Choi, Bong-Gyeol; Jeong, EuiSeob; Kim, Sang-Woo

Article

Multiple security certification system between blockchain based terminal and internet of things device: Implication for open innovation

Journal of Open Innovation: Technology, Market, and Complexity

Provided in Cooperation with:
Society of Open Innovation: Technology, Market, and Complexity (SOItmC)

Suggested Citation: Choi, Bong-Gyeol; Jeong, EuiSeob; Kim, Sang-Woo (2019) : Multiple security certification system between blockchain based terminal and internet of things device: Implication for open innovation, Journal of Open Innovation: Technology, Market, and Complexity, ISSN 2199-8531, MDPI, Basel, Vol. 5, Iss. 4, pp. 1-16, https://doi.org/10.3390/joitmc5040087

This Version is available at:
https://hdl.handle.net/10419/241370

Journal of Open Innovation: Technology, Market, and Complexity

MDPI

Article

Multiple Security Certification System between Blockchain Based Terminal and Internet of Things Device: Implication for Open Innovation

Bong-Gyeol Choi [1], EuiSeob Jeong [2,*] and Sang-Woo Kim [2]

[1] ICNCAST Co., Seoul, 08506, Korea; hanbtap@gmail.com
[2] Seoul Capital areal area Branch, Korea Institute of Science and Technology Information, Seoul 02456, Korea; swkim@kisti.re.kr
* Correspondence: esjng@kisti.re.kr

Received: 23 August 2019; Accepted: 16 October 2019; Published: 17 October 2019

Abstract: As the number of Internet of Things (IoT) devices increases, services expand and illegal hacking and infringement methods become more sophisticated, an effective solution for blockchain technology is required as a fundamental solution to security threats. In this paper, we develop the security module of an IoT device based on blockchain technology that blocks hacking and information infringement and forms a multi-security blockchain system between the IoT device and the user device and we develop a user application. We contribute to addressing the security threats faced by IoT application services by developing a new method. In particular, we present some schemes for the development of a multi-security certification system based on blockchain for IoT security.

Keywords: security certification system; blockchain certification system; device third-party security certification system; multiple security certification system between IoT devices

1. Introduction

The role of blockchain in the fourth industrial revolution, which includes information communication technology (ICT) convergence, is becoming more important. As the fourth industrial revolution is characterized by hyper-connectivity and superintelligence, blockchain technology is helping to reliably interconnect people and things. Blockchains are helping to reduce transaction costs based on mutual transparency and reliability through ICT convergence [1–3]. The rapid growth of the Internet of Things (IoT) is creating new levels of connectivity and empowering platforms by connecting people and devices in new ways of creating value. The platform revolution will ultimately unpredictably change our world and will require creative and human innovation to solve the problems that these changes will produce throughout society [4].

Open innovation is a theory of innovation that allows companies to develop technologies by leveraging not only internal but also external ideas and R&D resources [5]. A focus of modern technology development is open innovation through digital convergence. For effective open innovation concepts and for the realization of IoT, cumulative and advanced use of big data is necessary [6,7]. Social innovation is more than simply capitalist innovation, in which profits are only received by a certain minority, it is a creative method of inducing change so that all humans can pursue happiness equally [8]. In particular, political commitment and a certain ability to shape broad policy frameworks are both conducive to the use and development of ICT in social services. A social services system is generally defined as the combination of interventions, programs, and benefits that are provided by government, civil society, and community actors to ensure the welfare and protection of socially or economically disadvantaged individuals and families. Often, the design and provision of

new innovative services can be initiated by private or third sector organizations, and subsequently incorporated into the public service delivery system [9].

According to the Future of Economy Report, which was compiled through the Institute of the Future (IFTF), a nonprofit think tank organization in the United States and includes interviews with over 4600 business leaders from over 40 countries and the results of workshops involving futurists and experts, IoT and blockchain are among the five major new technologies (5G and 6G communication, artificial intelligence (AI), IoT, and virtual currency) that will change the economy of the future. The seven dilemmas that business leaders need to be addressed to realize a frictionless economy in the future are security, data privacy, human–machine interaction, trust, transparency, governance, and environmental impact. Therefore, IoT, blockchain, and security have become important technologies. For security, a certificate is required for performing functions such as identification of a certificate holder and the prevention of fabrication or modification of a document. The need exists for a certificate authority to create, discard, and verify these certificates. Companies or organizations that provide certificate services issue, revoke, and verify certificates at the request of the customer through a certificate authority to enable customers to use certificates. These certificate management procedures are concentrated in a single independent certification authority, so security requirements for certification authorities, such as key management for certificate issuance, are also concentrated. In the case of an accredited certification body, security measures are sufficiently provided, but for a private certification body, sufficiently securing security measures is expensive. Therefore, efficient and secure security measures for certification authorities are required.

In Industry 4.0, a collection of new innovative concepts that are leading the manufacturing industry to the future, service applications that use IoT-based blockchain technology are increasingly widespread, including big data, virtual reality, and three-dimensional (3D) manufacturing. Things such as devices and appliances are connected to the Internet, and by using the Internet access records of the things, their movements, behavioral patterns, and other connected things are also analyzed and have evolved into AI services. In these service applications, the confidentiality and integrity of IoT security technology for verification without the risk of hacking are crucial [1–3]. IoT service is vulnerable to various security threats due to the nature of IoT technology. In particular, IoT service faces limited hardware specifications, such as low power consumption, low memory, etc., and tends to operate in an environment that is difficult to manage. IoT service faces various security threats, such as physical attacks, which prevent the reliable operation of the IoT service platform, or resulting in the provision of services based on erroneous information, finally resulting in an IoT service platform that has lost its accuracy [10].

A blockchain is also called a public transaction book and is a technique used to prevent hacking that may occur when trading virtual currency. In the case of existing financial companies, transaction logs are maintained on a centralized server, whereas blockchains send transactions to all users participating in the transaction and are used to prevent counterfeiting of data during each transaction. In the blockchain method, since all nodes share the same information, malicious nodes need to modify the contents of the blockchain of all nodes to arbitrarily modify contents, which is advantageous for security because the arbitrary modification is virtually impossible. Since the blockchain method shares all the data in the user device, when more than 50% of the users manipulate by collusion, a problem may arise of recognizing the manipulated data in all user devices. Blockchain technology has achieved open innovation for all users by decentralizing transaction contents. These open innovations provide traceability and transparency for distributed storage and transactions, resulting in lower reliability and transaction costs for information users. Users who use blockchain technology can achieve open and social innovation through the application and spread of various industries. IoT technology and security technology using blockchain-based big data improve productivity through automation of AI. This allows companies, governments, consumers, and suppliers to analyze more productive and efficient information. Such effective and efficient intelligent information is expected to be highly valued for the development of social innovation [8]. Table 1 summarizes the open innovation and

social innovation application services using the IoT and convergence technology based on blockchain technology in the Industry 4.0.

Table 1. Blockchain-technology-based open innovation and social innovation application services.

Category	Open Innovation	Social Innovation
Blockchain role in Industry 4.0	Reduce time and transaction costs, increase productivity	Creative
Blockchain, security	Decentralization, transparency, integrity	Trust, interaction
Internet of Things (IoT)	Value creation	Human happiness
Convergence technology	Patent technology, license sharing	Social service development
Service	Artificial intelligence (AI), big data, virtual reality, and three-dimensional (3D) manufacturing applications	Change, spread

IoT platform specification is expected to improve interoperability between heterogeneous terminals, networks, and applications, producing a variety of technical and administrative security threats. Security threats that can occur in an IoT environment include those in existing ICT environments. Confidentiality, integrity, and availability (CIA) are often seen as threats to the provision and use of legitimate services and are the three main components of information security [11].

In the IoT system field, security algorithms mainly focus on individual security for each IoT service environment component based on lightweight standardized encryption keys. Therefore, we provide a things certification server system for integrity verification of IoT and user devices. IoT devices can respond to various hacking threats when transmitting information, so we propose a system that includes an IoT device, a user device, user certification, and data encryption for providing a secure channel between IoT devices. The smart devices that have not been applied in the existing security use end-to-end IoT security module adapter blockchain security technology with this method, and the smart device and the service platform are based on the certification service.

Using the blockchain certification system, data record multi-divisioned mixed hashes using the mixed hashes of IoT devices, and device information can be stored in write once read many (WORM) to prevent loss of personal information during hacking. Therefore, developing a low-cost security certification system that can prevent the loss of personal information even if the system is hacked is necessary. Any IoT security certification project based on blockchain technology experiences difficulties in the application of integrated encryption algorithms and blockchain construction due to the lack of security awareness and the excessive cost to small- and medium-sized enterprises (SMEs). Therefore, we designed IoT device makers to design smart devices to communicate with security while reducing development work difficulty and creating high added value by applying a hacking prevention process. In this paper, we propose a multiple security certification system between a mobile terminal and an IoT device based on blockchain. We studied the hacking prevention system of the third-party security certification server (things certification center) that prevents all smart devices connected to the Internet from logging in and controlling IoT devices even if hacking occurs. Using blockchain and things certification systems, users contribute to building a transparent and reliable environment based on anti-repudiation technology for service use.

This paper is organized as follows. Section 2 summarizes provides a literature review. Section 3 outlines the design of multiple security systems between blockchain-based terminals and IoT devices. Section 4 summarizes the development plan of the blockchain-based multiple security certification system and provides suggestions for future research directions.

2. Literature Review and Research Framework

2.1. Literature Review

IoT is being used extensively for a wide range of business situations by providing consumers with convenience [12]. IoT has become an important source of smart change, including smart homes, smart cities, and smart industries [13]. It is leading the digital revolution in both academia and industry [14].

Blockchain technology can be a tool for social innovation as well as improve the efficiency of government [15]. Blockchain is attracting attention as next-generation financial technology due to the provision of security suitable for the information age [16]. According to the World Economic Forum report, global spending on blockchain solutions is estimated to reach USD $12.4 billion in 2022 and provides several benefits across industries, including automotive, banking, consumer goods, energy, healthcare, insurance, and railroad industries [17].

IoT and blockchain are key topics when discussing the direction of future technologies [18]. Prior studies have categorized and compared blockchain methodologies that provide security and protect privacy with respect to blockchain models, specific security objectives, performance, limitations, and computational complexity through a comprehensive survey of blockchain protocols for IoT networks [16,19,20].

IoT is evolving from an early to a mature stage, developing at a rapid speed, and increasingly more data are being transmitted and processed. As a result, the ability to manage devices deployed around the world has become more sophisticated and platforms are being developed that use blockchain technology to ensure data integrity [21–23].

Kodama and Shibata [6,7] suggested that the accumulation and advanced use of big data are necessary prerequisites for IoT realization and for open innovation to be effective. In other words, the combination of big data accumulation and business model creation with advanced use can make market-driving claims more plausible and improve the accuracy of demand coordination. As far as the business model is concerned, big data enables experimentation and simulation of alternative business models. Big data is a necessary condition for the IoT to be realized. Thus, IoT innovation is achieved only by the economy of connectivity, not by economies of scale or scope.

The rapid growth of IoT-based smart applications has created a need for security to manage and maintain data integrity, security integrity, and certification of IoT-based applications. Park et al. [24] proposed a system in which a plurality of gateways share certification information using a blockchain and issue certification tokens to perform mutual certification. By sharing the certification information distributed to the blockchain network, integrity and reliability of the certification token are ensured.

Park et al. [25] proposed a blockchain-based IoT device certification scheme that provides certification, integrity, and non-repudiation functions through analysis of existing certification protocols, ensuring secure certification by enabling operation in low-performance IoT devices.

Kim et al. [26] proposed a model to address the security vulnerability of sensor multi-platforms using blockchain technology using an empirical model. They also tried to overcome the weaknesses of sensor devices such as automobiles, airplanes, and close-circuit television (CCTV) using complete blockchain technology by measuring various security strengths.

Makhdoom et al. [27] systematically studied the characteristics of the IoT environment, including security and performance requirements and the development of blockchain technology. The security and performance benefits inherent in blockchain and blockchain IoT applications were compared to IoT requirements to identify gaps through mapping, addressing some of the critical challenges.

Yu et al. [14] investigated the general security and privacy issues of IoT and developed a framework for integrating blockchain with IoT. IoT data, various functions and certifications, and distributed payment can be guaranteed to a large extent.

Hammi et al. [28] suggested a unique distributed system that ensures robust identification and certification of devices to address this limitation, since creating an efficient centralized certification system is almost impossible due to the size and other functions of the IoT. They relied on the security

benefits provided by blockchain and wanted to protect data integrity and availability by creating secure virtual areas (bubbles) that could identify things and trust.

Khan and Salah [29] investigated major IoT security issues. In addition to the protocols used for networking, communications, and management, they reviewed the most commonly used security issues with the IoT tier architecture and outlined the security requirements for IoT along with existing attacks, threats, and state-of-the-art solutions.

Applications have been developed that apply blockchain to specific needs of IoT. Fernandez-Carames investigated how blockchain could affect traditional cloud-based IoT applications and studied the impact on the design, development, and deployment of blockchain IoT applications [30].

Various studies have been conducted on security authentication systems using blockchain. Most research focused primarily on preventing hacking. However, if hacked, data safety cannot be ensured. Therefore, we studied security certification to ensure data safety even if hacked. As the IoT market expands, security vulnerabilities also increase, so information integrity and vulnerabilities need to be addressed. Therefore, manufacturers of IoT devices can design them to enable smart and secure device communication while reducing development work difficulty. As such, research that can create high added value by applying anti-hacking process is needed.

2.2. Research and Analysis Framework

As the IoT market spreads, security vulnerabilities increase, so information integrity and vulnerabilities must be addressed. Existing research results focus on the individual security of each IoT service environment component based on lightweight standardized encryption key using security algorithms in IoT system areas. Table 2 summarizes previous studies.

Table 2. Summary of previous research on blockchain and Internet of Things (IoT) certification system.

Subject	Previous Research Content	Author and Year	Problem
Blockchain concept	- Blockchain model proposal	- Park et al. (2019) [24], Kim et al. (2019) [26]	Program certification management and maintenance security required
	- Security and privacy blockchain methodology	- Zhou et al. (2019) [21], Park and Park (2017) [16], Khan and Salah (2018) [29]	
	- Blockchain technology data integrity guarantee	- Hang and Kim(2019) [23], Watanabe and Fan (2019) [12]	
Certification frame	- Certification protocol integrity and non-repudiation - Sensor multi-platform security vulnerability - IoT environment characteristics system - Proposal of IoT and blockchain integration framework	- Park et al. (2017) [25], Ferrag et al. (2019) [20] - Kim et al. (2019) [26], Zhou et al. (2019) [21] - Tiago and Paula (2019) [30], Jo et al. (2018) [22], Hang and Kim (2019) [23] - Yu et al. (2018) [14], Panarello et al. (2018) [19]	System limitations with centralized certification
High efficiency and low cost	- Distributed certification system - Low cost and high efficiency: overcoming IoT capacity limitation - Solve cyberattack problems: app development	- Ul Hassan et al. (2019) [18] - Hammi et al. (2018) [28], Park and Park (2017) [16] - Hang and Kim (2019) [23], Ferrag et al. (2019) [20]	Stop the whole system when a problem occurs due to a cyber attack

The problems and limitations identified in the preceding studies are as follows:

(1) IoT, blockchain-based certification management programs, security management programs, etc. are integrated with the system, creating a high cost limitation.

(2) The IoT is mostly a central certification system that needs to be adjusted based on the traffic volume, or a distributed system is required.

(3) Cyberattacks can lead to maintenance or software problems that escalate, causing the entire system to hang or become paralyzed.

Therefore, a hacking prevention system for the Things certification center is needed that prevents all smart devices connected to the Internet from logging in and controlling IoT devices even if hacking occurs. In other words, manufacturers of IoT devices need research to create high added value by reducing the difficulty of development work while enabling communication between smart devices and applying an anti-hacking process.

Therefore, we used a blockchain-based distributed security concept design system as a research and analysis framework. To execute this conceptual design, a basic configuration of a blockchain certification system, IoT device things certification center certification system, and a multiple security certification system between IoT devices is presented here.

3. Security Certification System

The IoT and blockchain are changing the reality of modern society, both rapidly transforming societies both individually or in combination. Since the advent of blockchain and the IoT, the widespread computer network has changed dramatically. blockchain is suitable for protecting data transactions between logical nodes with a good warranty. The IoT is expected to offer a variety of benefits to a wide range of businesses by offering consumers increased convenience. However, IoT security is still facing many problems.

Many of the things we use each day are equipped with electronic devices and protocol sets, and interacting with and connected to the Internet. People can process and exchange data without human intervention. Given this complete autonomy, these things must not only guarantee the integrity of the exchanged data but also recognize and authenticate each other. If not authenticated, it becomes a malicious user and a malicious object. Due to the size and other features of the IoT, it is almost impossible to create an efficient centralized certification system.

This section presents the system configuration of the secure channel, an IoT device, and terminal user certification and data encryption technology to manage the various hacking threats when transmitting information between IoT devices. IoT devices that have not been applied to security use end-to-end IoT security module adapter technology; we propose an IoT device and service platform system using multiple security as a blockchain-based security certification system provided by a things security certification management module. As a result, manufacturers of IoT devices can design security-enabled IoT device communications to reduce development effort and create high-value products that include anti-hacking processes.

3.1. Conceptual Design of Security Certification System

With regard to user certification technology, the user receiving the service must be certified to be an appropriate user given the non-face-to-face characteristics of online services. If the user cannot be properly authenticated, personal information may be exposed according to the type of service, so it is essential to secure safety and reliability through user certification. The factor used to determine whether a user receiving a service is legitimate is called a certification factor. In general, certification technologies for controlling an IoT device using an existing mobile terminal primarily use certification information such as an identification (ID) and a password, and secondarily use a security card or biometric information (fingerprint, iris, etc.). However, when such certification-related information is hacked, the certification information may be leaked, or the security check program logic may be disabled through fabrication, which refers to the insertion of counterfeit goods into the system by non-authorized persons as part of a security attack, which is an attack on authentication, or modification, which is a security attacks that involves illegal changes as well as illegal access by non-authorized people, of the program. The conceptual design of the multi-security certification system between the terminal and the IoT device based on blockchain is composed of an IoT device, a

user device, a certification server, and blockchain as shown in Figure 1. The detailed description of each component is summarized as shown in Table 3.

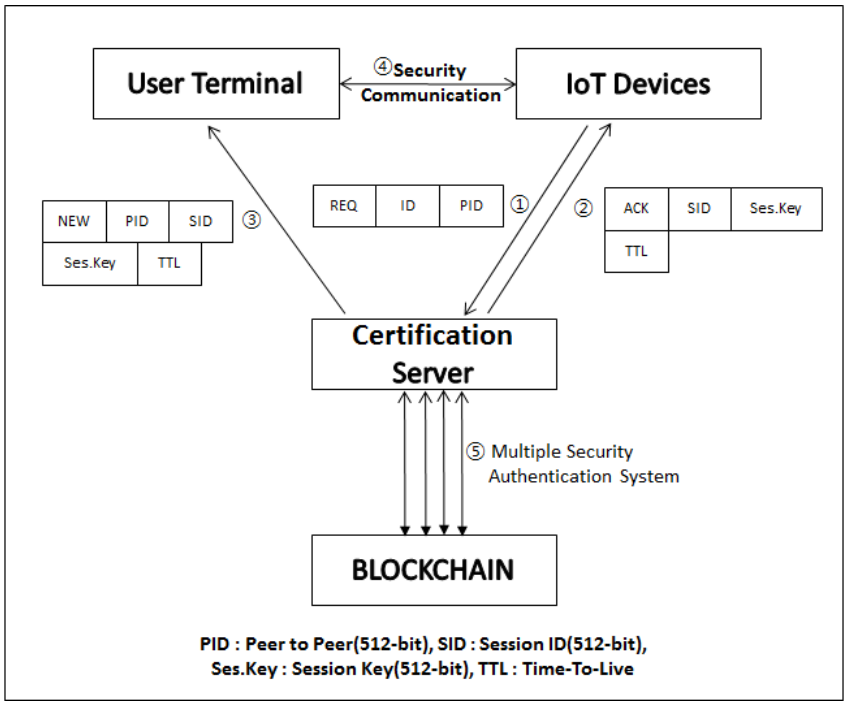

Figure 1. Conceptual Design of Security Authentication System.

Table 3. Role of multiple security certification system components between IoT devices.

Component	Description
IoT devices	- Operation of IoT electrical and electronic equipment is controlled by IoT communication with a user device through a wired or wireless Internet network such as a voice communication network, a data communication network, or a Wi-Fi network - IoT communication refers to the evolved form of ubiquitous sensor networks (USNs) and machine to machine (M2M). If M2M is the main purpose of communicating with a communication device (end device), the IoT would expand the scope of things to include security devices, smart appliances, air conditioners, closed circuit television (CCTV), lighting devices, smart factories, smart farms, and other means of communicating with people
User device	- A terminal that remotely controls the corresponding IoT device by communicating with the IoT device through a wired or wireless Internet network - Smart phones, tablets, wearable devices, and mobile terminals such as personal digital assistant (PDA), desk top computers, and notebook computers - An application program running in conjunction with a certification server or IoT device is installed
Certification server	- Registration of IoT device to be used for remote control of the mobile terminal - If a remote control request is sent from the user device to the IoT device, verify the legitimacy of this user device - Approval of IoT device remote control by the user device when authenticating the validity

Table 3. *Cont.*

Component	Description
Blockchain	- Decentralized electronic ledger or database platform - A digital record or transaction on a thread is called a block - Allows a set of publicly or controlled users to participate in the electronic ledger - Each time stamp is applied and generates an unchangeable record for the transaction associated with the previous one

In this system, when a user device generates and registers a registration hash value, the registration hash value is transmitted to the certification server, which receives it and records it in the blockchain. The registration hash value is transmitted directly to the certification server by the user device that generated it. The registration hash value may be provided to the certification server via the IoT device. That is, when the user device transmits the registration hash value to the IoT device, the IoT device receives the registration hash value and delivers it to the certification server. The blockchain authentication systems use mixed hashes and device information from IoT devices to store data record multi-divisioned mixed hashes in WORM to prevent loss of personal information during hacking.

3.2. Bblockchain Certification System

The blockchain certification system proposed in this paper can be shown in Figure 2. Information and communication services provided on a wired or wireless communication network are provided to a specific user who has an agreement with a service provider (operator). The user registers the ID and password through the certification process at the time of the initial user registration and accesses the service site through user certification of the operator system by inputting or automatically transmitting the registered ID and password when using the service.

To prevent the user account from being hacked, financial services and the like conduct a user certification procedure using an authorized certificate. However, when the operator system is hacked, there is a risk of theft. The risk of theft is increased when many user devices are registered and used for user convenience. Punishment of criminal behavior due to the theft of user accounts is necessary. When the operator system is hacked, following up and restoring are challenging since the log record can be manipulated.

Therefore, the blockchain certification system manages user registration and the login records of each user so that it cannot be manipulated artificially using the blockchain, and can be used as post-verification data. The blockchain certification system consists of an integrated security platform and demonstration technology that relays the multiple certification information pieces (patients and caregivers, medical services and healthcare providers, etc.) on the basis of blockchain. It is essential to design and operate an integrated automated identifier issuance and management system based on blockchain to prevent unauthorized access between IoT service things and things.

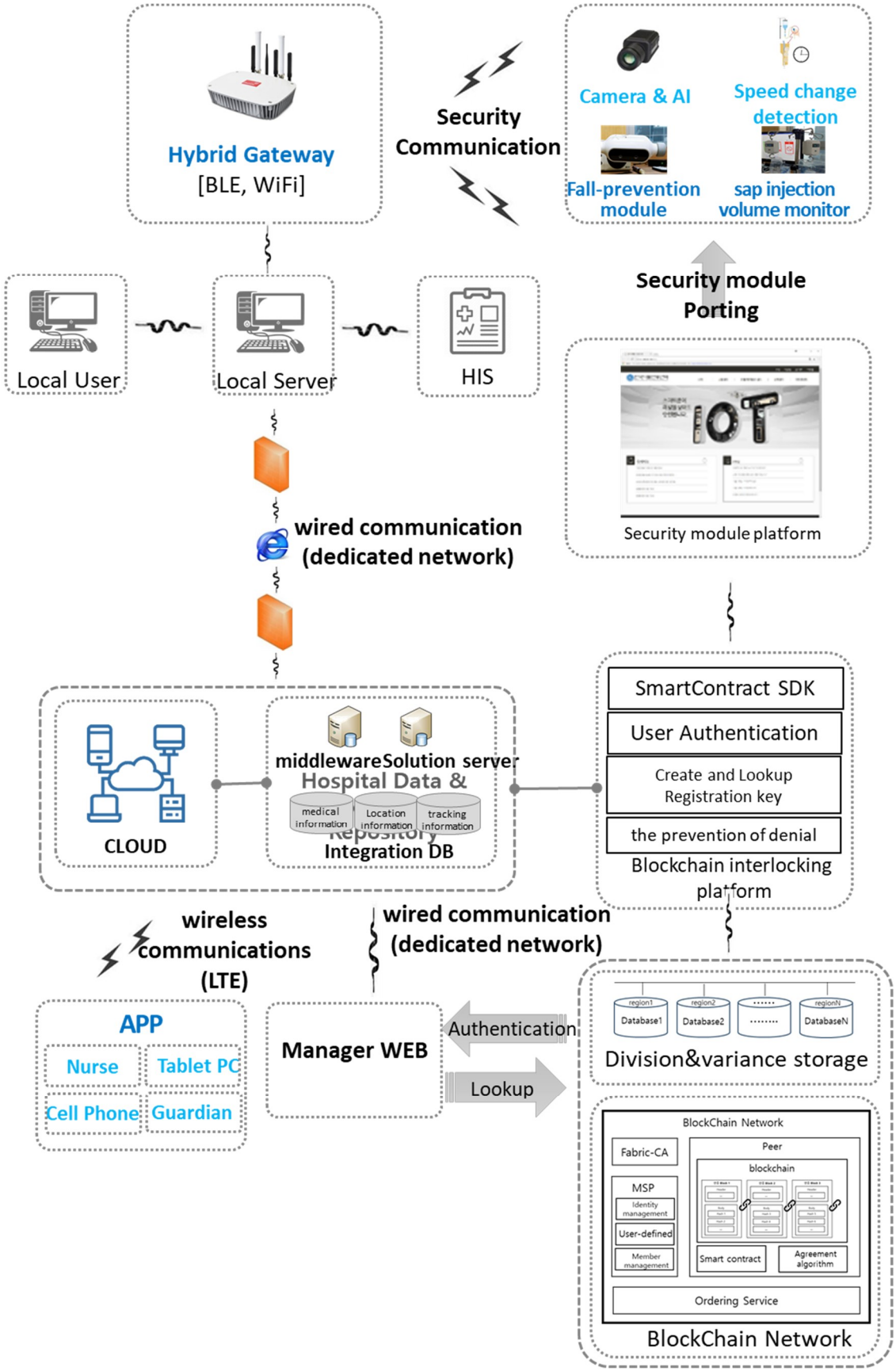

Figure 2. Blockchain Certification System.

3.3. IoT Device Third-Party (Things Certification Center) Security Certification System

With the advancement of the IoT, society is being continuously filled with new products and services in various fields such as smart homes, smart home appliances, smart cars, smart grids, health care, and wearable devices. One of the biggest challenges in introducing IoT is security and privacy. Many devices are constantly in the process of creating, collecting, distributing, managing, and using vast amounts of information over the Internet connection. In this process, vulnerable security systems face two problems: public safety threats and privacy violations. As a method to solve the problem of IoT service, we propose the IoT device things certification center certification system shown in Figure 3.

When the terminal logs in to the IoT device, hacking may occur at the application layer. First, the IoT device and mobile device user certification and a data encryption communication certification system that can handle various hacking threats in the communication between the mobile device and the IoT device should be applied. Second, an end-to-end security adapter module technology needs to be developed that can easily and quickly apply IoT security certification. Third, we need to develop the IoT security blockchain certification system through the IoT security relay management platform. Fourth, it is necessary to minimize the threat of a hacking attack caused by the encryption key theft by providing the encryption session key and to strengthen certification when the user certification key is lost or stolen. Finally, in case of hacking, the third-party security certification server (things certification center) should safely control the IoT device with communication, encryption, hacking recognition, notification, and packet sniffing protection modules (interceptions) (this is a security attack on the credibility of unauthorized access by unauthorized persons), which verify the integrity of the mobile terminal and the IoT device.

This system is a study of anti-hacking technology that introduces a third-party security certification server (things certification center) and a blockchain certification system between smart devices and IoT devices under the assumption that all mobile or Internet terminals are hacked. Existing recognition technologies (ID, pass word (PW), Media Access Control (MAC), fingerprint, iris recognition, etc.) stored in user accounts, unique identification numbers and codes, smart terminals, and IoT devices can all be disabled when hacking IoT devices. To prevent hacking, a verification process of certification data for smart devices and certification servers should be followed. Smart devices and certification servers should enforce the use of only smart devices authorized through certification applications or certification modules.

Researching and developing logic modules in preparation for hacking is necessary. The logic module includes source cord random modification check, sniffing packet stealing prevention logic, packet manipulation prevention parity check, security key capture, physical code, and prevent a change of security logic. In this case, hacking prevention process technology should be applied. Finally, the system is a hash of a mixture of information from mobile and thing devices. Certification data relay management and encryption key data record, according to each device's risk, are multi-divisioned and stored in WORM format in the blockchain distributed storage system.

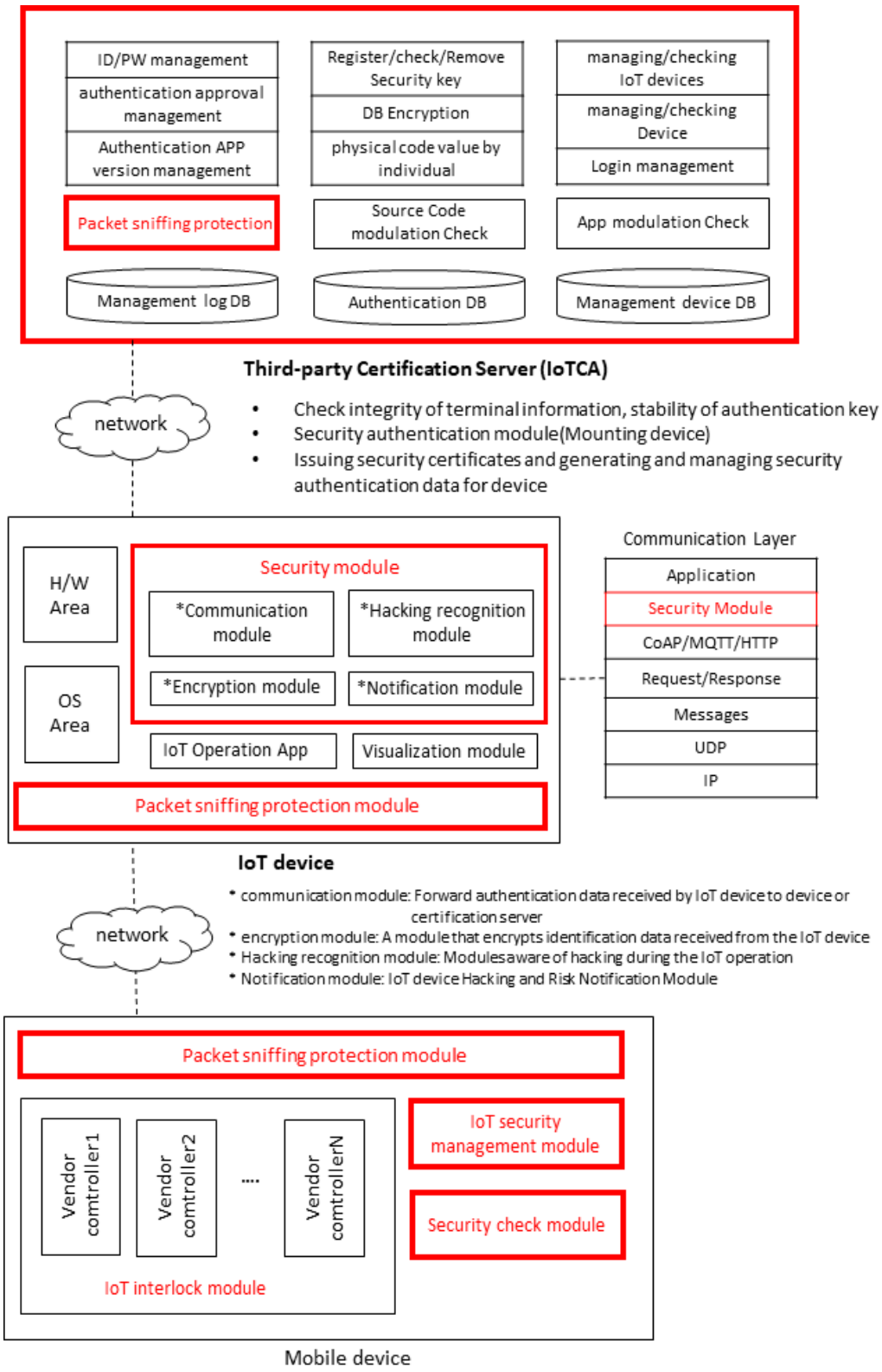

Figure 3. IoT Device Third-party (Things Certification Center) Security Certification System.

3.4. Multiple Security Certification System between IoT Devices

Figure 4 depicts a flow chart showing the IoT device control request and approval process [31]. The IoT application is executed in the user device and the IoT device is logged in. At this time, if

the login is not normally performed in the IoT device, the number of failures is counted, and the certification process is resumed from the beginning by proceeding to the initial certification application step. If the IoT device is properly logged in, the IoT device accepts the login of the user device.

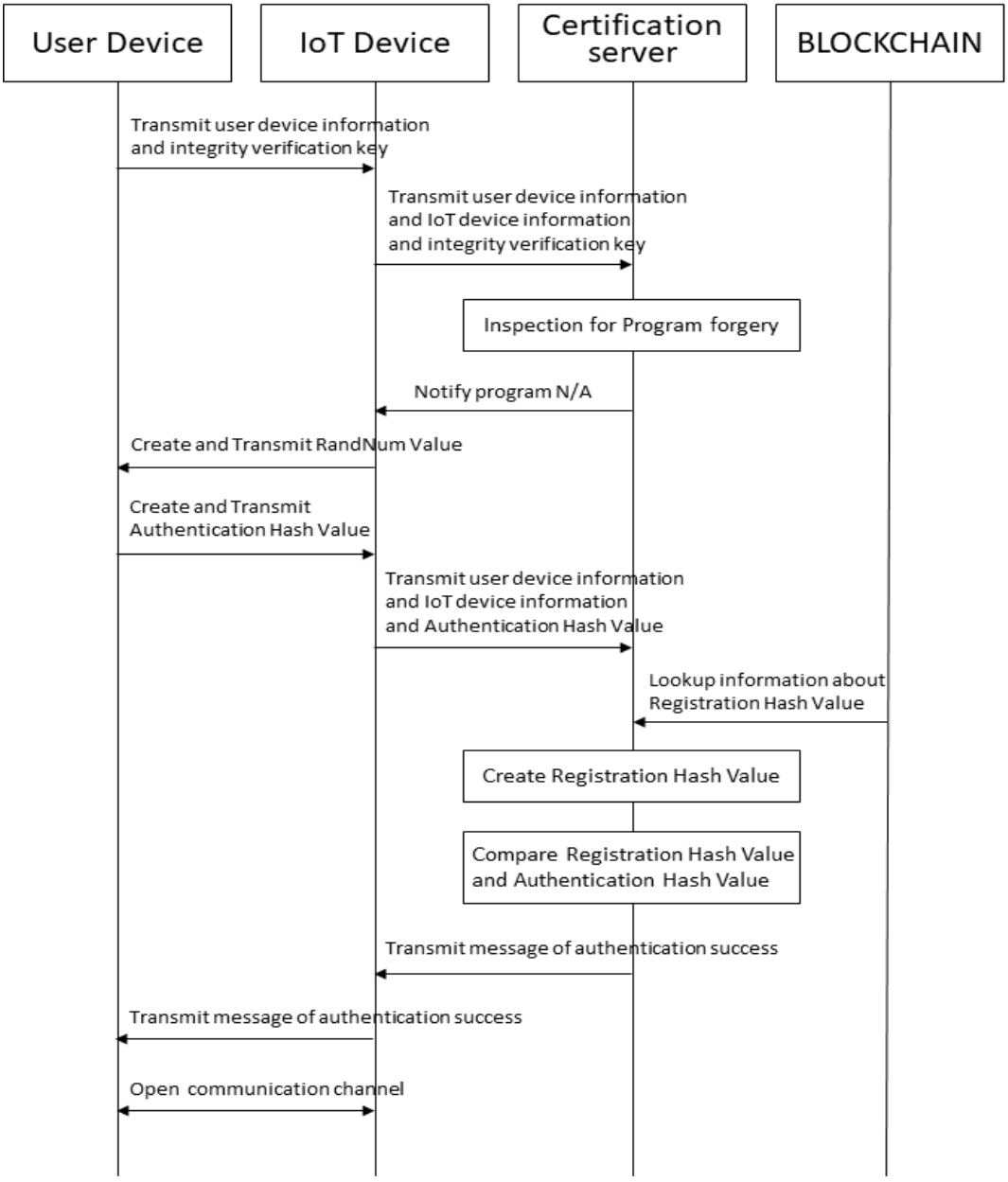

Figure 4. Multiple security certification system between IoT devices.

When the login is approved, the user device transmits the user device information and the integrity verification key (e.g., version information, checksum, etc.) of the IoT app installed on the user device to the IoT device. The IoT device transmits the user device information, the integrity verification key, and the IoT device information received from the user device to the certification server.

The certification server checks the integrity verification key received from the IoT device and confirms that no abnormality exists in the IoT app of the user device, which may include, for example, checking whether the corresponding IoT app is fabricated or modified by hacking or the like. The integrity verification key inspection may be performed by comparing the integrity verification key with the IoT application integrity verification key of the user device previously registered in the

management terminal database of the certification server. As a result of the integrity verification key check, if an error exists in the IoT app, the certification server sends a certification failure message to the IoT device. Then, the IoT device transmits the received certification failure message to the user device.

If no abnormality exists in the IoT application, the certification server notifies the IoT application of the user device that no abnormality exists. Then, the IoT device generates a random number value through the random number generator and transmits it to the user device. When the random number is received from the IoT device, the user device generates a certification hash value using the random number and transmits it to the IoT device. Here, the certification hash value is a value generated using the first hash, the second hash, or the third hash as certification means for confirming the validity of the user device, or a combination of at least two of the first hash, the second hash, and the third hash. The certification hash value may be a value generated by further combining a random number value.

The IoT device transmits the certification hash value, user device information, and IoT device information received from the user device to the certification server. When the certification hash value is received from the IoT device, the certification server generates the registration hash value using the identification information registered in the management DB, the random number value generated in the IoT device, and the related registration hash value information recorded in the blockchain.

Specifically, when the certification server receives a request for control approval from the IoT device (when receiving the certification hash value from the IoT device), the certification server browses the related registration hash value information (information on the combination method) recorded in the blockchain. The timestamp recorded on the blockchain proves and records that the hash existed at the time for the data to enter the hash. Each time stamp contains a previous time stamp in the hash to form a chain, with each additional time stamp reinforcing the previous time stamp [32].

Then, the certification server compares the certification hash value generated by the user device with the registration hash value and determines the legitimacy of the certification hash value (legitimacy of the user device). If the certification hash value does not match the registration hash value, the certification server sends a certification failure message to the IoT device. The certification failure message is transmitted from the IoT device to the user device again. If the certification hash value matches the registration hash value, the certification server authenticates the user device logged in to the IoT device as a legitimate user device and transmits a certification success message to the IoT. When the certification server transmits a certification success message to the IoT device, the IoT device notifies the user device that the certification succeeded. An encrypted communication channel is established between the IoT device and the user device, and the user device can control the IoT device remotely.

4. Conclusions

4.1. Implications

IoT devices are widely used in smart homes and smart cities, and in the automotive, healthcare, and aerospace industries. However, recent hacking has caused many problems. The purpose of this study was to overcome the security weaknesses of existing IoT devices by using emerging blockchain technologies. With this method, it is possible to block the use of certification-related information, even if it is hacked, to enhance the integrity and security of the security certification process between the user device and the IOT device without a certification card or Universal Serial Bus (USB) certification device, and to provide a multi-security certification system based on blockchain that can be prevented.

The core of modern technology development is open innovation through digital convergence, which is necessary to realize the IoT. Internal MISSING and blockchain, which have developed security technology by using external ideas and R&D resources, together can be called open innovation. The development of service applications using IoT-based blockchain technology in Industry 4.0, a new and innovative concept that leads the manufacturing industry into the future, has produced social innovation.

The proposed blockchain certification system, the IoT device third-party (things certification center) multiple security certification system between IoT devices, will affect the industry. In the blockchain certification system, it is essential to design and operate an integrated automated identifier issuance and management system based on a blockchain to prevent mutual unauthorized access between IoT service things and things. In the IoT device third-party (things certification center) security certification system, hacking can occur at the application layer when logging into an IoT device on a mobile terminal. In case of hacking, the third-party security certification server (things certification center) should safely control the IoT device with the communication, encryption, hacking recognition, notification, and packet sniffing protection modules, which verify the integrity of the mobile terminal and the IoT device. In a multiple security certification system between IoT devices, when a user device generates and registers a registration hash value, the registration hash value is sent to the certification server, which receives it and records it in the blockchain. The registration hash value is directly transmitted to the certification server by the user device that generated the certification hash value. The registration hash value may be provided to the certification server via the IoT device. That is, when the user device transmits the registration hash value to the IoT device, the IoT device receives the registration hash value and delivers it to the certification server.

The certification server verifies the integrity of user and IoT devices and provides certification between smart devices and mobile devices. We need to expand the things certification center blockchain certification system through anti-hacking process technology, which includes source cord random fabrication/modification check, sniffing packet stealing prevention logic, packet manipulation prevention parity check, security key capture, physical code, prevent a change of security logic, all included in a logic module for hacking. To enhance the security of intelligent smart devices, mixed hashes in smart device information should be used to prevent malicious unauthorized access. With the development of artificial intelligence, a person's identification number plays an important role in protecting personal information. Among the information that can be used to identify an individual, in particular, the identification of the device used by a group or an individual is one of the important information assets to be protected by law. A process of verifying reliable transactions between the IoT and user terminals is needed due to the introduction of blockchain-based online non-face-to-face services and intelligent artificial intelligence. Therefore, the framework of this study (conceptual design) is expected to play a role in the development of the smart industry. Continuously integrated security, blockchain, and edge-hybrid algorithms will evolve.

4.2. Limitations

The design and delivery of new and innovative services often start with individuals or third parties and can be integrated into public service delivery systems. We conducted research on things security and blockchain technology in the device environment to prevent hacking. In this paper, we proposed the design of a secure multiple security system even during hacking. Constraints exist in the demonstration of the proposed design, which will require further study.

Direct application to various industries requires research to overcome difficulties due to various environmental factors. We will continue research to apply the proposed security system design to the smart healthcare industry. Based on this research, additional research is needed to overcome the limitations of independent R&D analysis applied to various fields such as smart cities, smart manufacturing, smart distribution, smart agriculture, and smart finance.

Author Contributions: B.-G.C. is responsible for writing—original draft preparation. E.J. is responsible for data curation and supervision. S.-W.K. is responsible for validation.

Funding: This research was supported by the Ministry of Science, and ICT (Koita-clister-2019-core-05).

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

References

1. Xu, M.; Kim, S.H.; David, J.M. The Fourth Industrial Revolution: Opportunities and Challenges. *Int. J. Financ. Res.* **2018**, *9*, 90–95. [CrossRef]
2. Schwab, K.; Davis, N. *Shaping the Fourth Industrial Revolution*; World Economic Forum: Cologny, Switzerland, 2018; pp. 91–93.
3. Brant, J.; Lohse, S. *The Open Innovation Model*; International Chamber of Commerce: Paris, France, 2014; pp. 3–24.
4. Parker, G.G.; van Alstyne, M.W.; Choudary, S.P. *Platform Revolution*; W. W. Norton & Company: New York, NY, USA, 2017.
5. Helfat, C.E. Open Innovation: The New Imperative for Creating and Profiting from Technology. *Acad. Manag. Perspect.* **2006**, *20*, 86–88. [CrossRef]
6. Kodama, F.; Shibata, T. Beyond fusion towards IoT by way of open innovation: An investigation based on the Japanese machine tool industry 1975–2015. *J. Open Innov. Technol. Mark. Complex.* **2017**, *3*, 23. [CrossRef]
7. Kodama, F.; Shibata, T. Demand articulation in the open-innovation paradigm. *J. Open Innov. Technol. Mark. Complex.* **2015**, *1*, 2. [CrossRef]
8. Mulgan, G. *Social Innovation: How Societies Find. The Power to Change*; Bristol University Press: Bristol, UK, 2019.
9. Misuraca, G.; Pasi, G.; Abadie, F.; Kucsera, C.; Virginillo, M. *Exploring the Role of ICT-Enabled Social Innovation to Support. The Modernisation of EU Social Protection Systems*; Publications Office of the European Union: Luxembourg, 2017; pp. 19–64.
10. Kim, T.; Kim, J.; Lee, S.; Ahn, I.; Song, M.; Won, K. An automatic protocol verification framework for the development of wireless sensor networks. In Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TridentCom '08), Innsbruck, Austria, 18–20 March 2008; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2008; p. 5.
11. Hu, P.; Ning, H.; Qiu, T.; Song, H.; Wang, Y.; Yao, X. Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 1143–1155. [CrossRef]
12. Watanabe, H.; Fan, H. A Novel Chip-Level Blockchain Security Solution for the Internet of Things Networks. *Technologies* **2019**, *7*, 28. [CrossRef]
13. Alamri, M.; Jhanjhi, N.Z.; Humayun, M. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 244–258.
14. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wirel. Commun.* **2018**, *25*, 12–18. [CrossRef]
15. Jun, M.S. Blockchain government—A next form of infrastructure for the twenty-first century. *J. Open Innov. Technol. Mark. Complex.* **2018**, *4*, 7. [CrossRef]
16. Park, J.H.; Park, J.H. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry* **2017**, *9*, 164. [CrossRef]
17. Warren, S.; Treat, D. *Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits*; White Report; World Economic Forum: Cologny, Switzerland, 2019.
18. Ul Hassan, M.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput.* **2019**, *97*, 512–529. [CrossRef]
19. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
20. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things, J.* **2019**, *6*, 2188–2204. [CrossRef]
21. Zhou, Y.; Liu, T.; Tang, F.; Wang, F.; Tinashe, M. A Privacy-Preserving certification and Key Agreement Scheme with Deniability for IoT. *Electronics* **2019**, *8*, 450. [CrossRef]
22. Jo, B.; Khan, R.; Lee, Y.S. Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring. *Sensors* **2018**, *18*, 4268. [CrossRef]

23. Hang, L.; Kim, D.H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors* **2019**, *19*, 2228. [CrossRef] [PubMed]
24. Park, H.; Kim, M.; Seo, J. IoT Multi-Phase certification System Using Token Based Blockchain. *KIPS Trans. Comput. Commun. Syst.* **2019**, *8*, 139–150.
25. Park, B.; Lee, T.; Kwak, J. Blockchain-Based IoT Device certification Scheme. *J. Korean Inst. Inf. Secur. Cryptol.* **2017**, *27*, 343–351.
26. Kim, S.; Kim, U.; Huh, J. A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security. *Energies* **2019**, *12*, 402. [CrossRef]
27. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–2791. [CrossRef]
28. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based certification system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
29. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
30. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
31. Yoo, Y.; Choi, B. Multi-Security Authentication System and Method between Blockchain-based Mobile Devices and IoT Devices PCT/KR2018/010193 (03.SEP.2018, PCT18011ICN).
32. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, pp. 2–3. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 October 2019).