, the reputation of router is periodically calculated and updated. The traditional indirect/direct evaluation mentioned in [26] [27] is computationally expensive at each device and will limit the applicability of the RM systems. Thus, we propose a lightweight algorithm to evaluate the trustworthiness of the IoT routers from a global view to reduce the computation overhead caused by individual evaluation. The algorithm utilizes two categories of router centrality as the criteria for the evaluation, and its detection performance is presented in Section 4.5.2.1.

4.4.2.2 Communication Overhead

After analyzing the computation requirements in the previous subsection, we now investigate the communication overhead (CO) for the blockchain-based RM model. As we previously mentioned in Chapter 3 about the blockchain technology, each information packet transmitted to the blockchain includes a transaction (a routing report in our case) and a corresponding signature signed by the private key of the source node. Thus, the total communication overhead of a routing packet P transmitted to the edge device server is given as follows:

$$CO_{total}(P) = CO_{Report}(P) + CO_{Signature}(P), \quad (4.8)$$

where $CO_{Report}(P)$ is the communication overhead caused by the transmitted routing report and $CO_{Signature}(P)$ is the communication overhead caused by its corresponding signature.

As mentioned in Section 4.3, a routing report contains a report router ID, a reported router ID, the number of requested packets and the number of forwarded packets. The average size of a routing report is calculated as 36 bytes [66]. Since we use a 32-bit modulus for the signature in the SHA 256 encryption, the size for a signature is 4 bytes. So, for each transmitted packet, the per-hop communication overhead of the packet transmission in the proposed RM system is $36 + 4 = 40$ bytes. For a path of H intermediate hops, the total communication overhead for all transmitting routing reports is $40H$ bytes. For a case with 10 intermediate hops, the total communication overhead at the edge server side is 400 bytes/packet. For an IEEE 802.11 system, this is about 17.36% of the maximum MSDU (2,304 bytes). Therefore, the proposed RM system will not be limited by the communication overhead caused by routing reports.

4.4.2.3 Storage Overhead

As mentioned in Chapter 3, each mining node is required to store its own private key, the public keys of all the entities, and the blockchain information. In the proposed blockchain-based RM system, we use 32-byte private key and 32-byte public key for each router. Therefore, for a routing network with N routers, each edge mining device should have $32N + 64$ bytes for the key storage.

In order to calculate the storage size of the blockchain information, the size for each block component of a blockchain is summarized in Table 4.2 [67][68].

Table 4.2: Memory Size for Each Block Component of a Blockchain.

Blockchain Component	Size (bytes)
Previous Block Hash	32
Transaction	36
Time stamp	4
Nonce	4
Current Block Hash	32
Rest of a Block (Transaction Counter, Difficult Target)	12
Block Counter	4

Since SHA 256 can encrypt any size plaintext/transaction into a fixed size 256-bit cryptographic hash, the size for hash value of a block is always 256 bits/ 32 bytes [67]. In the bitcoin blockchain, the average transaction size is assumed to be 400 bytes [69]. Whereas, in our IoT scenario, the transaction is the routing reports, which is set to be 36 bytes per report. Thus, for a blockchain network with B blocks (blockchain size) and D transactions in each block (block size), the size of the blockchain is $(84 + 36D)B + 4$ bytes. For example, for a network with 1000 devices, the blockchain size is 1000 and average block size is 10, the total storage overhead would be $[(84 + 36 * 10) * 1000 + 4] + (32 * 1000 + 64) = 476068$ bytes, which is 464.91 KB. For edge device server, the average storage capacity of each device is assumed to be 100 GB [70]. Thus, the storage overhead caused by the proposed blockchain-based RM is affordable as it costs approximately 0.000443% of the storage size of the edge device.

4.5 Performance Evaluation

This section evaluates the performance of the proposed blockchain-based RM system in terms of 1) attacks detection performance, 2) RM system convergence performance and 3) robustness and efficiency performance.

4.5.1 Simulation Settings

We carry out our simulation experiments in MATLAB. We simulate 50 routers for evaluating the performance of attacks detection and RM system convergence performance. The routers number chosen here could provide enough routing reports for the reputation calculation scheme, and we compare our model with three existing RM models. Then, we further test the RM convergence performance against different network sizes. In order to evaluate the blockchain efficiency compared with existing works, 100 routers are simulated.

Table 4.3: System Settings Comparison and Parameter Settings.

	Traditional Blockchain	Voting Blockchain	Group Mining Blockchain
Mining Members	All nodes	Cluster head nodes	Edge devices
Percentage of Miners	100%	20%	20%
Mining Groups	No	No	Four groups
Voted Transaction before Mining	No	All nodes vote	All edge devices
Hash Value Verification	Happens during block verification	Happens during block verification	Happens within mining group
New Block Verification	All nodes	All miners	Same group miners
Broadcasting New Block	To all nodes	To all miners	To other mining groups
CPU Frequency of IoT Nodes(GHZ)	Between 1 to 2.8	CH nodes: 2 to 2.8 Other nodes: 1 to 2	Edge devices: 2 to 2.8 Other nodes: 1 to 2

All routers are classified into two types, i.e. normal routers and malicious routers. Normal routers will cooperate during the routing process and will be accepted by the system while still

under monitoring by the RM system. In contrast, malicious routers provide ineffective routing process and will be eventually isolated by RM based on their malicious behaviors detected. All the experimental results are averaged over 30 runs and initialized reputation values for all routers are set to be 0.5. The experimental parameters for analyzing the blockchain efficiency are summarized in Table 4.3.

Since different IoT nodes have different computational powers to process the transactions, we need to set different CPU frequency for high computational nodes and low computational nodes in order to evaluate the performance of block generating process. The CPU frequencies of mining nodes are set between [2GHZ, 2.8GHZ], and CPU frequencies of the rest of nodes are between [1GHZ, 2GHZ] [71]. We assume that each routing report (blockchain transaction) is 36 bytes, 100 cycles per byte for each nodes and 5 transactions for each block (block size).

4.5.2 Analysis of Experimental Results

4.5.2.1 Attack Detection Performance

In the first experiment, we focus on analyzing the performance of attack detection. We have studied mainly two types of routing misbehaviors, namely packet dropping and selfish behavior.

Packet dropping attacks interfere the IoT routing process by selectively dropping packets in order to increase the packet loss rate, It is a common router's malicious behavior, but it is hard to detect and control in the IoT system. In the first test, we simulate the packet dropping attacks in routing process, and the results are shown in Fig. 4.4. In the test, We use four routers with different levels of packet loss frequency to show the performance of the proposed blockchain-based RM system in terms of malicious routers detection. For the first 10 transactions, we set all routers as general routers in order to gain routing histories from other routers for initialization. Then, their malicious behaviors start during the following 30 transactions. We can observe from Fig. 4.4 that the router with zero packet dropping attack frequency gains trusts from others, and its reputation increases steadily and slowly. On the contrary, for those routers with packet dropping behaviors, their reputation values decline continuously. When their reputation values are less than the certain threshold, the routers will be identified as the malicious routers

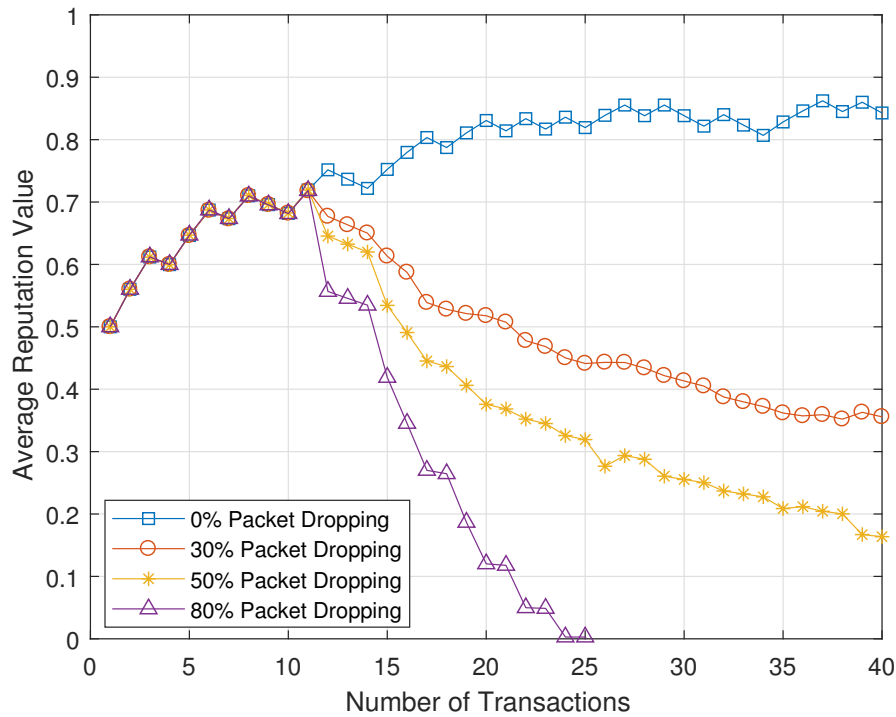


Figure 4.4: Packet dropping attacks detection for different malicious levels.

by the proposed RM management system. As a result, their device IDs will be put onto the blacklist and isolated from other routers.

Selfish router, as a common type of malicious misbehaving router, keeps refusing packets delivery in order to break down the network and save its own energy. We also simulate the selfish behavior attacks in our system, and the results are shown in Fig. 4.5. We use three routers with different malicious levels to show the performance of the proposed RM system. For the first 10 transactions, we set them all as general routers for gaining reputation purpose. In the next 30 transactions, their reputation values will be affected by their malicious routing behaviors. For instance, the one with 100% selfish behavior loses its reputation soon and gets isolated from the network. The router with 50% selfish behavior is set to be the on-off attack, which impacts the network by alternatively providing good and bad services in order to cover its damage to the network. By using the proposed RM system, the on-off attack could also be efficiently detected. As shown in the figure, this router has experienced a continuous decline until it reached the bottom threshold and got isolated. The one with 0% packet

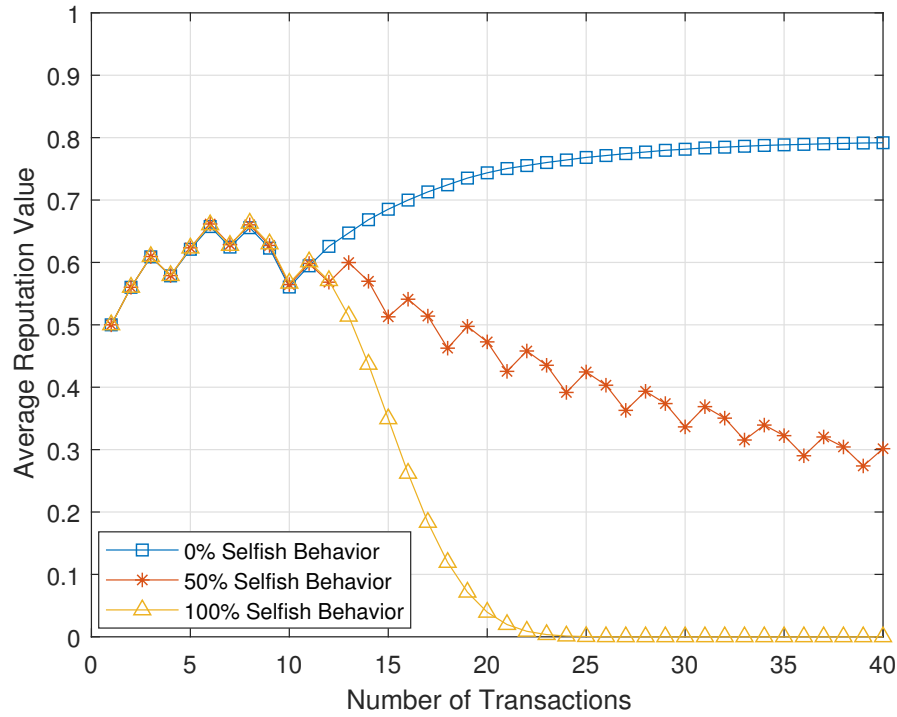


Figure 4.5: Selfish behavior detection for different malicious levels.

dropping attack frequency is a general router and its reputation experienced a slow increase.

4.5.2.2 System Convergence Performance

This subsection demonstrates the performance of the proposed distributed blockchain-based RM model by presenting the system convergence analysis. In IoT networks, the reputation value of each router is hard to manage with the number of malicious routers dramatically increasing and the size of this network significantly increasing. Thus, we analyze the convergence performance of the proposed blockchain-based RM system from two aspects: malicious level and network size.

Convergence Performance With Different Malicious Levels: In this test, we focus on the convergence analysis of the proposed RM system with different malicious levels. We use 50 IoT nodes as the network size. For evaluation criterion, we use the number of malicious routers left in the network.

Fig. 4.6 depicts the convergence performance of the proposed RM with different malicious

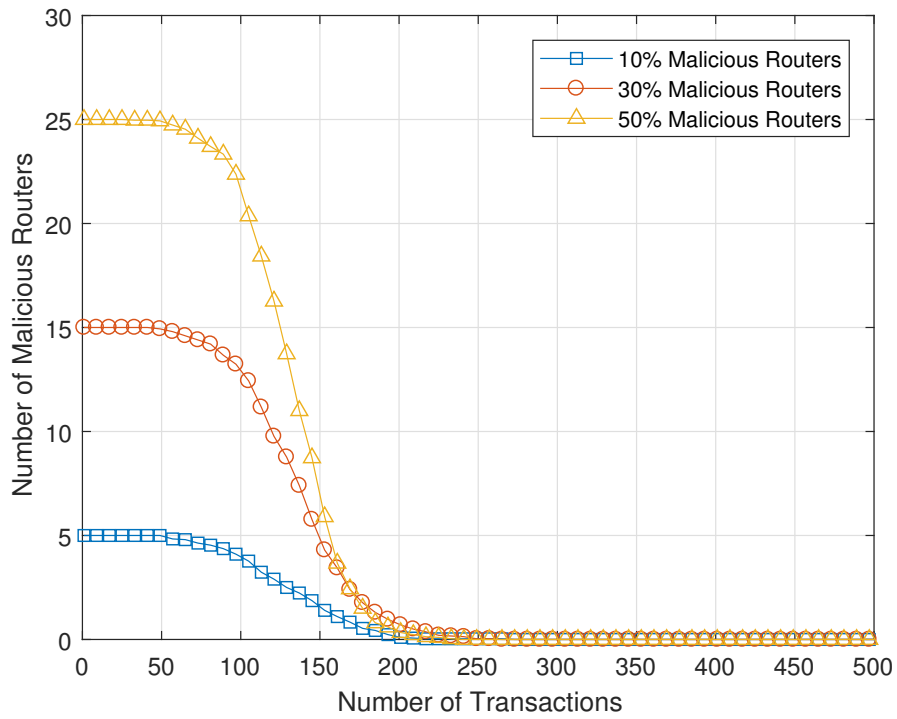


Figure 4.6: Convergence of the proposed reputation system for different malicious levels.

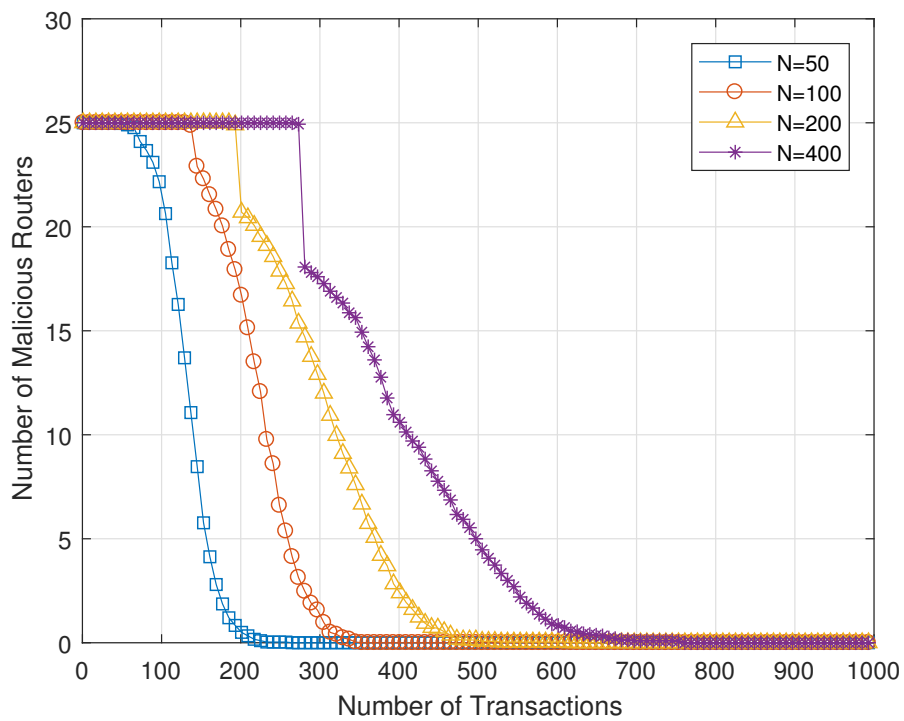


Figure 4.7: Convergence of the proposed reputation system for different network sizes.

routers percentage: 10%, 30% and 50%. As we can observe from the figure, with the increase of transactions, all the malicious routers have been detected and isolated from the system for these three cases. The RM system converges at respectively 224th, 252nd and 280th transaction for 10%, 30% and 50% malicious routers cases. The result illustrates that the proposed BC-based RM model converges with different malicious as the all the malicious routers are identified and isolated.

Convergence Performance With Different Network Sizes: The second test evaluates the convergence performance of the proposed RM system with different network sizes. We set 25 malicious routers in each network in order to control the impact of different number of misbehaving routers. Fig. 4.7 shows the convergence performance of the proposed RM system with different network sizes (N= 50, 100, 200, 400). The system converges to 0 at respectively 265th, 353rd, 617th and 761st transaction for N= 50, 100, 200, 400. This figure suggests that the proposed blockchain-based RM system has a strong scale capacity for monitoring the routing behaviors in IoT networks.

However, the convergence performance could be challenged when the size of the IoT network becomes excessively high due to the large memory size requirement in RM system.

4.5.2.3 Robustness and Efficiency Performance

In this subsection, we analyze the robustness and efficiency performance of the proposed blockchain-based RM system.

Robust Performance: For evaluate the robust performance of the system, two criteria have been tested, namely, global reputation value performance and successful transaction rate.

In the first experiment, we consider the global reputation performance of the system. We compute global average reputation value as the evaluation criterion against different malicious percentage scenarios. We perform a total of 1000 transactions and test the performance with three malicious levels: 10% malicious routers, 30% malicious routers and 50% malicious routers. As shown in Fig. 4.8, the global average reputation value drops in the beginning due to the malicious routers' behaviors when the total transactions number is less than 100. After

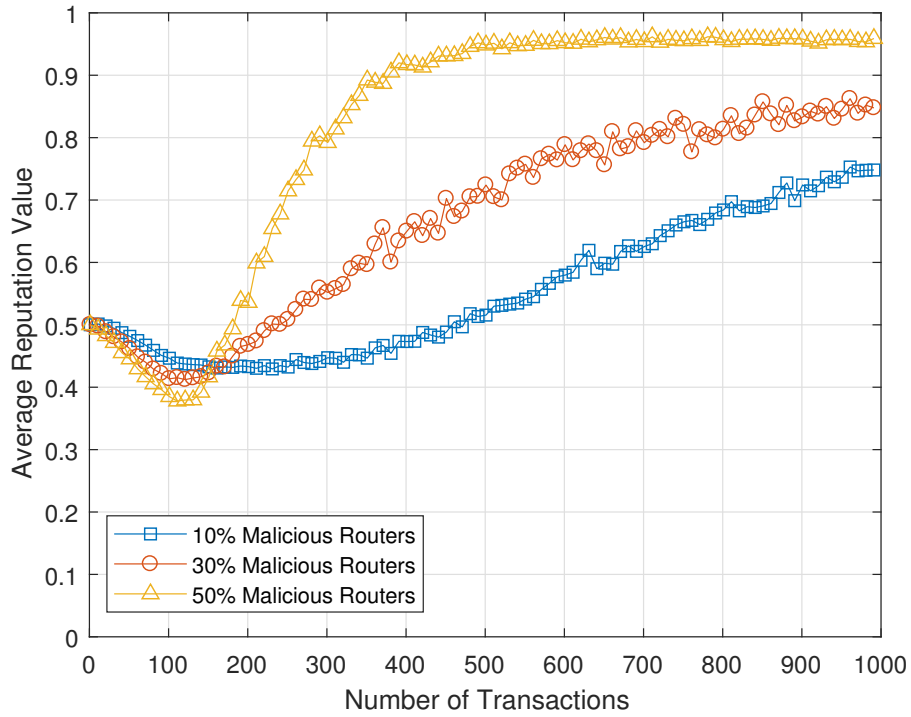


Figure 4.8: Global reputation value performance detection for different malicious levels.

that, the average reputation value of the system starts to recover. The reason of the recover is that the blacklist removes the malicious routers with low reputation values from the system. At the 1000th transaction, the average global reputation valves are respectively 0.7482, 0.8477 and 0.9589 for 10% malicious routers, 30% malicious routers and 50% malicious routers. Thus, with using the proposed distributed blockchain-based RM system, the whole system can be optimized by removing misbehaving routers.

In the second experiment, we compute the Successful Transaction Rate (STR) as the evaluation criterion in order to test the robust performance of the proposed RM model. We perform a total of 1000 transactions and take the average result for 30 experiments. Transactions initiated by malicious routers have been discarded from the calculation of STR. The following equation (4.9) shows the STR calculation.

$$STR = \frac{\text{Number of Successful Transaction}}{\text{Total Number of Transaction}} \quad (4.9)$$

In this test, we compare the proposed model with FCTrust [72], SFTrust [73], and Dynamic

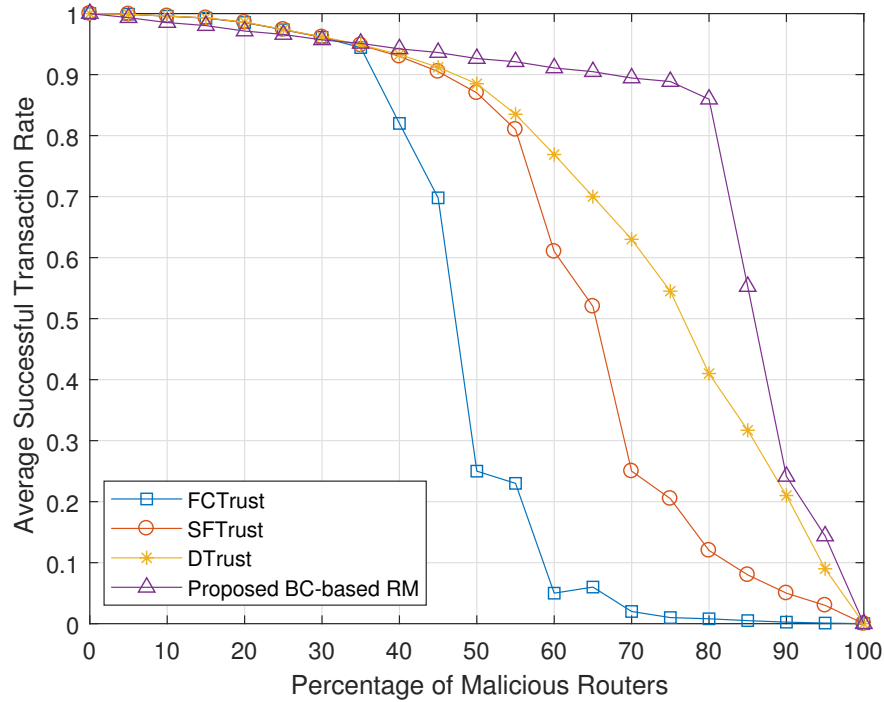


Figure 4.9: Comparing the proposed RM system with other existing trust models in terms of average STR against malicious percentage.

trust model for Multi-agent systems (for short we will use DTrust) [74]. As we observe from the Fig. 4.9, the proposed BC-based RM model shows its superiority over the remaining trust models in maintaining successful transactions as the percentage of malicious routers increases. Only until the percentage of malicious routers reaches more than 80%, the average STR then starts to decrease sharply, due to the lack of trusted routers existed in the network. Whereas, the turning point for FCTrust, SFTrust and DTrust are approximately 35%, 55% and 60%. The figure proves that the presented blockchain-based RM model could not only hold back malicious routers from data forwarding, but also ensure a higher successful transaction rate for maintaining the operation of the system.

Blockchain Efficiency: In this subsection, we mainly analyze the proposed group mining blockchain efficiency in order to prove the rationality of applying blockchain technology. In the experiment, we mainly test the efficiency enhancement of the proposed group mining scheme compared with the traditional blockchain mining technology and existing mining method.

To evaluate the efficiency, we use the processing time of generating one block as the measurement criterion for the simulation. Specifically, the processing time of a new block generation is consisting of the process of new block generating, the process of verifying the transactions and hash values, mining process and the time of broadcasting the new block to other blockchain members. The traditional blockchain technology, cooperative mining blockchain proposed in [33] and voting blockchain proposed in [44] are simulated for comparing with the proposed group mining model.

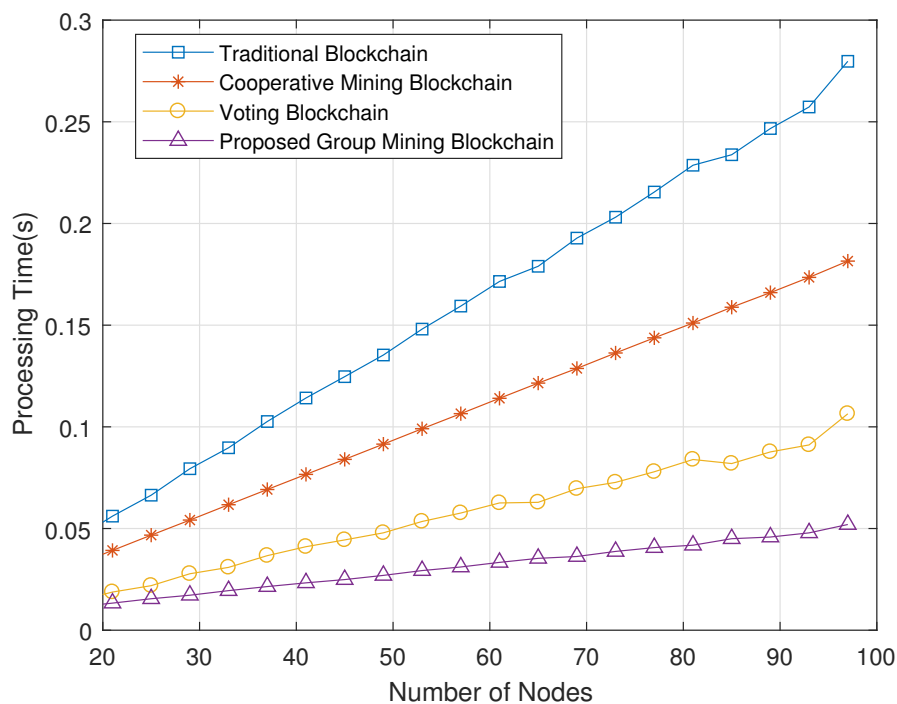


Figure 4.10: Comparison results of our blockchain model with other existing blockchain models in terms of processing time for creating one new block.

Fig. 4.10 compares the proposed group mining model with the traditional blockchain technology, the cooperative mining blockchain and the voting blockchain in terms of processing time of mining a new block. For the traditional blockchain, the processing time is the longest among these four due to the high consumption of the traditional PoW. For the cooperative mining blockchain, the processing time is less than the traditional one because the cooperative mining process simplifies the PoW process by allocate the mining tasks to different mining devices group. However, the efficiency performance is not well improved and the whole system

is under the threat of 51% attack. For the voting blockchain, when the number of IoT nodes in the network is less, this method significantly reduce the processing time of a new block generation for the reason that the number of nodes required to vote for each transaction is less enough. Thus, the total processing time is close to the performance of the proposed group mining model. However, with the number of nodes increasing, the number of voting nodes are getting enormous, and the processing time is required more than the proposed model. For the proposed efficient group mining process, with the number of routers increasing, it shows high efficiency improvement compared with other three models because of the efficient grouping mechanism and specific verification process among the mining group members.

Overall, our method substantially decreases the processing time compared with the traditional blockchain, cooperative mining blockchain and the voting blockchain. With the increasing number of IoT nodes, it shows more advantages in the processing time of new block generation while keeps the security level of the PoW technique. It should be noted that the proposed group mining process presented in this chapter could also be employed in other blockchain-based systems in order to achieve the goal of simplifying blockchain technology.

4.6 Chapter Summary

With the rapid proliferation of Internet of Thing (IoT) devices, many security challenges could be introduced at low-end routers. Misbehaving routers affect the availability of the networks by dropping packets selectively and rejecting data forwarding services. Although existing Reputation Management (RM) systems are useful in identifying misbehaving routers, the centralized nature of the RM center has the risk of one-point failure. The emerging blockchain techniques, with the inherent decentralized consensus mechanism, provide a promising method to reduce this one-point failure risk. In this chapter, we proposed a blockchain-based reputation management system for routing process protection in IoT networks. By applying the blockchain technique onto the edge server, the proposed distributed reputation management system can effectively handle the reputation value of each router in the system. A global reputation management scheme was presented to determine the reputation value for each router. To improve the implement efficiency of blockchain, we also proposed an efficient group mining technique

for the blockchain. The overhead of the proposed work has been investigated. Simulation results validate the distributed blockchain-based RM system in terms of attacks detection, system convergence performance, and robustness and efficiency performance. The comparison results of the proposed group mining process with existing blockchain models illustrate the applicability and feasibility of the proposed works.

Chapter 5

A Sidechain-based Decentralized Authentication Scheme via Optimized Two-way Peg Protocol for Smart Community

5.1 Introduction

IoT smart community is an IoT application scenario where different IoT systems are combined, such as smart homes, smart health, and smart agriculture. In smart community, personal data are collected and processed in each system by smart devices, and then get shared with other systems [8]. In order to ensure the security of personal information, it is fundamental to make sure that only the registered and authenticated devices can make use of the system and share information. Otherwise, it will result in numerous potential security risks such as information stealing, data tampering and identity usurpation [36]. Local authentication process in each smart system and sharing authentication information within sub-systems remain the major obstacle for privacy protection in IoT smart community due to imperfect mechanisms and the resource-constrained nature of IoT devices [37].

As previously mentioned in Chapter 2, the existing architectures in IoT smart community

suffer from low device authentication efficiency, authentication methods uniformity, and centralized sharing server. In order to overcome these challenges and limitations, we propose a novel sidechain structure with an optimized two-way peg protocol for the device authentication in smart community, with an emphasis on establishing a decentralized structure for local authentication process and realizing information sharing with other systems, as well as achieving minimal time and storage consumption at constrained IoT devices. The proposed sidechain model utilizes a public mainchain as a reference chain to keep a local information record, and private side blockchains to manage the local authentication process in each system. We also come up with the optimized two-way peg protocol for sidechain system to realize a secured information sharing procedure between the main chain and side blockchains, by dynamically evaluating the trustworthiness of the target device. Both PoW and Simplified Payment Verification (SPV) has been reached as consensus mechanisms for blocks generation and efficient information tracking purposes [50] [75].

This chapter is organized as follows. In section 5.2, the proposed decentralized sidechain-based authentication scheme with optimized two-way peg protocol is demonstrated. In section 5.3, technology comparison results are given among the proposed sidechain model and other existing methods. In section 5.4, the simulation results are presented and analyzed. Finally, this chapter is concluded in section 5.5.

5.2 System Model

Fig. 5.1 presents the proposed sidechain-based authentication model in a smart community, which is composed of a public blockchain as a mainchain and private blockchains as side blockchains. To illustrate the model, we use two smart home cases to represent the IoT smart systems. In each smart system, central mining nodes are chosen among local smart devices based on their computational abilities and locations. The private blockchain is built among the central mining nodes and gateway in order to securely manage the authentication processes with the distributed PoW consensus mechanism. Among all the gateways in this smart community, a public mainchain is employed to securely manage the authentication information sharing process with implementing the optimized two-way peg protocol. In order to reduce

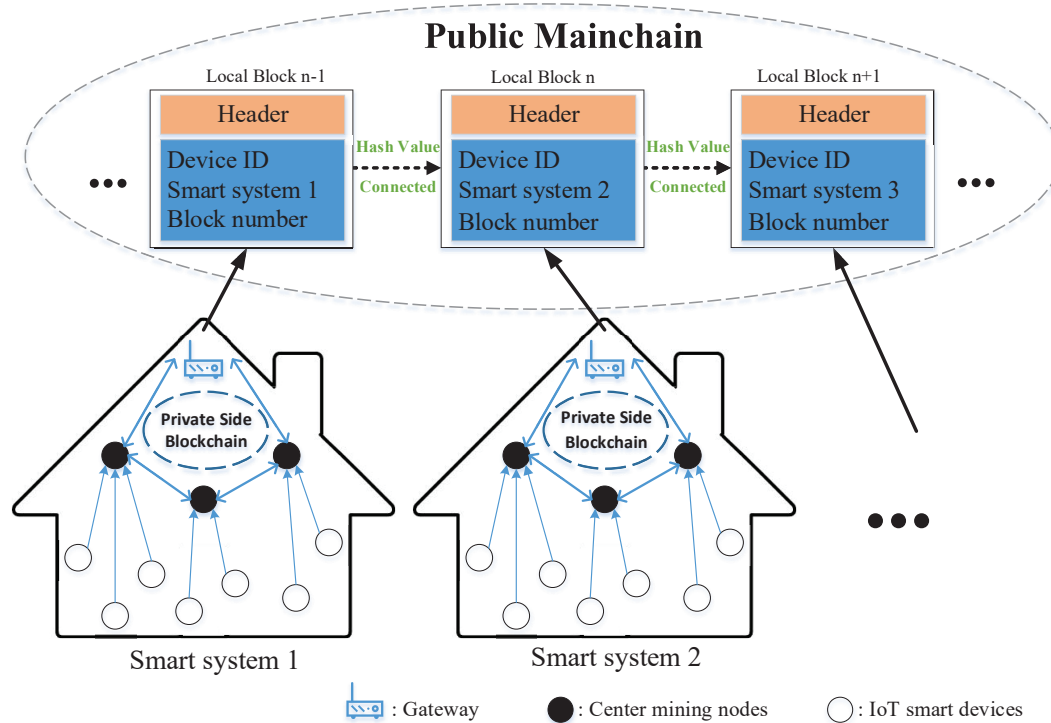


Figure 5.1: Proposed sidechain-based authentication model. The proposed model consists of a public mainchain and private side blockchains.

the storage consumption at the gateway level, each mainchain block will only be saved at local gateway after the verification process without updating an entire mainchain.

5.2.1 Local Authentication Procedure at Private Side Blockchains

In this section, we mainly illustrate the implementation procedure of authentication process at each private side blockchain. We divide the procedure into two phases: Registration phase and Authentication phase. In the Registration phase, the authentication information will be viewed as the transactions and uploaded to the local private side blockchain to form a block. In the Authentication phase, the authentication parameters saved in the block will be extracted and compared with the received parameters to decide if the device has been successfully authenticated or not.

5.2.1.1 Registration Phase

When a new IoT device is firstly added to a smart system, the device should be registered by the corresponding private side blockchain in this system.

Firstly, the device sends its ID to the gateway, and its ID will be searched in the public mainchain to see if it is newly registered. If there is previous authentication information existed in other smart systems, the gateway will send a request to the public mainchain for authentication information sharing process. Otherwise, the local registration process will start.

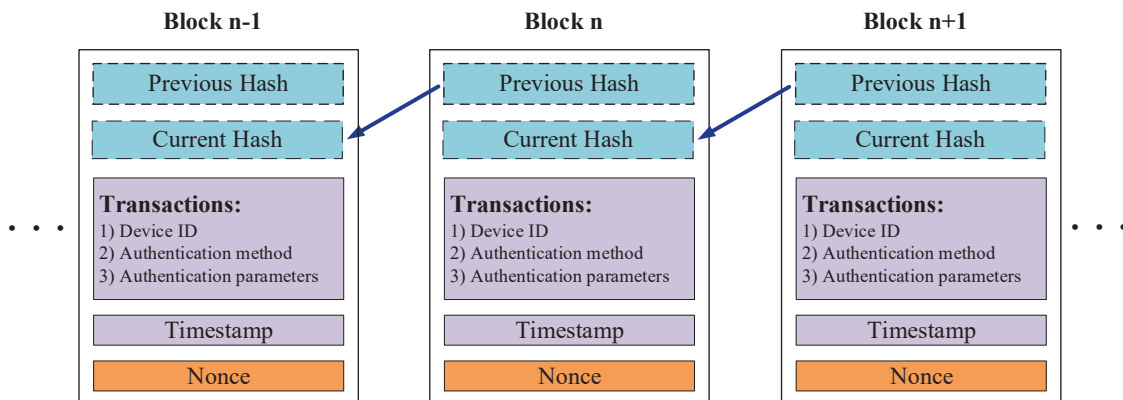


Figure 5.2: Structure and content of the private side blockchain.

The local registration process is achieved by creating a new block into the private side blockchain. Fig. 5.2 shows the structure of a block in the private side blockchain, which consists of the header information (previous hash and current hash, time stamp and nonce value) and transactions. By adopting the PoW consensus mechanism, a trusted relationship among all the central mining nodes will be established. The data saved in the blockchain cannot be changed or manipulated. In our model, the authentication information of each device will be saved as three transactions into one block, which contains the following components: (1) device ID; (2) authentication method; (3) corresponding authentication keys or parameters. The authentication method can be various based on the devices' computational powers and usage scenarios. Except of the device ID for the tracking purpose, all transactions are encrypted by using Secure Hash Algorithm (SHA) 256 with the device's private key [75].

When a new device has been successfully registered, the devices ID and its block number will be uploaded along with the corresponding smart system ID to the public mainchain to

form a reference records for the authentication information sharing procedure, which we will mention in the next Section 5.2.2.

5.2.1.2 Authentication Phase

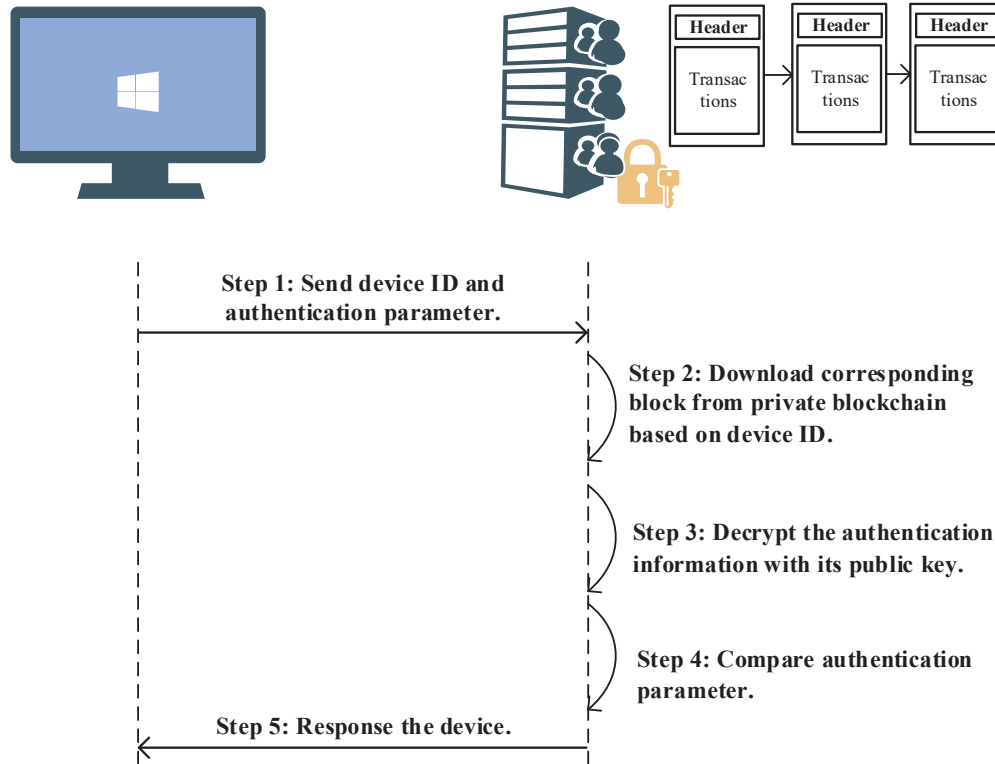


Figure 5.3: Procedure of the proposed authentication process at private side blockchain.

When a smart device wants to establish a communication session within the smart system for data uploading or downloading after the registration process, the authentication process will be required.

Fig. 5.3 displays the procedure of the proposed authentication process. First, a request that contains the device's ID and authentication parameters will be sent to the nearest central mining node. Secondly, the central mining node downloads the corresponding block from the private side blockchain relying on the device ID. Then, after decrypting the block with the public key of the device, the central mining node will compare the decrypted authentication parameters with the received parameters. Finally, a response will be sent to the device to inform whether it is successfully authenticated.

Since the device authentication process is achieved at the nearest central mining node instead of the gateway device, the communication burden of the gateway has been significantly decreased.

5.2.2 Authentication Information Sharing at Public Mainchain

The IoT device with mobility features can move from one smart system to another system, such as drones and community service robots. If this device requires to get access to the data in the new system, it should be authenticated by the system. However, if there is no previous authentication information block existed in the system (side blockchains), the device would be required to repeatedly register in the new system, which will cost large amounts of energy and time. Therefore, authentication information should be able to be shared within a smart community.

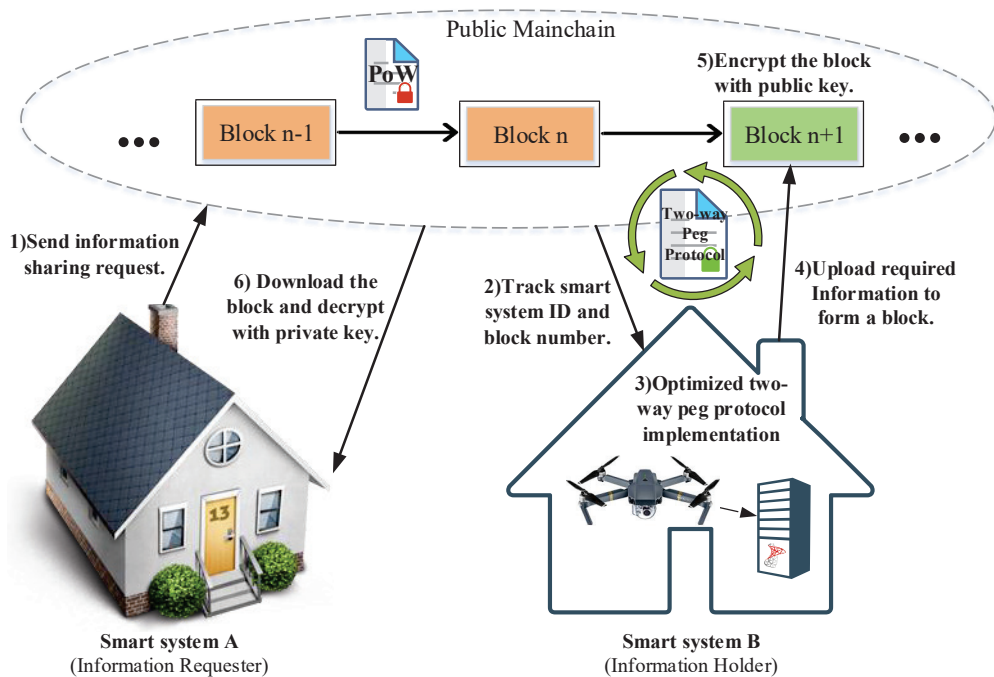


Figure 5.4: Model of authentication information sharing at the public mainchain. Both PoW consensus mechanism and the proposed optimized two-way peg protocol have been applied for safe operation of the proposed sidechain-based smart community system.

Although a device can be successfully registered by one system, it still has a risk of being compromised later on to become a malicious device, and its authentication information can no

longer be used by other systems. The original two-way peg protocol is designed to defend the financial sidechain systems from a unique business attack which is double spending attack, but it cannot prevent the risk in our presented scenario. Thus, we propose an optimized two-way peg protocol to guarantee the trustworthiness of the shared information in the information sharing procedure by dynamically calculating the trust value of the target device. Fig. 5.4 demonstrates the procedure of the proposed authentication information sharing procedure guaranteed by the optimized two-way peg protocol. The procedure mainly consists of the 4 steps as follows:

Information Source Tracking: When an IoT device firstly registers in a smart system, the corresponding gateway will send a tracking request along with the device ID to the mainchain in order to check if there is previous authentication information of this device. When the public mainchain receives the request from the information requester (smart system A), the corresponding block that contains the information resources (including smart system ID and block number) will be tracked based on the device ID.

SPV Proof Collection: For those smart systems with required information, an SPV proof (device ID, device ID list, block header list) is required to send to smart system A in order to prove the existence of the target information without downloading the full chain. Then, the gateway of smart system A will do the SPV verification. However, offloading the SPV verification task to a single node (gateway) is a security concern for the smart system since a malicious gateway could deceive the system by responding with adulterated outcomes. Therefore, the local center mining nodes will be required to handle the verification voting process with local gateway. Only more than half of them successfully verify the SPV proof will the result be proved.

Trustworthy Evaluation: Based on the SPV proofs, the current trust value of this device will be calculated and get compared with the trust threshold of the smart system A. Only when the gateway provides the positive result will the information be shared with the information requester. Otherwise, the device will be reported to be manually registered in order to protect the security of the smart community.

For the trust value calculation rule, we mainly consider three aspects a device: authentication method evaluation, information sharing history evaluation and authentication process evaluation. We set the whole range of trust value in [0-1], and each IoT smart system can have different acceptance threshold to filtrate the untrustworthy devices.

T_{meth} represents the trust value for using different authentication methods. The harder the authentication method is, the higher T_{meth} it gets. The reason is that we assume the harder authentication method can provide a higher security performance, and we set that each device can pick one authentication method depending on its computational powers and its usage scenario. For example, we set 0.4 for using PSK authentication method and 0.5 for using certificates authentication method.

The following two equations express the calculation process for information sharing history evaluation and authentication process evaluation.

$$T_{sharing} = \frac{\alpha_i}{N_{sys} * M_{thre}} \sum_{i=1}^{N_{use}} T_{thre}, \quad (5.1)$$

where $T_{sharing}(i)$ is the trust value of information sharing for this device. N_{sys} is the total number of IoT smart systems in this smart community. M_{thre} is the average trust threshold of the whole smart community. N_{use} is the number of smart systems that currently have the authentication information of this device. T_{thre} is the corresponding trust threshold of the smart system. α_i is decay factor.

$$T_{authen} = \beta \sum_{i=1}^{N_{succ}} T_{thre} - \gamma \sum_{i=1}^{N_{unsucc}} T_{thre}, \quad (5.2)$$

where $T_{authen}(i)$ is the trust value of authentication process for this device. N_{succ} is the total number of successful authentication process in the smart community, and N_{unsucc} is the total number of unsuccessful authentication process in this smart community. T_{thre} is the corresponding trust threshold of each smart system. Both β and γ are weight factors.

By combining these three trust value components, the trustworthy of a device can be dynamically calculated as in equation (5.3).

$$T_d = \lambda * T_{meth} + \mu * T_{sharing} + \nu * T_{authen}, \quad (5.3)$$

where T_{meth} , $T_{sharing}$ and T_{authen} are in $[0-1]$. λ , μ and ν are weight factors, and $\lambda + \mu + \nu = 1$.

Information Sharing: When the trust value of this device meets the threshold of smart system requester, the required authentication information will be allowed to get shared. The decrypted required information will be uploaded to the public mainchain from the nearest information holder (smart system B) to form a new block by using the PoW consensus mechanism. Then, the information will be encrypted with the public key of smart system A so that only the information requester can read and download the content of the block with its own private key. It should be noted that the optimized two-way peg protocol presented in this chapter could also be employed in other sidechain-based IoT systems to ensure the trustworthiness of the required information.

5.3 Technology Comparison

In order to illustrate the technical advantages of the proposed sidechain model, we compare the proposed sidechain model with traditional blockchain technology used in bitcoin system, and the traditional sidechain technology used for crypto-currency transferring.

The Table 5.1 presents the comparison results of these three technologies in terms of technical details and security capability. As we can obtain from the table, both blockchain technology and traditional sidechain technology have the risk of being threatened by double spending attack and worthless information attack. Whereas, the proposed sidechain technology in the smart community is a non token-used system and it does not suffer from double spending attack. Moreover, the proposed optimized two-way peg protocol protect the system from the worthless information attack during the information sharing procedure among side blockchains and mainchain.

5.4 Simulation Experiment and Result Analysis

In this section, we evaluate the proposed sidechain-based device authentication scheme in terms of the authentication time consumption, the optimized two-way peg protocol performance,

Table 5.1: The Technology Comparison Between the Traditional Blockchain Technology, the Traditional Sidechain Technology and the Proposed Sidechain Model.

	Blockchain Technology in Bitcoin System	Sidechain Technology for Crypto-currency Transferring	Proposed Sidechain in This Chapter
Member Permissions	Public Blockchain; (Every entity can read and write)	Public mainchain and public side blockchains	Public blockchain and Private side blockchains
Transaction Content	Crypto-currency	Crypto-currency	Collected data
Transaction Relationship	Continuously, Related	Continuously, Related	Independent, Unrelated
Consensus Mechanism	PoW	Pow and SPV	PoW and SPV
Protocol for Transferring Information	No	Two-way peg protocol	Optimized two-way peg protocol
Double Spending Attack	Yes	Yes	No
Worthless Information Attack	Yes	Yes	No

information management efficiency and storage consumption.

5.4.1 Authentication Time Consumption Analysis

As previously mentioned in Chapter 2, a blockchain-based method has been proposed to distributively manage the local authentication process and information sharing process [43]. The authentication information has been viewed as transaction saved in blockchain and can be shared within the community. However, this structure increases the burden of gateways by treating them as central devices to handle the local authentication procedure and saving authentication information from other systems. In this experiment, we compare the proposed sidechain-based method with the blockchain-based method and conventional authentication without any additional method in terms of authentication time consumption.

5.4.1.1 Simulation Settings

We simulate an authentication process between a gateway that hosts the blockchain/sidechain and a smart device in MATLAB. Table 5.2 describes the environment features of the simulation. We test the authentication time consumption by comparing these three methods: (1) the conventional authentication process without applying any additional method; (2) the authentication process with using the proposed sidechain-based method; (3) the authentication process with using the blockchain-based method. We use PSK as the authentication method for this experiment. The experimental results are averaged over 30 runs.

Table 5.2: Environment Features of Authentication Process.

CPU Processor	Operating System	CPU Max Speed	Computing Environment
x64	64-bit Microsoft Windows 10	2.6 GHz	MATLAB

5.4.1.2 Authentication Time Consumption Against PSK Character Lengths

For the first test, we evaluate the effect of PSK character lengths to the authentication time consumption. We simulate a smart community with 10 smart systems and each system have 10 smart devices. Fig. 5.5 presents the authentication time comparison results of using three abovementioned methods with different PSK character lengths. Although the conventional method without any additional method realizes the lowest authentication time among three methods, it has lowest functionality and security enhancement performance. For 12 chars PSK, the authentication time for the blockchain-based method is 0.0054 seconds, and 0.0046 seconds for the proposed sidechain-based method. With increasing the number of characters in PSK, the average authentication times for the conventional method, the proposed sidechain-based method and blockchain-based method are respectively 1) 0.0053 seconds, 0.0076 seconds and 0.0088 seconds when PSK has 24 characters; 2) 0.0098 seconds, 0.0133 seconds and 0.0153 seconds when PSK has 24 characters.

As we can observe from that the proposed sidechain-based method shows its superiority in reducing authentication time compared with the blockchain-based method, with saving

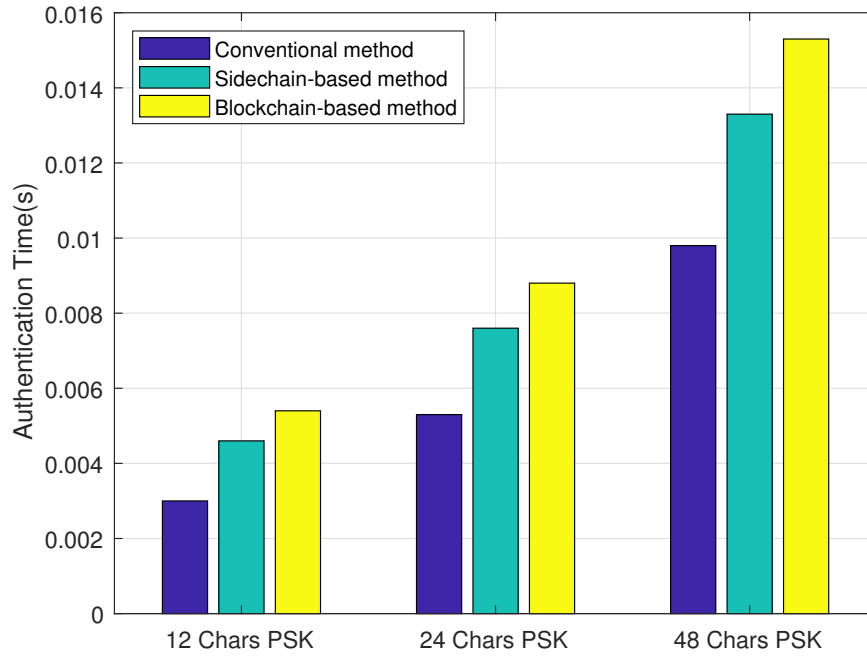


Figure 5.5: Authentication time comparison among three methods with different PSK character lengths.

33.33%, 34.29% and 36.36% of the additional cost on authentication time caused by using blockchain structure for these three cases. As the character length of PSK increases, the proposed sidechain-based method shows more advantages in decreasing authentication time compared with the method in [43]. The reason is that the complexity of searching the target device ID in the block has increased with the number of PSK increases. With using the proposed sidechain, the offload of public mainchain could be noticeably reduced compared with the existing blockchain-based method.

5.4.1.3 Authentication Time Consumption Against Blockchain Parameters

Considering the position of the block that owns the authentication parameters and the blockchain length may induce to an additional time cost, we focus on analyzing the influence of blockchain parameters to the authentication time results in the second test.

We simulate the blockchain/sidechain with 100 blocks and 200 blocks, and use 12 chars PSK as the authentication method for this experiment. We compare three block positions

for each block length scenario: (1) the authentication parameters are in the first block of the blockchain, presented as B_F ; (2) the authentication parameters are in the middle block of the blockchain, presented as B_M ; and (3) the authentication parameters are in the last block of the blockchain, B_E .

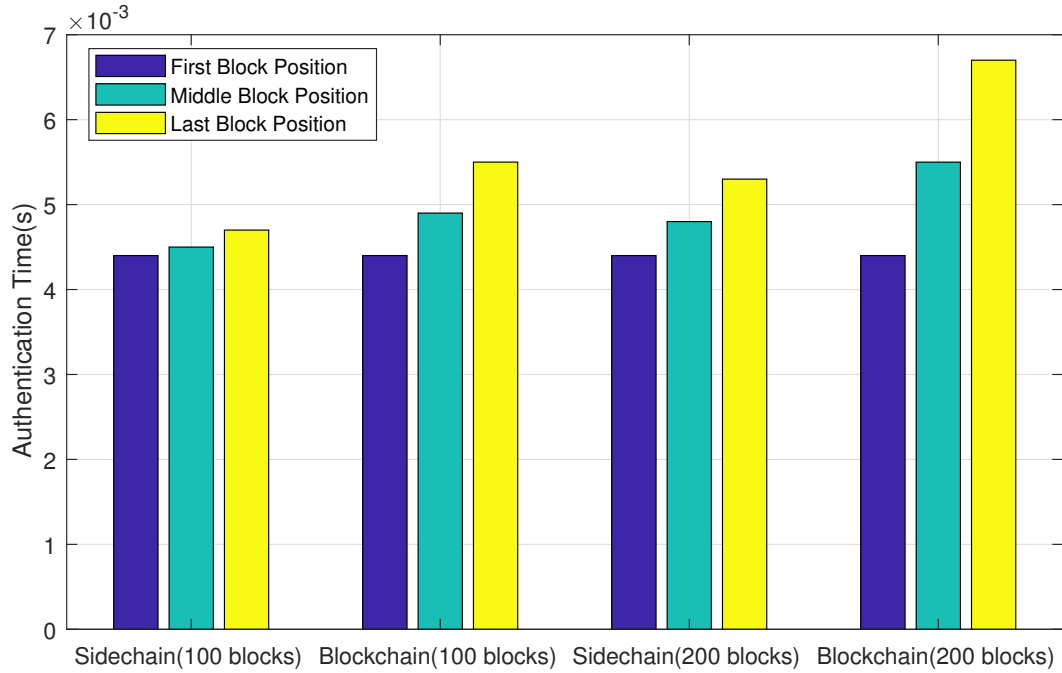


Figure 5.6: Authentication time comparison of three block positions with different blockchain lengths.

Fig. 5.6 exhibits the authentication time comparison results of three abovementioned block positions with different blockchain lengths. For the 100 block length scenario, the authentication times for blockchain-based model are 0.0044 seconds, 0.0049 seconds and 0.0055 seconds, respectively for the scenarios B_F, B_M and B_E . Whereas, the authentication times for the proposed sidechain model are 0.0044 seconds, 0.0045 seconds and 0.0047, respectively for these three block positions. It can be concluded that the proposed sidechain-based authentication model could decrease the additional implementation time caused by block positions compared with the existing blockchain-based authentication model. Take B_E for 100 blocks as an example, it decrease 0.0008 seconds. which is 14.55% of the total time consumption of blockchain-based model. For the 200 block length scenario. the authentication time for

blockchain-based model are 0.0044 seconds, 0.0055 seconds and 0.0067 seconds for these three positions, while 0.0044 seconds, 0.0048 seconds and 0.0053 seconds for the sidechain-based model. The proposed sidechain-based model saves 0.0014 seconds at the last blockchain position compared with blockchain-based method, which is 20.90% of the total time consumption of blockchain-based model. Therefore, as the number of block increase, the proposed sidechain model show its benefit in reducing the complexity of information searching compared with blockchain model.

5.4.2 Performance Analysis of the Proposed Optimized Two-way Peg Protocol

In this experiment, we evaluate the proposed optimized two-way peg protocol in the simulated sidechain system.

5.4.2.1 Simulation Settings

Table 5.3: Parameter Configurations for Testing the Proposed Trust Scheme.

	Number of Smart Systems (N_{sys})	Acceptance Trust Threshold (T_{thre})	Registered Systems (N_{succ})
Systems with Low Trust Threshold	60	[0.30-0.50]	10
Systems with High Trust Threshold	40	[0.50-0.70]	5

We simulate a smart community with 100 smart systems and record the trust value of smart devices with different malicious behavior percentage. The parameter configurations for testing the proposed optimized two-way peg protocol are listed in Table 5.3. The experimental results are averaged over 30 runs.

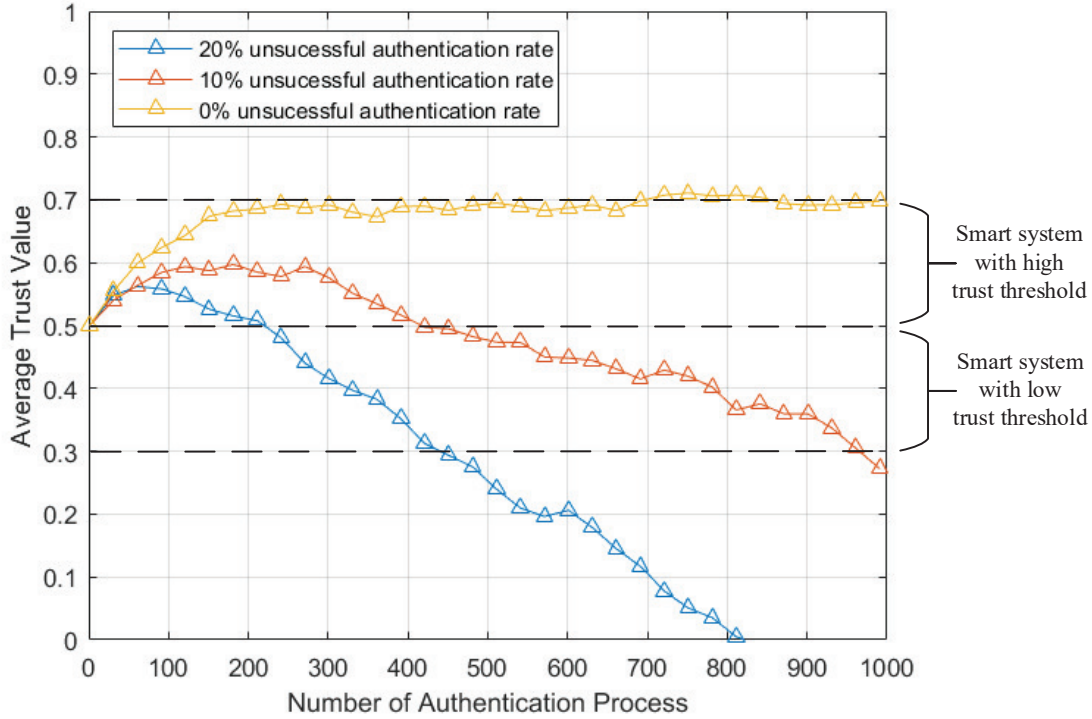


Figure 5.7: Performance evaluation for optimized two-way peg protocol with using certificates as the authentication method.

5.4.2.2 Optimized Two-way Peg Protocol Performance

We use certificates method as the authentication method to show the performance of the proposed protocol. In this experiment, we test the performance of the trust evaluation scheme with three malicious levels: 20% unsuccessful authentication rate, 10% unsuccessful authentication rate and 0% unsuccessful authentication. As shown in Fig. 5.7, the device with 0% unsuccessful authentication rate continuously gains trust values by its successful behaviors, and its average trust value increases steadily and slowly. Its authentication information can be allowed to be shared with other smart systems through the public mainchain as long as it can provide the proof that its trust value is higher than the trust threshold of a target smart system. As previously mentioned, the trust value of this device with no malicious behavior approximately stays 0.70, which can meet the requirements of most smart systems with high trust threshold ([0.50-0.70]) and all the smart systems with low trust threshold ([0.30-0.50]). On the contrary, for the devices with 10% unsuccessful authentication rate, its trust value will decline continuously. After 412nd authentication, its authentication information can no longer be shared in the

smart systems with high trust threshold. Then, after 964th authentication, its information will not be allowed to be shared in the smart community. For the devices with 20% unsuccessful authentication rate, its trust value will decline sharply. Its authentication information cannot be shared with smart systems with high trust threshold at 221st authentication. After 438th authentication, its information will not be allowed to be shared in the smart community.

When the trust value is less than the threshold of the target IoT system, the authentication information cannot be shared with other smart systems in order to protect the information security of the community.

5.4.3 Performance Analysis of the Information Management Efficiency

Due to the low computational power of constrained IoT smart device, one of the most important requirements for the proposed sidechain-based authentication method is to decrease the computational overhead caused by managing the authentication information at the gateway side. Thus, this subsection mainly demonstrates the comparison results between the proposed sidechain-based method, the traditional sidechain method and the blockchain-based method mentioned in terms of information management efficiency.

5.4.3.1 Simulation Settings

Table 5.4: Parameter Configurations for Analyzing the Implementation Cost.

CPU Frequencies of Each Gateway (Mining Nodes of Public Mainchain)	CPU Frequencies of Each Central Mining Nodes (Mining Nodes of Private Side Blockchain)	Cycles per Byte	Block Size for private sidechain	Block Size for public mainchain
[2GHZ, 2.8GHZ]	[1GHZ, 2GHZ]	100	248 bytes	108 bytes

Since gateways and other IoT devices have different computational powers processing the transactions, we set different CPU frequency for them in order to evaluate the authorization and authentication time [71]. As shown in Table 5.4, we assume that the block sizes for private side blockchain and public mainchain are respectively 248 bytes and 108 bytes. The CPU

frequency for IoT center mining nodes and gateways are between [1GHz, 2GHz] and [2GHz, 2.8GHz], respectively.

5.4.3.2 Information Management Efficiency Performance

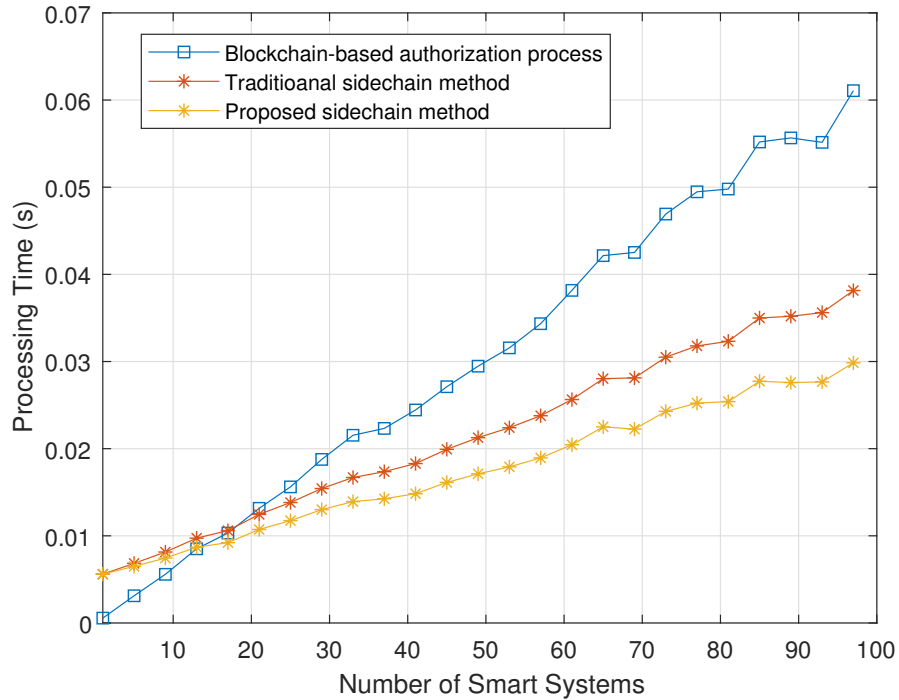


Figure 5.8: Information management efficiency comparison among the proposed sidechain-based method, traditional sidechain method and existing blockchain-based method.

Fig. 5.8 presents the information management efficiency comparison between the proposed sidechain-based method, traditional sidechain method and existing blockchain-based method. We use the processing time consumption during the device registration phase as the criterion for this experiment. As we can observe from Fig. 5.8 that both sidechain methods have higher time consumption compared with the blockchain method when the number of smart systems in the IoT smart community is lower than 16. The reason is that the authorization time of the sidechain-based method consists of two folds: time for creating one local block in private side blockchain for saving the local authorization information and time for uploading a reference block to the public mainchain for sharing purpose. Thus, when the number of smart systems is low, the processing time for the proposed method would be high than the blockchain-based

method, which only needs to store one blockchain in each gateway. However, with the number of smart systems increasing, the sidechain methods show their superiority of decreasing implementation cost. For instance, they save more than 37.33% and 49.12% respectively of processing time compared with the blockchain-based method when the number of smart systems reaches 100. Therefore, compared to the existing methods, our method could enhance the information management efficiency at constrained IoT community.

5.4.4 Storage Consumption Comparison

Unlike the traditional sidechain structure, the public mainchain proposed in this work is viewed as a reference database, and it requires the gateway to save simplified information blocks at local memory. Whereas, both the blockchain-based method and traditional sidechain method are required to update the full chain after each new block verification. In this subsection, we compare the storage consumption at the gateway side among the conventional method, blockchain-based method, traditional sidechain and proposed sidechain method.

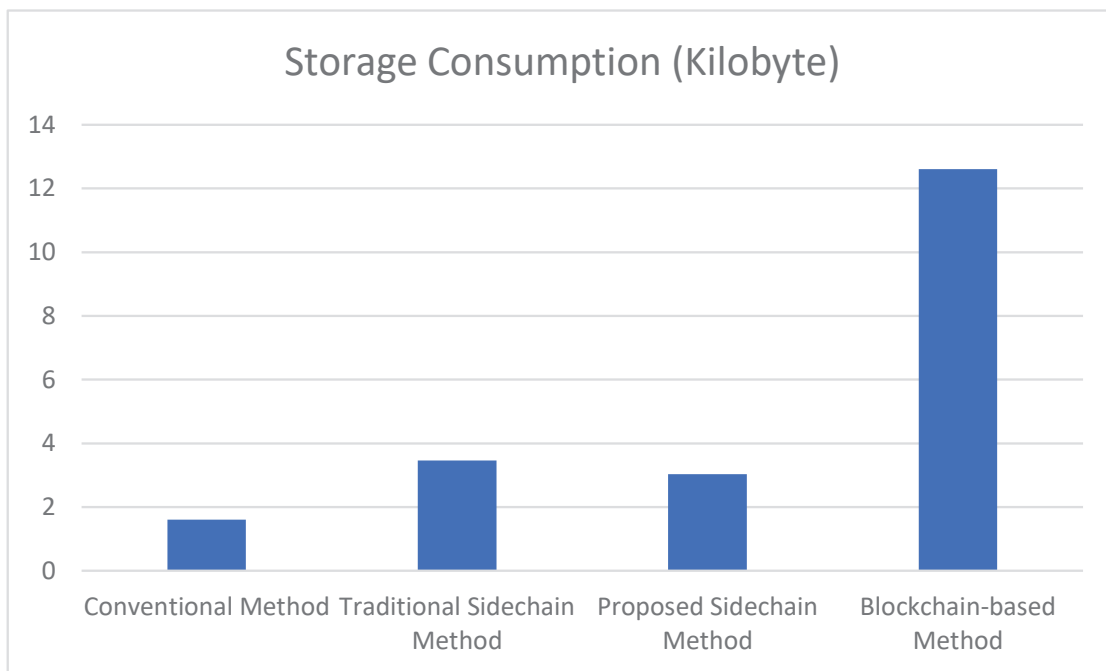


Figure 5.9: Storage consumption comparison between conventional method, blockchain-based method, traditional sidechain and proposed sidechain model.

In this experiment, we consider a smart community with 5 smart systems and each system

has 10 IoT devices. As mentioned in Section III, a local sidechain block contains device ID, authentication method and authentication parameters as transactions. The first two transactions (device ID and authentication method) are both 8 bytes. For the authentication parameters, we take certificate-based authentication as an example. As mentioned in [76], the average message size for the certificate-based authentication parameter is 148 bytes. Based on the quantitative data listed about the size for block component in Table 4.2, the storage sizes required for the conventional method, blockchain-based method, traditional sidechain and proposed sidechain method are respectively 1.60 KB, 12.61 KB, 3.45 KB and 3.03 KB. The proposed sidechain method only takes 24.02% of the memory space that the blockchain-based method has required, and 87.82% of the memory space that the traditional sidechain method has required.

5.5 Chapter Summary

In a smart community with large amounts of Internet of Things (IoT) devices, the authentication process for each device is vital for protecting the security of personal data for each user. Current authentication approaches suffer from numerous challenges when they are applied in a smart community, such as poor authentication efficiency, inflexible authentication approach and insecure information sharing server. Blockchain technology, as a decentralized peer-to-peer platform, provided a promising solution for managing the local authentication information and sharing the information within the smart community. However, it increased the storage burden and the complexity of the local authentication process at the constrained IoT device. Sidechain significantly reduces the information burden of the main blockchain by segmenting information into small blockchain systems and securely transferring key information between different systems, whereas, the traditional two-way peg protocol it uses does not protect the system against certain attacks. In this chapter, we propose a novel sidechain structure via optimized two-way peg protocol for the device authentication in smart community in order to overcome the limitations of existing approaches. The proposed sidechain structure requires the mining nodes of the mainchain to only store the local mainchain blocks without downloading or updating the entire mainchain after each block generation. By using Simplified Payment Verification (SPV) consensus mechanism, the existence of the target authentication informa-

tion could be proved. More importantly, we propose the optimized two-way peg protocol in the proposed sidechain system in order to prevent the worthless information attack during the authentication information sharing procedure. The simulation results prove the superiority of the proposed scheme in terms of reducing authentication time, improving information management efficiency and decreasing storage consumption compared with existing works, and the applicability and feasibility of the optimized two-way peg protocol have been approved.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In the first chapter, after a brief introduction to IoT networks, the motivation behind this thesis is presented. Security protection is one of the fundamental parts of IoT networks since most of IoT devices have constrained computational powers and imperfect self-protection mechanisms. Most of existing IoT model still follow the traditional centralized model, which has a high risk of one point failure. Therefore, the need for a secured decentralized IoT platform is undeniable. Specifically, two scenarios in IoT networks were detailedly investigated in this thesis, namely, IoT routing protection and device authentication in smart community.

The second chapter presents a comprehensive literature review of the existing challenges and solutions in the area of IoT routing process and IoT smart community authentication process. A large number of techniques and models have been studied, and their advantages and drawbacks are reviewed in this chapter. In order to overcome existing challenges in both scenarios, we studied the blockchain technology and focused on applying the blockchain technology into the IoT environments.

In Chapter 3, a detailed overview of blockchain technique has been firstly summarized, including the whole procedure of encryption and decryption, the concept of proof of work (PoW) and other blockchain related knowledge. Then, sidechain, an extended technology of blockchain, has been demonstrated in details, including its structure, the two-way peg protocol and the technology comparison results with blockchain. After that, several promising applica-

tions of blockchain technology are summarized based on different application fields, such as crypto-currency, identity management and medical applications. Finally, both advantages and disadvantages of the blockchain technique are analyzed for future research.

In Chapter 4, we proposed a blockchain-based reputation management system for routing process protection in IoT networks. By applying the blockchain technique onto the edge server, the proposed distributed reputation management system can effectively handle the reputation value of each router in the system. A global reputation management scheme was presented to determine the reputation value for each router. To improve the implement efficiency of blockchain, we also proposed an efficient group mining technique for the blockchain. Simulation results demonstrated that the proposed schemes can improve the security level of routing process in IoT networks by detecting routers' malicious behaviors. The convergence performance of the proposed reputation management system was also evaluated, and the results proved that the proposed technique has stable convergence with different network sizes. Furthermore, result comparison between the proposed group mining process and existing methods proved the efficiency of the proposed group mining process, which will directly reduce the latency of generating blocks in the proposed blockchain based on RM system.

In Chapter 5, we proposed a novel sidechain-based decentralized authentication scheme via optimized two-way peg protocol for smart community. By applying a optimized mainchain and private side blockchains, the local device authentication process can be effectively handled and a secured authentication information sharing procedure could be achieved. The optimized two-way peg protocol was identified to dynamically monitor the trustworthy of target smart device to ensure the security of the smart community during the information sharing procedure. Simulation results demonstrated that the proposed scheme could significantly reduce the authentication time by comparing with the existing blockchain-based method. Furthermore, the proposed optimized two-way peg protocol was also measured with different malicious authentication cases, and its practicability and feasibility in evaluating the trustworthy of each smart device have been confirmed. Moreover, compared with the blockchain-based authentication method and traditional sidechain method, the proposed sidechain-based scheme has improved the information management efficiency and reduced the storage burden at the gateway level.

6.2 Future Work

For the future work, some aspects of the proposed algorithms are still worthwhile to be further investigated. Some potential research works are summarized as follows.

6.2.1 The Proposed Blockchain-based Reputation Management System

In Chapter 4, we presented the proposed blockchain-based reputation management system for IoT routing protection. The proposed model efficiently detect the misbehaving routers by calculating the reputation values of each routers and blacklisting the malicious ones. There are two aspects that we can further improve the model.

Edge Computing Optimization As we mentioned in the Section 4.2, the proposed blockchain-based RM model is built on the edge layer due to the low data latency performance. However, we did not further design the technical relation between the blockchain technology and edge devices. There are many optimized edge computing algorithms designed for reducing the data latency and improving OoS performance. By applying suitable edge computing algorithms into the blockchain, the system efficiency and detection accuracy of the proposed blockchain-based model could be significantly improved.

Task Reallocation in the Proposed Group Mining PoW Consensus Mechanism In order to introduce the blockchain technology into the IoT routing protection, we optimized the traditional PoW consensus mechanism due to the resource-constrained nature of IoT devices. In the proposed group mining process, IoT devices are equally grouped for mining a same block based on their computational powers and locations. The inside group cooperation could be achieved by allocating the total nonce value range to all the group members based on their different computational powers. There is a certain scenario that some group members with high computational powers have already finished the allocated nonce task while other members are still working on their parts. In this circumstance, these devices will wait until other members finish, which will waste both time and resources. A better solution for this would be applying a suitable task reallocation into the group mining. When some devices finish their task earlier

than other group members, they can provide help to other with their extra available resources. With a certain smart contract of task reallocation, the mining task could be distributed to the members in a reasonable and intelligent way, and the efficiency of generating a block for a group could be noticeably improved.

6.2.2 The Proposed Sidechain-based device Authentication Scheme

In Chapter 5, we presented a sidechain-based device authentication scheme for smart community. The proposed sidechain model provides a local adaptive device authentication method for IoT devices in each smart system, and a decentralized structure for managing the authentication information sharing procedure. Moreover, the proposed optimized two-way peg protocol could evaluate the trustworthiness of the target IoT device to decide whether its authentication information is allowed to be shared with other systems. There are two orientations that we can further improve the work.

Optimized Two-way Peg Protocol Improvement In order to apply the sidechain technology into device authentication in IoT smart community, we proposed an optimized two-way peg protocol in order to prevent the worthless information attack during the information sharing process between the mainchain and side blockchains. The proposed protocol guarantees the data security for the whole community by dynamically monitoring the trust value of the target IoT device. However, in order to increase the detection accuracy and QoS performance, the protocol could be further enhanced by improving the trust evaluation algorithm. For example, the equations for evaluating the trust for a device could add more criteria to improve the detection accuracy performance. Moreover, we could apply the machine learning into the system. Based on the previous authentication records, the malicious devices and behaviors could be detected and predicted.

PoW Consensus Mechanism Optimization In the proposed sidechain-based device authentication model, PoW consensus mechanism has been applied to generate new blocks in both mainchain and side blockchains, which is considered as the most secured consensus mechanism in blockchain-related technology. However, the resource-constrained IoT devices cannot

meet the high computational power requirements cause by PoW consensus mechanism. The group mining PoW proposed in Chapter 4 may not be appropriate to the mining process at public mainchain due to the processing latency during the data transmission of the blockchain update. Thus, an optimized PoW consensus mechanism could be designed for the sidechain-based model in order to further enhance QoS performance.

Bibliography

- [1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar. A survey on iot security: Application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.
- [2] R. M. Gomathi, G. H. S. Krishna, E. Brumancia, and Y. M. Dhas. A survey on iot technologies, evolution and architecture. In *2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP)*, pages 1–5. IEEE, 2018.
- [3] S. Cho and S. Lee. Survey on the application of blockchain to iot. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, pages 1–2, Jan 2019.
- [4] D. Bastos, M. Shackleton, and F. El-Moussa. Internet of things: A survey of technologies and security risks in smart home and city environments. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pages 1–7, 2018.
- [5] J. Yu and Y. Kim. Analysis of iot platform security: A survey. In *2019 International Conference on Platform Technology and Service (PlatCon)*, pages 1–5, Jan 2019.
- [6] M. Gulzar and G. Abbas. Internet of things security: A survey and taxonomy. In *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, pages 1–6, Feb 2019.
- [7] K. Aurangzeb, S. Aslam, H. Herodotou, M. Alhussein, and S. I. Haider. Towards electricity cost alleviation by integrating rers in a smart community: A case study. In *2019 23rd International Conference Electronics*, pages 1–6, June 2019.
- [8] S. Mahmud, S. Ahmed, and K. Shikder. A smart home automation and metering system using internet of things (iot). In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pages 451–454, Jan 2019.
- [9] P. Hao, X. Wang, and W. Shen. A collaborative phy-aided technique for end-to-end iot device authentication. *IEEE Access*, 6:42279–42293, 2018.
- [10] S. Babkin and A. Epishkina. Authentication protocols based on one-time passwords. In *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 1794–1798, Jan 2019.

- [11] F. Kuo, H. Tschofenig, F. Meyer, and X. Fu. Comparison studies between pre-shared and public key exchange mechanisms for transport layer security. In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pages 1–6, April 2006.
- [12] D. Kim and J. Lee. Efficient and secure device clustering for networked home domains. *IEEE Transactions on Consumer Electronics*, 65(2):224–232, May 2019.
- [13] C. Kapoor, H. Singh, and V. Laxmi. A survey on energy efficient routing for delay minimization in iot networks. In *2018 International Conference on Intelligent Circuits and Systems (ICICS)*, pages 320–323, April 2018.
- [14] A. Raoof, A. Matrawy, and C. Lung. Routing attacks and mitigation methods for rpl-based internet of things. *IEEE Communications Surveys Tutorials*, 21(2):1582–1606, Secondquarter 2019.
- [15] I. Kechiche, I. Bousnina, and A. Samet. An overview on rpl objective function enhancement approaches. In *2018 Seventh International Conference on Communications and Networking (ComNet)*, pages 1–4, Nov 2018.
- [16] Tim Winter, Pascal Thubert, Anders Brandt, Jonathan Hui, Richard Kelsey, Philip Levis, Kris Pister, Rene Struik, Jean-Philippe Vasseur, and Roger Alexander. Rpl: Ipv6 routing protocol for low-power and lossy networks. Technical report, 2012.
- [17] G. Ma, X. Li, Q. Pei, and Z. Li. A security routing protocol for internet of things based on rpl. In *2017 International Conference on Networking and Network Applications (NaNA)*, pages 209–213, Oct 2017.
- [18] A. Kamble, V. S. Malemath, and D. Patil. Security attacks and secure routing protocols in rpl-based internet of things: Survey. In *2017 International Conference on Emerging Trends Innovation in ICT (ICEI)*, pages 33–39, Feb 2017.
- [19] L. Gao, Z. Zheng, and M. Huo. Improvement of rpl protocol algorithm for smart grid. In *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, pages 927–930. IEEE, 2018.
- [20] M. O. Farooq, C. J. Sreenan, K. N. Brown, and T. Kunz. Rpl-based routing protocols for multi-sink wireless sensor networks. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 452–459, Oct 2015.
- [21] B. Khemapataphan, A. Kheaksong, K. Thakulsukanant, and W. Lee. Weight ranking mechanism of energy balancing routing metric for rpl protocol in smart grid communications. In *2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 640–644, June 2017.

- [22] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson. A security threat analysis for the routing protocol for low-power and lossy networks (rpls). Technical report, 2015.
- [23] S. Sharma. A secure reputation based architecture for manet routing. In *2017 4th International Conference on Electronics and Communication Systems (ICECS)*, pages 106–110, Feb 2017.
- [24] P. Kamgueu, E. Nataf, and T. Ndie Djotio. On design and deployment of fuzzy-based metric for routing in low-power and lossy networks. In *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, pages 789–795, Oct 2015.
- [25] R. Mehta and M. M. Parmar. Trust based mechanism for securing iot routing protocol rpl against wormhole & grayhole attacks. In *2018 3rd International Conference for Convergence in Technology (I2CT)*, pages 1–6, April 2018.
- [26] A. Melnikov, J. Lee, V. Rivera, M. Mazzara, and L. Longo. Towards dynamic interaction-based reputation models. In *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pages 422–428, May 2018.
- [27] F. Bao, I. Chen, M. Chang, and J. Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transactions on Network and Service Management*, 9(2):169–183, June 2012.
- [28] H. Fang, L. Xu, and X. Huang. Self-adaptive trust management based on game theory in fuzzy large-scale networks. *Soft Computing*, 21(4):907–921, 2017.
- [29] N. B. Truong, T. Um, B. Zhou, and G. M. Lee. From personal experience to global reputation for trust evaluation in the social internet of things. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–7, Dec 2017.
- [30] I. Ud Din, M. Guizani, B. Kim, S. Hassan, and M. Khurram Khan. Trust management techniques for the internet of things: A survey. *IEEE Access*, 7:29763–29787, 2019.
- [31] J. Chen and Y. Xue. Bootstrapping a blockchain based ecosystem for big data exchange. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 460–463, June 2017.
- [32] J. Zhang, R. Shankaran, A. O. Mehmet, V. Varadharajan, and A. Sattar. A trust management architecture for hierarchical wireless sensor networks. In *IEEE Local Computer Network Conference*, pages 264–267, Oct 2010.
- [33] S. Goka and H. Shigeno. Distributed management system for trust and reward in mobile ad hoc networks. In *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1–6, Jan 2018.
- [34] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21, March 2018.

- [35] N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852, Sep. 2018.
- [36] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo. Toward a lightweight intrusion detection system for the internet of things. *IEEE Access*, 7:42450–42471, 2019.
- [37] X. Li, M. Wang, H. Wang, Y. Yu, and C. Qian. Toward secure and efficient communication for the internet of things. *IEEE/ACM Transactions on Networking*, 27(2):621–634, April 2019.
- [38] A. AlHammadi, A. AlZaabi, B. AlMarzooqi, S. AlNeyadi, Z. AlHashmi, and M. Shatnawi. Survey of iot-based smart home approaches. In *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, pages 1–6, March 2019.
- [39] H. F. Azgomi and M. Jamshidi. A brief survey on smart community and smart transportation. In *2018 IEEE 30th International Conference on Tools with Artificial Intelligence (ICTAI)*, pages 932–939, Nov 2018.
- [40] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu. Iot-based smart rehabilitation system. *IEEE Transactions on Industrial Informatics*, 10(2):1568–1577, May 2014.
- [41] B. Kuang, A. Fu, S. Yu, G. Yang, M. Su, and Y. Zhang. Esdra: An efficient and secure distributed remote attestation scheme for iot swarms. *IEEE Internet of Things Journal*, pages 1–1, 2019.
- [42] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.
- [43] A. Fayad, B. Hammi, and R. Khatoun. An adaptive authentication and authorization scheme for iot’s gateways: a blockchain based approach. In *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–7, Oct 2018.
- [44] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*, pages 1–1, May 2018.
- [45] Q. E. Abbas and J. Sung-Bong. A survey of blockchain and its applications. In *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, pages 001–003, Feb 2019.
- [46] B. Zhou, H. Li, and L. Xu. An authentication scheme using identity-based encryption blockchain. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 00556–00561, June 2018.
- [47] I. D. Alvarenga, G. A. F. Rebello, and O. C. M. B. Duarte. Securing configuration management and migration of virtual network functions using blockchain. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–9, April 2018.

- [48] O. Novo. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, April 2018.
- [49] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, 2008 [online]. Available: <http://bitcoin.org/bitcoin.pdf>.
- [50] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, and P. Wuille. Enabling blockchain innovations with pegged sidechains. Technical report, Accessed: 2014 [online]. Available: <https://www.blockstream.com/sidechains.pdf>.
- [51] Roberto Casado-Vara, Pablo Chamoso, Fernando De la Prieta, Javier Prieto, and Juan M Corchado. Non-linear adaptive closed-loop control system for improved efficiency in iot-blockchain management. *Information Fusion*, 49:227–239, 2019.
- [52] F. X. Olleros and M. Zhegu. Research handbook on digital transformations. Technical report, 2016.
- [53] C. Worley and A. Skjellum. Blockchain tradeoffs and challenges for current and emerging applications: Generalization, fragmentation, sidechains, and scalability. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1582–1587, July 2018.
- [54] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017.
- [55] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak. Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, 55(12):119–125, Dec 2017.
- [56] X. Liang, J. Zhao, S. Shetty, and D. Li. Towards data assurance and resilience in iot using blockchain. In *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, pages 261–266, Oct 2017.
- [57] J. Sotos and D. Houlding. Blockchains for data sharing in clinical research: Trust in a trustless world. *Intel, Santa Clara, CA, USA, Blockchain Appl. Note*, 1, 2017.
- [58] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri. Autonomic identity framework for the internet of things. In *2017 International Conference on Cloud and Autonomic Computing (ICCAAC)*, pages 69–79, Sep. 2017.
- [59] S. Amofa, E. B. Sifah, K. O. . Obour Agyekum, S. Abia, Q. Xia, J. C. Gee, and J. Gao. A blockchain-based architecture framework for secure sharing of personal health data. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6, Sep. 2018.

- [60] I. Stelliou, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys Tutorials*, 20(4):3453–3495, Fourthquarter 2018.
- [61] W. Bziuk, C. V. Phung, J. Dizdarević, and A. Jukan. On http performance in iot applications: An analysis of latency and throughput. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 0350–0355, May 2018.
- [62] H. Fang, X. Wang, and L. Hanzo. Learning-aided physical layer authentication as an intelligent process. *IEEE Transactions on Communications*, pages 1–1, March 2018.
- [63] S. K. Sharma and X. Wang. Live data analytics with collaborative edge and cloud processing in wireless iot networks. *IEEE Access*, 5:4621–4635, 2017.
- [64] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys Tutorials*, 21(2):1508–1532, Secondquarter 2019.
- [65] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.
- [66] Gianni Di Caro and Marco Dorigo. Mobile agents for adaptive routing. In *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, volume 7, pages 74–83. IEEE, 1998.
- [67] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):326, 2019.
- [68] Yoshiaki Kawase and Shoji Kasahara. Transaction-confirmation time for bitcoin: a queueing analytical approach to blockchain mechanism. In *International Conference on Queueing Theory and Network Applications*, pages 75–88. Springer, 2017.
- [69] Mehrdad Salimitari and Mainak Chatterjee. An overview of blockchain and consensus protocols for iot networks. *arXiv preprint arXiv:1809.05613*, 2018.
- [70] Guthemberg Silvestre, Sébastien Monnet, Ruby Krishnaswamy, and Pierre Sens. Caju: a content distribution system for edge networks. In *European Conference on Parallel Processing*, pages 13–23. Springer, 2012.
- [71] M. Qin, L. Chen, N. Zhao, Y. Chen, F. R. Yu, and G. Wei. Power-constrained edge computing with maximum processing capacity for iot networks. *IEEE Internet of Things Journal*, pages 1–1, June 2019.
- [72] A. Das and M. M. Islam. Securedtrust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, 9(2):261–274, March 2012.

- [73] Y. Zhang, S. Chen, and G. Yang. A study on hybrid trust evaluation model for identifying malicious behavior in mobile p2p. In *Peer-to-Peer Networking and Applications*, volume 9, page pp 578–587, May 2016.
- [74] M. K. Rahman and M. A. Adnan. Dynamic weight on static trust for trustworthy social media networks. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 62–69, Dec 2016.
- [75] M. Li, H. Tang, and X. Wang. Mitigating routing misbehavior using blockchain-based distributed reputation management system for iot networks. In *IEEE International Conference on Communications (ICC) 2019 Workshop*, pages 1–6, May 2019.
- [76] Kui Ren, Wenjing Lou, Kai Zeng, and Patrick J Moran. On broadcast authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 6(11):4136–4144, 2007.

Curriculum Vitae

Name: Min Li

Post-Secondary Education and Degrees: 2017 - present, M.E.Sc
Electrical and Computer Engineering
The University of Western Ontario
London, Ontario, Canada

2012 - 2016, B.Eng (Hons)
Automatics Engineering
Beijing University of Posts and Telecommunications
Beijing, China

Honours and Awards: The national college students' science and technology innovation project, China
The second award in 2015 Gao Tong Robot Cup, China

Related Work Experience: Teaching Assistant
The University of Western Ontario
2017 - 2019

Research Assistant
The University of Western Ontario
2017-2019

Publications:

- [1] M. Li, H. Tang and X. Wang, "Mitigating Routing Misbehavior Using Blockchain-based Distributed Reputation Management System for IoT Networks," IEEE International Conference on Communications (ICC) 2019 Workshop, pp. 1-6, 2019.
- [2] Y. Chen, Z. Wen, S. Wang, J. Sun and M. Li, "Joint Relay Beamforming and Source Receiving in MIMO Two-Way AF Relay Network with Energy Harvesting," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), pp. 1-5, 2015.