energies

Article

A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security

Seong-Kyu Kim [1], Ung-Mo Kim [1] and Jun-Ho Huh [2,*]

[1] School of Electronic and Electrical Computer Engineering, Sungkyunkwan University, Suwon 110-745, Korea; guitara7@skku.edu (S.-K.K.); ukim@skku.edu (U.-M.K.)

[2] Department of Software, Catholic University of Pusan, Busan 46252, Korea

* Correspondence: 72networks@pukyong.ac.kr or 72networks@cup.ac.kr

Received: 26 December 2018; Accepted: 25 January 2019; Published: 27 January 2019

Abstract: IoT devices are widely used in the smart home, automobile, and aerospace areas. Note, however, that recent information on thefts and hacking have given rise to many problems. The aim of this study is to overcome the security weaknesses of existing Internet of Things (IoT) devices using Blockchain technology, which is a recent issue. This technology is used in Machine-to-Machine (M2M) access payment—KYD (Know Your Device)—based on the reliability of existing IoT devices. Thus, this paper proposes a BoT (Blockchain of Things) ecosystem to overcome problems related to the hacking risk of IoT devices to be introduced, such as logistics management and history management. There are also many security vulnerabilities in the sensor multi-platform from the IoT point of view. In this paper, we propose a model that solves the security vulnerability in the sensor multi-platform by using blockchain technology on an empirical model. The color spectrum chain mentioned in this paper suggests a blockchain technique completed by using the multiple-agreement algorithm to enhance Thin-Plate Spline (TPS) performance and measure various security strengths. In conclusion, we propose a radix of the blockchain's core algorithm to overcome the weaknesses of sensor devices such as automobile, airplane, and close-circuit television (CCTV) using blockchain technology. Because all IoT devices use wireless technology, they have a fundamental weakness over wired networks. Sensors are exposed to hacking and sensor multi-platforms are vulnerable to security by multiple channels. In addition, since IoT devices have a lot of security weaknesses we intend to show the authentication strength of security through the color spectrum chain and apply it to sensor and multi-platform using Blockchain in the future.

Keywords: blockchain; IoT; KYD; M2M; IOTA (MIOTA); whitechain; authentification; rainbowchain; computer architecture

1. Introduction

In the world of the Internet of Things (IoT), various users provide new services and communicate with each other. According to Gartner's report, the number of smart devices such as tablet PCs, mobile phones, and laptops will reach 30 billion by 2020; IoT devices whose number is about four times the size of the global population will be installed and operated so that they can communicate without intervention by their users, thereby creating a new world [1–3]. In addition, IoT devices will be able to communicate with each other without user intervention and provide convenient services. If an IoT device is hacked, however, such is expected to result in disasters in the SOC (railway, airplane, and ships) and financial sectors [4,5].

In Russia, domestic and overseas CCTV videos are watched and recorded in real time, and CCTV videos of personal and public spaces such as department store space are hacked, recorded, and circulated. Although in Korea, sites providing those videos are blocked as harmful, it is possible for foreigners to watch all hacked CCTV videos in their countries.

The biggest problem with IoT security is that "there is no biggest problem [6–8]." IoT has more complex specifications than traditional information technology (IT) infrastructure. It is much more likely to consist of various hardware and software products. According to Forrester senior analyst Merit Maxim, the three main areas of IoT security are device, network, and back-end, all of which can be a target and we should be careful of.

He added that, due to the Mirai botnet incident that took place in 2016, the view on IoT security threats has changed; 92% said that the issue will continue to be serious. In this case, a vast number of IoT devices whose security is not guaranteed, mainly digital security cameras, were used by robotic botnets for Distributed Denial of Service (DDoS) attacks. The problem is that the effort to solve this is still in its infancy stage Figure 1. Only 23% of the security experts who monitored the connected devices in the office checked for the presence of malicious code. Two-thirds of the respondents said they do not know the total number of connected devices coming into the network. Edge computing is also an important concept for IoT. This is because many applications—especially those that do not tolerate delays—can only take action with shorter cycle of history data coming from the endpoint to the data center and back again. As a result, IoT hubs and other devices will occupy some of the computation and management slack, and additional places to implement security are added within the stack. In this paper, we make a proposal based on this blockchain-based BoT (Blockchain of Things).

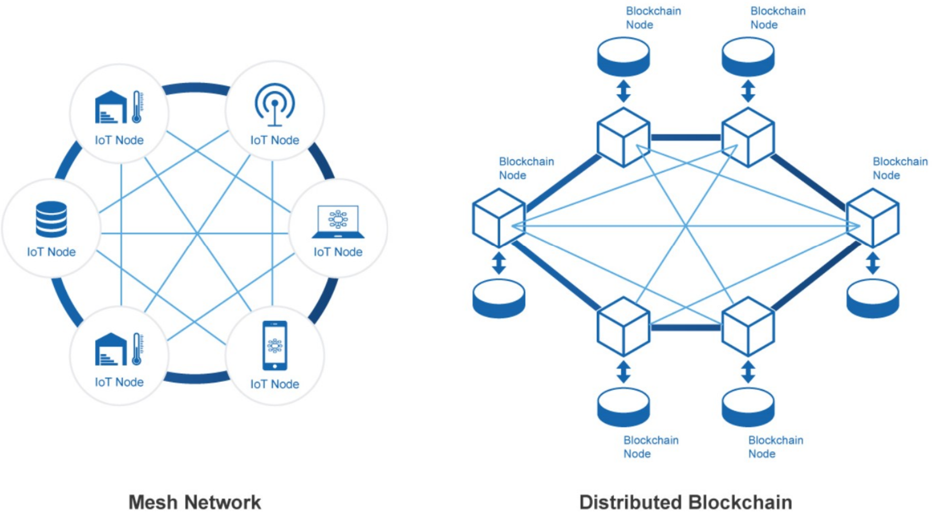


Figure 1. Blockchains applied to the Internet of Things (IoT).

In addition, for sensor multi-platforms, 10 billion IoT devices are expected in 2014, and more than 20 billion, in 2017 [8,9]. Likewise, blockchain technology is forecast to be applied in various fields of the Internet, and blockchains can be introduced for data management, transaction, or authentication. For the data management of the blockchain, the blockchain can be used to store and manage the data collected by the Internet of Things. If the collected data hash value for audit is stored in the blockchain, it is possible to check for abuse, modification, or deletion of the collected data by an unauthorized person. The collected data is stored in a separate repository (database, cloud storage, etc.), and metadata such as the hash value necessary for managing the collected data is stored in the blockchain. The network also stores the access policy (policy or rule) for access data in the blockchain so that only authorized users can access it [10]. IoT for transactions enables transactions without a third party by using the blockchain to provide a secure trading environment for data collected from sensors. The authentication keys (public keys) of the IoT sensor multi-platform devices are stored in the blockchain to perform key management such as registration, renewal, and revocation and verification to use the blockchain to verify the authentication between the IoT devices if necessary.

Therefore, the blockchain technology can be applied and used in various fields. We propose a methodology and a model to overcome the security weakness through comparison with the existing blockchain by presenting a color spectrum chain among consensus algorithms. The sensor multi-platform is highly vulnerable to hacking because of the concentration of devices between various heterogeneous devices. We propose a model for verifying and authenticating using blockchain radix rather than the authentication key scheme.

2. Background Knowledge

The blockchain is being regarded as a most effective technology for maintaining the security of public account books and according to the United Nations (UN), it holds a high potential in the age of the 4th Industrial Revolution. Bank of Korea (2016) described the technology as "a technology that dispersively maintains one's account book for the online (P2P) transactions [11–13]. Also, Gartner Research in the US forecasted that this futuristic technology will be used widely for businesses which are expected to reach the value of up to 10 billion US dollars by 2022 [14]. The blockchain technology was originally developed and used for the transaction of bitcoins providing a higher level of security and anonymity but as it has become clear that the value of bitcoins could be quite unstable and many countries are reluctant to accept them as a legal currency [15–17], IT researchers have redirected their attention to the other possible application fields for the technology, especially paying close attention to P2P services. They understood that it was possible to apply blockchain technology to these services because it can provide the same security and anonymity levels as in the bitcoin transactions when used as a service platform. The theoretical aspects of blockchain technology are quite novel and innovative in terms of security so that it is being considered that the data containing encrypted user information, transaction records, and the other information stored in blocks are nearly impregnable. It is expected that such a strong feature of blockchain will allow it to be applied to the other fields of business services where information security is vital to their success [18,19].

The browsers used in the Republic of Korea are IE and Chrome, followed by Firefox, Safari, and Opera but Chrominum also has some potential in this market due to its lightness and rapid processing capacity. Also, as an open-source browser, it can operate on the major operating systems (OS) such as Windows, Mac, Linux, or Android [20,21]. Currently, a fingerprint authentication system is being widely adopted by smart devices: Application Programming Interface (API) for Android Marshmellow, Touch ID (iOS), and the similar systems used by Chinese-made smartphones. IT researchers believe that such a phenomenon will continue even though security concerns over the increasing number of smart devices are yet to be solved [22–24]. Meanwhile, Satoshi Nakamoto (200) had proposed a solution [1] for the duplicate payment issue on P2P networks. The solution adopts a method of using a distributed network-oriented timestamp server which collects the block hash of each time-stamped items and publishes it in a form similar to a newspaper or a Usenet posting [25–29]. Based on the hash-based timestamp history in which there are all the timestamps of previous transactions, it is possible to prove that the data in question data was actually present in a specific time and, having done so, its blockchain will be extended or reinforced to provide better security.

2.1. Internet of Things (IoT) Sensors

A sensor is a device that detects information such as pressure, temperature, acceleration, and biological signals from an object to be measured and converts it into an electrical signal; it is a key element of IoT. Electronic devices acquire and analyze information through sensors, as humans perceive and understand the environment through their senses. Sensors are likened to human sensory functions [30–32]. In addition to simple sensing functions, a smart sensor retains data processing, decision making, communication functions, etc. They are intelligent sensors that can obtain the necessary information and make a decision and carry out information processing by itself.

With the introduction of Micro Electro Mechanical Systems (MEMS) technology, sensors are becoming more compact, developing from a single sensor module to a complex sensor module and to one-chip composite sensor and becoming more advanced and intelligent [33–35].

The sensor industry includes a materials industry for sensor manufacturing, a device industry that uses materials, and a module/system industry that assembles several devices. Sensors are intermediary products that acquire and sense information to provide a specific service instead of being used as a final product. The evolution of sensors is transforming the automotive and consumer electronics industries, and a "sensor revolution" called "sensorization" is underway. Sensorization plays a leading role in the data economy by connecting devices through sensors [36–39].

The sensor industry has been used in most industries in the stages of chips, packages, modules, and systems. Industrial use is expected to increase explosively with the spread of IoT. The sensor industry is a technology-intensive field. Due to the high technology barriers, entry into new markets is difficult; it is also hard to determine the policy direction due to the diversity of types and characteristics of each sensor. Given the diversity of device utilization, enabled technologies such as device development technology are very important, and it is necessary to have various experts in development for combining various technologies.

In addition, it is an important industry that is suitable for the cultivation of global specialist companies, and win-win cooperation with the demand enterprise—which is mainly a large enterprise—is important because the material technology, design technology, and process technology differ by application field. With the progress of information and communication technology (ICT) convergence, sensor becomes the core component of most devices, and securing the competitiveness of the sensor industry is an essential element in strengthening national industry competitiveness.

Smart sensors are actively being studied in the US, Germany, and Japan, which have the highest level of sensor technology. Since the manufacturing technologies of semiconductors and MEMS are integrated with them, advanced sensor development is actively underway. Korea's core sensor technology is at a very low level (55.8%) compared to that of advanced countries. In the case of smart sensors, domestic demand is mostly dependent on imports (about 80%) [40–42]. Large companies (telecom manufacturers, automotive companies, and telcoms) are responding to this quickly, but the movements of small and medium enterprises (SMEs) are still insufficient.

Sensors are applied to various fields such as measuring devices, automobiles, mobile devices, household appliances, medical devices, environmental devices, and industrial devices. The applications of the sensor will expand as it evolves into the IoT era wherein data is exchanged between all objects Figure 2.

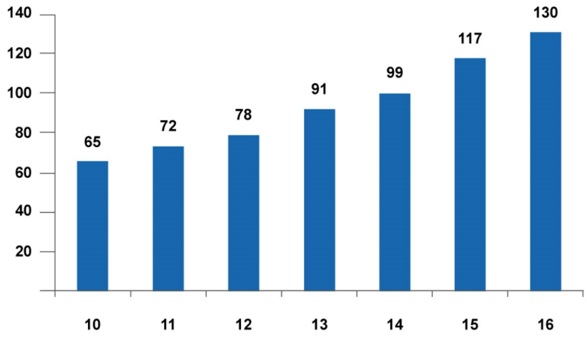


Figure 2. Diagram of smart grid.

The global sensor market is expected to grow at Compound Annual Growth Rate (CAGR) of 12% from KRW 65 trillion in 2010 to KRW 130 trillion in 2016 and to KRW 220 trillion by 2021.

The mobile sensor market is dominated mostly by image sensors, followed by pressure sensors and biosensors; 5~17 sensors applied to mobile smart devices (smart phones, tablet PCs, notebooks, etc.) are mainly used in the market for sensor type, pressure sensor, and biosensor (microphones, image sensors, touch sensors, Global Positioning System (GPS), motion sensors, geomagnetic sensors, illuminance sensors, proximity sensors, etc.). In addition, it is necessary to take the overall ecosystem approach considering the sensor industry and companies' competitiveness in a wide variety of fields and consumer convenience.

In addition, LTE Cat1, LTE Cat0, and NB-IoT sensors among IoT sensors were compared and analyzed Table 1. Distributed IoT data. In all the proposed IoT scenarios, data is distributed between devices often geographically dispersed. The computation and processing power is going on the network trunk but it is vulnerable to security. The work of these IoT sensors and multi-sensors is to enhance the strength of security through the Color Spectrum chain.

Table 1. Type of IoT sensor.

Type of IoT Sensor	LTE Cat1 (Rel.8)	LTE Cat0 (Rel.12)	NB-IoT (Rel.13)
Downlink peak rate	10 Mbps	1 Mbps	150 Kbps
Uplink peak rate	5 Mbps	1 Mbps	150 Kbps
UE receiver bandwidth	20 MHz	20 MHz	200 Khz
Duplex mode	Full Duplex	Half Duplex.	Half Duplex.

2.2. Blockchain

The blockchain technically enables the replacement of the current centralized ledger structure with the distributed ledger by using the public key algorithm, hash encryption technique, and low cost based on the distributed processing structure. The blockchain technology is the biggest threat to the payment relay system because Peer to Peer (P2P) financial transactions are possible between parties without the involvement of a third party (financial company or trusted third party) as long as Internet connection is available [43–45].

The blockchain is an enabling security technology that maintains the most commonly used and widespread "bitcoin [1]" virtual money. In bitcoin, the blockchain is a kind of distributed digital book that stores the history of the changed value of the bitcoin, a currency issued periodically. This book is made up of cryptographic techniques that cannot be falsified, and the digital book—wherein transactions of cryptography are recorded publicly for the transfer of ownership of the bitcoin—also starts from the first block (Genesis Block) [46,47]. The blockchain, which refers to all the transaction information of the chain including information on the previous block, is started from being distributed and stored across several nodes Figure 3 [8].

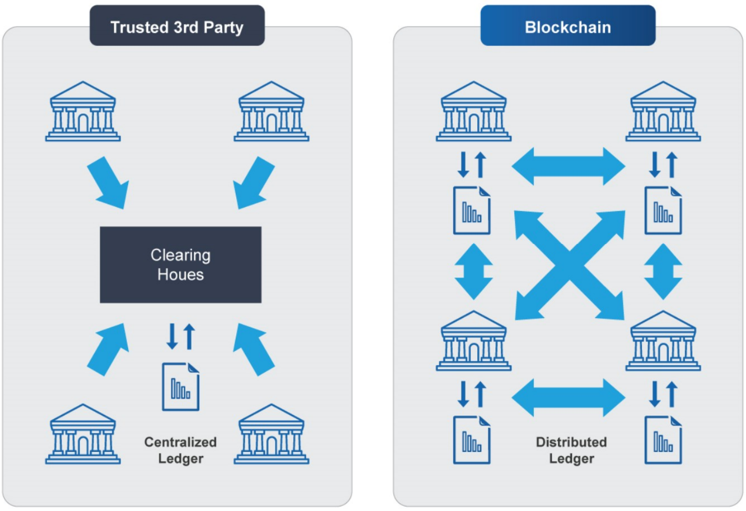


Figure 3. Diagram of blockchain.

There are three types of blockchains: public, private, and consortium Table 2. In the case of a public blockchain, verifying the transaction details of all participants can help with integrity, but privacy issues can arise. There is also information that must be hidden in case of the capital market, such as internal information or business secrets. Private blockchains are the type designed to meet realistic needs in actual operation while ensuring high privacy [48]. Finally, the consortium type is a semi-central-type blockchain consisting of consortiums of several organizations, and the pre-selected nodes are authorized so that each of the N agencies operates one node. The right to view the record of the blockchain is granted to all participants or only to the agency, to be disclosed only to specific persons through the API.

Table 2. Type of blockchain.

Type of Blockchain	Public Blockchain	Private Blockchain	Consotium Blockchain
Management subject	All participants	Managed by central institution	Participants in the consotium
Network participating condition transaction speed	Non Slow	Managed by central institution Quick	Non or Managed by selected institution Quick
Identification	Anonymous	Identifiable	Identifiable
Transaction proof	Proof of work algorithem, transaction verifier cannot be know in advance	Transaction verification is made by central institution.	Transation verifier is know through cetification transaction verification and block

In this paper, we also introduce blockchain technology for security performance from the blockchain viewpoint to overcome the sensor limitations of IoT devices and multi-platform security.

2.3. Blockchain of IoT Multiplatform Security

Protocols between different devices for inter-network interface require interoperability and compatibility technologies that are appropriate for the network environment. In the case of Wi-Fi, Bluetooth, and Zigbee devices, M2M protocol is applied to each of them, and they should work without any problem when connected through the IoT gateway. In particular, when different programs use different languages, an IoT ecosystem that is not actually smart can be created [37].

Among the elements constituting the IoT terminal, there are smart devices already connected to the Internet and devices newly connected to the Internet through BYOD (bring your own device). There is a robot cleaner that works with wireless CCTV in the home network; if hacked inside the related network, however, it can be used for privacy invasion and crime. Currently, Wi-Fi, Bluetooth, and Zigbee have their own communication and Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code (AES-CCM)-based security modules, but they are vulnerable to external attacks through network sniffing tools. Therefore, there is a need for low-power consumption encryption tools that can solve these problems, and the importance of Datagram Transport Layer Security (DTLS) and Internet Protocol Security (IPSec) is emerging. According to the Gartner report, the market for IoT security products is in a period of rapid growth as the market for general-purpose IoT becomes more widespread [49,50]. Gartner pointed out in the report that, while there are a number of reasons for the surge in demand for IoT security, one of the biggest factors is the perception that regulatory compliance will be a problem.

According to Gartner's IoT adoption survey, security is the biggest barrier to the success of the IoT initiative. The report pointed out that companies often do not have complete control over the devices and software used at each stage of the IoT project. This means that the organization must have higher level of visibility. Ruggero Contu, research director at Gartner, expects the demand for tools and services aimed at improving discovery and asset management, software and hardware security assessments, and intrusion testing to increase. He added that the organization also wants to improve its understanding of the impact of externalization of network connectivity. According to the report, about $900 million of next year's $1.5 billion budget for IoT security spending will be used for expert services rather than endpoint security or security gateway solutions [51–53]. This figure is expected to increase to $2 billion by 2021. Gartner sees the total IoT security spending in 2021 to reach $3 billion. Regulatory issues will not be the primary factor in spending on IoT security this year, but infrastructure protection and privacy-related compliance will become increasingly important from 2019 onward.

In addition, Wi-Fi, Bluetooth, and Zigbee have their own communication and AES-CCM are relatively weak compared to cable because they use wireless. WiFi does not require a complicated cable arrangement like a wire but it can be exposed to security threats because anyone can access it like a TV and radio system. Various encryption methods are provided in the router to make it difficult for others to decode the unprotected WiFi signal. However, because there are not many wireless security settings that can be applied all at once and users should should eventually choose one according to the Institute of Electrical and Electronics Engineers (IEEE) [54,55]. It is recommended to use the latest router or Wi-Fi-enabled devices for compatibility with older devices that are old enough to be encrypted. In order to increase the security of Wired Equivalent Privacy (WEP) a method of increasing the encryption key such as 64bit and 128bit is used. However since there is still security hole. It is better to use the encryption method that is more secure than WEP if security is important. Is still vulnerable using the TKIP algorithm so the way it came out is the AES algorithm mentioned above and the WAP2 encryption method that enhanced the existing Wi-Fi Protected Access (WPA) method. WAP2 abandons Temporal Key Integrity Protocol (TKIP) and uses AES-based Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP) as a basis. However, even wireless systems that support WPA2 support TKIP for compatibility. As mentioned above TKIP uses the AES-CCMP algorithm because it is a method that can be used for encryption in less than one minute. Since the AES-CCMP algorithm introduces a method of automatically changing the cryptographic key after transmitting a certain time or a certain amount of packets by using a cipher encryption algorithm with a variable key size there is no need to worry about information leakage through hacking do. Depending on the length and format of the password the time it takes to break a password with a Brute Force attack an eight-digit password created by combining uppercase and lowercase letters, numbers, and special characters may take up to 58 years to run 500,000 times per second it will be deciphered in days. In this paper a wireless sensor has security weakness compared to wired network. So we propose security through blockchain authentication.

3. Design and Implementation of IoT Sensor Platform of Blockchain

3.1. Issue Raising

Note however that 70% of the digital devices that can connect to the IoT network transmit the collected information unencrypted to the cloud computing system or the local network. In addition, 60% of IoT devices have been found to use a vulnerable web interface. Even when updating the software, 60% do not use encryption; thus, they are vulnerable in terms of encryption and user access. The IoT network security survey shows that two-thirds of the respondents are concerned about security.

Among the respondents, 70% said they were "very concerned" or "somewhat concerned" about sensitive personal information exposure, 17.2% were worried that IoT is so vulnerable to security to the point of being disastrous, and 48.8% were concerned about the same security issues as other applications and systems. In addition, the most IoT security-vulnerable device was reported to be the smart phone (41.3%), followed by tablet PC (10.7%), automobile (9.4%), home electronics/automation (8.8%), wearable device (8.3%), and medical device (7.2%).

3.2. Research Methodology

Since the keys generated by the software of existing IoT devices are mainly stored in the memory of the device, they are likely to be leaked by hacking. To eliminate the structural problems of the software-based security method, we propose a new chain concept based on blockchain among the hardware-based and software-based methods. We propose a color spectrum chain method using a blockchain used in the equity structure utilized in an existing blockchain.

Public certificates are written for Unix-based servers that include tools such as OpenSSL's SSLl-CA and SuSE Linux's gensslcert. In the intact online e-commerce, digital signatures are required for contract writing and identity verification with the other party. At the same time, the identity of the person who generated the digital signature is verified with the official certificate.

Public key infrastructure (PKI) presupposes the existence of a trusted third party (certification authority) responsible for securely distributing the private and public keys used to generate and verify digital signatures. Korea's public certificate system is also based on public key infrastructure. A certificate based on public key infrastructure can be divided into a server certificate used to verify the identity of the server and a personal certificate used to verify the identity of the user. Although the public certificate can be used for both purposes, when the public certificate of Korea is used as the server certificate, the Firefox web browser does not trust such server certificate. Therefore, using server certificates is not easy. We propose a color spectrum chain for various random authentications among Blockchain for security Figure 4.

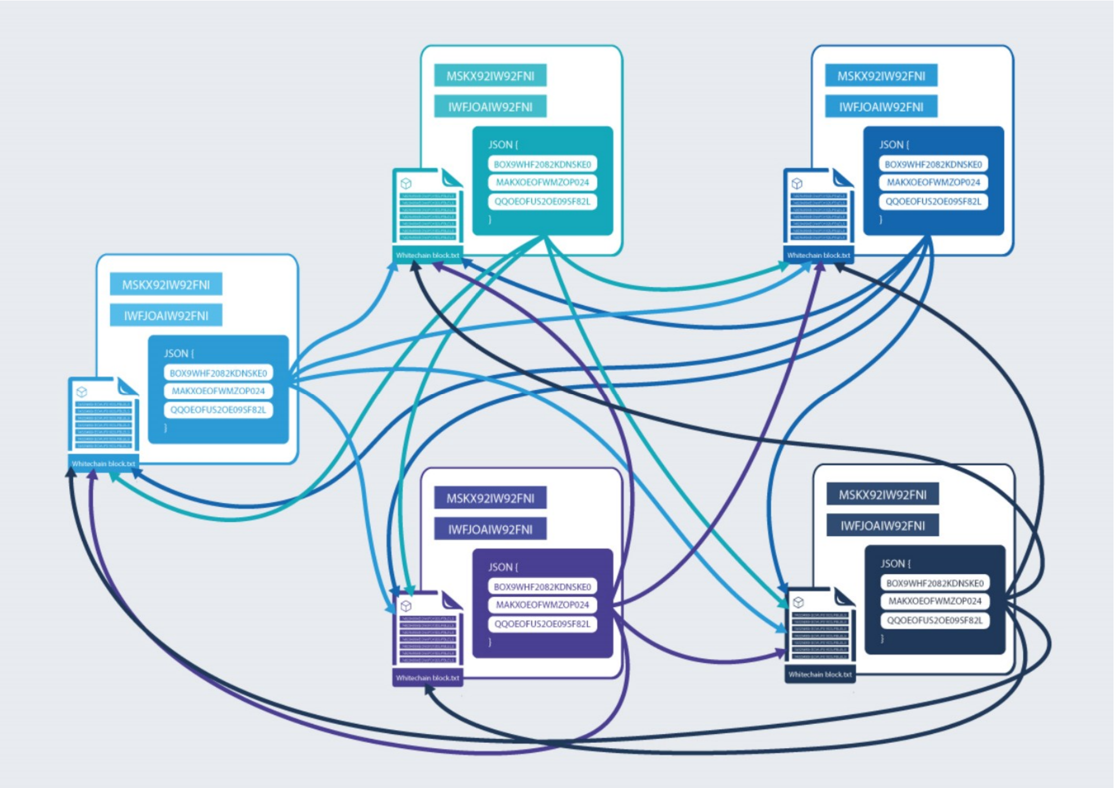


Figure 4. Color spectrum chain architecture.

The device authentication method of IoT using blockchain is called color spectrum chain. The method of applying the color spectrum chain to IoT is as follows: The blockchain used in the color spectrum chain stores the authentication status of the devices that can access IoT and operates on various servers of the IoT device. In the server, the color spectrum chain carries out the steps of confirming the information of the device, storing the authentication state of the identified device in the blockchain, and checking the authentication state of the stored device. The various devices connected to the server are registered in the blockchain through the color spectrum chain and communicated through the authentication step.

In the IoT environment, communication takes place between the server and the device. For secure communications, the server must verify that the device is a trusted device before communicating.

The device authentication process is performed by registering the device authentication status in the color spectrum chain as follows: as a device registration procedure of the color spectrum chain, a server and a device generate a public key and a private key—such as an elliptic curve digital signature algorithm (ECDSA)—through a color spectrum chain for blockchain transactions. The device then electronically signs the unique information and the public key and transmits them to the server, thereby requesting registration of the device to the color spectrum chain. The server compares the received information with the IoT authentication device information to confirm that the device is an authenticated device. Afterward, it stores the transfer of ownership to the device in the blockchain to the server-owned authentication token issued by the color spectrum chain. The stored blocks are synchronized between the color spectrum chain servers; in the synchronized server, the contents of the blocks are verified by the respective authentication device information and the block verification algorithm. If consensus is made in all servers, the devices in the relevant block are regarded as authenticated.

An IoT device communicates through the authentication token transferred from the server in the color spectrum chain. As a device authentication procedure of the color spectrum chain, the device transmits digitally signed authentication information to the server in order to communicate with the server. The server then confirms the authentication status in the color spectrum chain through the received information and verifies that it is an authentication device before performing the security procedure for secure communication.

In addition, the color spectrum chain has multiple authentications, these blocks are generated most quickly using the random function and also using the Smart Contract function. It is verified by using a hash protocol instead of using the existing key generation protocol.

3.3. Blockchain Methodology Architecture

Every security system can be a security problem if the private key is stolen. This key is stored in memory and can be hacked and stolen. However these public or private key-based systems have structural problems. In this paper we use a hash function without using a private key to eliminate the security problem. This is called color spectrum architecture. This color spectrum shows the architecture for structural security issues and the architecture uses a decentralized database of InterPlanetary File System (IPFS) types rather than a centralized it. Therefore an architecture structure that does not use a centralized service which is an existing Relational DataBase (RDB) can complement the structural problem of performance. If you are hacked by a primary attack on your server you have double-core dApp authentication and source level authentication like JASON. This part has multi-Factor authentication. Such a structure has a structure using a protocol on Https. This Https protocol has the structure of any device, any OS, any platform. This structure is called a color spectrum chain architecture.

3.4. Verification Method Using Color Spectrum Chain

3.4.1. Server-Based Color Spectrum Chain Certificate Verification Protocol

For digitally signed electronic documents, the validity of the certificate is verified through the self-validation of the certificate, certificate path validation, and policy validation and by checking the status of the certificate. As protocols between a client and a server, delegated path discovery (DPD) and delegated path validation (DPV) protocols are characterized by the server performing discovery and verification for an authentication path on behalf of a client. These protocols are important protocols that can be applied to environments where certificate validation paths must be included in electronic documents to verify the authenticity of electronic documents.

In other words, the authentication path processing task of the certificate necessitates various verification processes such as the validation of signatures, checking of certificate revocation status, and validity of certificate validity for each of the certificates on the path. Therefore, storing data with documents has given rise to considerable technical difficulties. Various methods have been suggested to solve these problems, the most effective of which is the method of delegating all tasks related to the authentication path to the online server. Server-based certificate validity protocol (SCVP), which satisfies the DPD and DPV requirements, discovers the authentication path and verifies the status of the certificate online on behalf of the client as well as the protocol between client and server.

As shown in Figure 1, the SCVP can delegate all or part of the certificate verification process included in the electronic document to the server. Even if the verification information such as the certificate revocation lists (CRL) is not stored in the electronic document, services such as certificate path creation, certification path verification, and certificate status checking are provided.

3.4.2. Color Spectrum Chain of Online Certificate Status Protocol

Generally, a method of verifying the delegation certificate of the SCVP method using the CRL and a method using the online certificate status protocol (OCSP) are available.

For OCSP, when the user queries the OCSP server about the status of a specific certificate, the OCSP server notifies the user only whether the OCSP server has canceled the certificate so that the user need not download the list of all canceled certificates.

In addition, it can be used efficiently by performing real-time verification of certificate status between client and server. The request message and response message of OCSP and the extended area used at this time are as follows: The OCSP request message consists of protocol version, service request, and target certificate ID as well as optional extensions processed by the OCSP responder. The OCSP response message consists of the version of the response format, the name of the responder, the response to each certificate contained in the request, the optional extension, the signature algorithm OID (object identifier), and the signature value for the compressed response message. The response to each certificate included in the request consists of the ID of the certificate for which the current status is to be known, the certificate status value, the response validity interval, and the optional extensions. Here, the certificate status value is expressed as GOOD, REVOKED, or UNKNOWN. The extensions of OCSP are additionally included in the request and response messages and processed by the OCSP responder as follows:

Nonce: Prevents the replay attack when exchanging request message and response message.

CRL reference: indicates information about the CRL referenced by the OCSP responder.

Acceptable Response Types: the response message types that OCSP clients understand are classified as OID and are included in the request message.

Archive Cutoff: value minus the time of OCSP responder storing the revocation information after certificate revocation from the time of issuing the OCSP response message.

CRL Entry Extensions: the one referred to in Request For Comments (RFC) 2459 is used.

Service Locator: used when a particular server receives a request message, which is subsequently forwarded to a trusted OCSP server with a validated certificate.

This is standardized in IETF RFC 2560, and we used “Archive Cutoff” in the OCSP extension for the long-term verification of expired certificates.

3.4.3. Efficient Long-Term Verification of Electronic Documents Color Spectrum Chain

The long-term verification of a digitally signed electronic document requires the verification of own certificate, certificate path validation and policy verification, and verification of the status of the certificate to validate; therefore, if the certificate does not have the relevant information in the electronic document or has only the certificate status information, judging whether the certificate is a valid certificate cannot guarantee the integrity and authenticity of the corresponding electronic document.

As such, we verify the certificate against the digital signature of the electronic document stored in the SCVP client using the SCVP server standardized in RFC 5055.

Here, the client is assumed to store an electronic document containing a complete certificate as well as related information digitally signed through a public certificate issued by a public certification authority.

The SCVP server and the SCVP client communicate with each other through the SCVP Tool Kit (API, application program interface). The SCVP server and the certificate authority (CA) can communicate with each other through the existing PKI tool kit.

It is the basic process structure of the certificate status checking API of electronic documents between the SCVP client and SCVP server certification authority.

(1) SCVP Request: the client who wants to verify the electronic document selects the appropriate certificate verification method (CRL or OCSP) and sends a certificate validation request message to the SCVP server.
(2) CRL Request/OCSP Request (OCSP Request): the SCVP server requests the certification authority (HTTP, LDAP, OCSP, etc.) to verify the certificate based on the certificate verification request from the client.
(3) CRL Acquisition/OCSP Response (OCSP Response): the SCVP server acquires the response message of the verification request received from the certification authority.
(4) SCVP Response (certificate verification process response): the verification result is sent to the client based on the response message of the verification request.
(5) Certificate Verification Completed: the client completes the verification of the target certificate based on the result of the SCVP Response.

For the long-term verification of digitally signed electronic documents, the client requests certificate verification to the SCVP server. At this time, the client selects a certificate revocation list (CRL) or an OCSP method to verify the electronic document possessed by the client and transmits a certificate verification request message. The CRL request message is used for verifying whether or not the certificate is discarded to a specific certification authority, including certificate path verification and policy verification.

At this time, the SCVP server and the specific CA can communicate with each other via hypertext transfer protocol (HTTP), lightweight directory access protocol (LDAP), and the like. Upon receiving the certificate verification processing request message from the client, the SCVP server transmits a CRL request message to the certification authority based on the certificate verification request message.

The SCVP server receives from the CA a response message to the certificate verification request. At this time, the response message can be processed on the precondition that the certification authority verifies the certificate based on the CRL.

Then, the SCVP server sends an OCSP request message to the certification authority based on the certificate verification request message. The OCSP request message is for requesting a specific certification authority to check the real-time status of the corresponding certificate.

At this time, the specific certification authority may be the same or a different certification authority to which the CRL request message is transmitted. When the certificate verification request is made, the certification authority performs verification of the corresponding certificate based on the OCSP and transmits the verification result (GOOD, REVOKED, UNKNOWN) to the SCVP server. Certificate verification is performed using only the current certificate.

Therefore, in this case, the verification is stopped for the certificate whose validity period has expired, and only the verification result "REVOKED" is transmitted to the SCVP server; hence the impossibility of long-term verification of the digital signature.

In order to solve this problem and proceed with the long-term verification without stopping the verification even when the validity period of the certificate expires, an extended field is added to the OSCP response message to inform the certificate revocation time information. In other words, the OSCP response message is implemented using the archive cutoff, which is an extension of the OCSP standard.

"Archive Cutoff" is the time minus that when the OCSP respondent retained the revocation information after revoking the certificate from the time the OCSP response message was issued. This is used to verify the authenticity of the signature value generated on the cutoff date, even if the certificate was revoked a long time ago, to verify the signature value.

For example, if the data of "Archive cutoff = 2003.1.1" is recorded in the response message of the verification result, this OCSP means that it has the revocation information of the certificates after 2003. 1.1.

Therefore, when the SCVP server receives the OSCP response message, it verifies the verification result in the response message; if it is "REVOKED," it searches the extended field and checks the revocation time field of the revoked information. If the certificate is revoked before the digital signature is made, the digital signature is invalidated. If the certificate is revoked after the digital signature is made, the digital signature is valid.

Finally, the SCVP server sends to the client a certificate verification processing response based on the OSCP response message. The client completes the certificate verification based on the certificate verification processing response message received from the SCVP server.

In other words, the client can obtain the validation information with regard to the validity of the digital signature certificate according to the contents of the certificate verification processing response message and check the validity and authenticity of the digital signature document stored by the client according to the obtained verification information.

Therefore, even when the validity period of the certificate expires, it is possible to carry out long-term verification without interrupting the verification and to verify the certificate since the revocation information of the expired certificate is maintained.

3.4.4. Identity-Based Cryptographic Verification Color Spectrum Chain

This is a new public key authentication scheme proposed by Adi Shamir in 1984. The cryptosystem uses the user's identity information as the public key of the user and replaces the complex key value of the existing public key scheme. The TTP (trust third party) generates the private key using the user's identity information and transmits it securely to the user. TTP should be absolutely trusted. The process of deriving the private key from the user's identity information should be performed entirely by the TTP. If there is a dispute between users, the trust authority acts as a mediator of the dispute as the authority that generated each user's private key. In Adi Shamir 's proposal, the digital signing scheme was suggested, but not the password transfer algorithm based on identity information; only a concept was presented.

Also the secret-key is being developed as DES, 3DES, AES and etc have a secret key. Moreover, the secret-key cryptographic algorithm is an algorithm that allows a person who knows the key to view the encrypted document without revealing the key used for encryption to the general public. The secret-key encryption algorithm has the same encryption key and decryption key. With this property the secret-key encryption algorithm is also called a symmetric-key encryption algorithm. Therefore in order to use the secret-key encryption algorithm in the communication both parties to communicate must share the encryption key in advance. In order to generate a key there are methods of generating a key using a random number generator included in a computer or other device and a method of directly generating a key by a user. A key generated by using a random number generator is strong in an attack method in which a key is predicted and substituted like a dictionary attack but the user has difficulty in memorizing a key. On the other hand the user-generated method is easy for the user to remember the key but vulnerable to the key predictive attack method. Among the conflicting concepts there is a public-key infrastructure algorithm. Basically, it is a type of cipher that allows users who do not share the secret key in advance to communicate securely. In the public key cryptosystem. There exists a public-key and a secret key. Anyone can know the public-key but the corresponding secret-key must be known only to the owner of the key. The algorithm for constructing the public-key cryptosystem is called asymmetric cryptosystem in comparison with the symmetric key cryptosystem, Rivest Shamir Adleman (RSA), Data Acquisition System (DAS), Diffie–Hellman and others.

(1) Pairing-Based Identity-Based Cryptosystem

In 2001 Dan Boneh and Matt Franklin presented a practical implementation by proposing an identity-based cryptosystem according to Weil Pairing based on elliptic curves. Identity-based cryptography was implemented by applying a mathematical structure called a bilinear map.

$$Pair\ (a{\cdot}X, b{\cdot}Y) = Pair\ (b{\cdot}X, a{\cdot}Y)$$

The operator used in the expression above represents the product of the points on the elliptic curve. The multiplication itself is easy, but it is impossible to know X and a $\cdot$ X and find a. The key server generates s and P from the random numbers and notifies all users of the P and s $\cdot$ PP values. Next, s $\cdot$ ID as the private key of user x is computed and transmitted to the user. The ciphertext procedure using these values is shown in Figure 5.

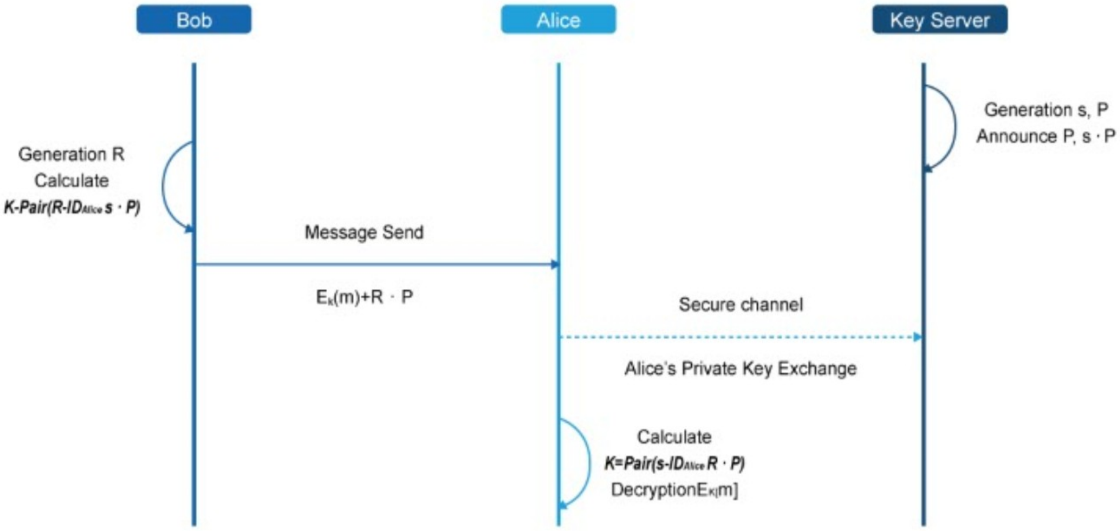


Figure 5. Pairing-based identity encryption.

Sender Bob sets a random number and computes the following symmetric key:

$$k = (r{\cdot}ID_{Alice}, s{\cdot}P)$$

Here, $s \cdot P$ is a value notified by the key server, and $r \cdot ID$ is a value calculated by using all open values. It is encrypted with the generated key k for the next message m. It sends the ciphertext E [m] and $r \cdot P$ to Receiver Alice, who calculates the decryption key for protection as follows:

$$k = Pair(s{\cdot}ID_{Alice}, r{\cdot}P)$$

The generated decryption key is Alice's private key distributed to Alice—called $s \cdot ID$—and $r\ P$ is the value that Bob sends to Alice. The private key value is known only to Alice; and decryption of ciphertext is possible only by Alice. And finally we do not use K-defined equations

(2) Session Key Generation Protocol

In the IoT network, a session key must be generated between the access server and the core server for mutual authentication. For the session key, we propose a session key generation protocol based on ID-based encryption. This protocol is used in session key generation protocol, device registration and authentication protocol, and proposal system.

3.4.5. Color Spectrum Chain Security Performance Verification Method

A color spectrum chain means that the structure of a block is not defined. This also means that the attributes making up the block are not structured. Since existing blockchains are structured with continuous bits, there are limitations in applying them to digital coins suitable for various services.

The elements constituting the informal chain have hash points considering extended chains in order not to use the fork method. Hash point is a structure for linking other chains considering the fact that the existing chain structure should be expanded. If the existing blockchain exchanges blocks through fork with a P2P–P2P independent chain structure, the unstable network suspension behavior through these forks will not create a full agreement between Peer and Peer. Therefore, we have devised a way of maintaining the connection link using the extension.

In addition to adding fields and adding and modifying tables in existing databases, extension can be done using hash pointers to elements of the formatting block, just like adding a field to refer to the table's index.

These extensions can create processes for the interworking of various services and become flexible because the nodes in the central network can apply spontaneous extensions.

If the length of the existing block is set to the standardized size, the informal chain allows the length of the block to be varied.

Since the length of the variable block can go to an infinite increase of the block, the concept of time to limit it is applied to induce the limit block increase; thus preventing the overflow of the transaction.

Competing for compensation aids in rational decision making, and rational opinions are classified as either formal or interdependent. The transaction recorded in the block is held for each node. The problem is that the risk must be distributed in such a way that all the nodes that are in each case are synchronously involved, and the risk must be modified in various ways. All that is needed is a book on individual transactions. It is important that the books for individual transactions be rebased. This should rebase the transaction of the node wherein the proof of the block is confirmed.

All the resource holding behaviors of the participating nodes want compensation. It is necessary to publicize what is most suitable for compensation during the resource holding act and share it reasonably.

In order not to undermine such reasonable sharing, it is necessary to determine a reasonable price for compensation that has a positive formation.

Note, however, that such reasonable price decision should make the mode node fall into the prisoner's dilemma. This is to avoid making the most dangerous decisions for the prisoner's dilemma and to reduce these risk factors so that decisions are best served. A game is required to induce competitive participation. This color spectrum chain plays a role in extracting information about the process of the transaction. The path of information is not the right to have a particular place, but the subject who created it has rights. If the entity that generated the information is recorded on a particular platform with the value of this information, and it wants to be compensated through the value of the record, the attribute of the value can be said to have been transferred. The challenge lies in proving that the transfer of these values is their own initiative value.

Comparing whether values' interpretations have responses can also be a Byzantine factor. The interpretation of value differs in magnitude of extensibility when different purposes are applied differently. The problem is that Nash believes this to be contrary to his theory because it means that it has a variant variable.

Even if a key session key used only once for each communication is known, it is defined that only one communication is decrypted and another session key is used in the next communication. The process is defined in the SSL connection process. In the SSL server authentication step the web browser authenticates the other web server. This step is a function to authenticate whether or not the client has been issued from the trusted CA and the SSL client authentification step is the step of authenticating the client that the Web server has requested. In this step the SSL-enabled software or SSL heardwares placed in front of the server examine whether the certificate of the client and the public

ID actually received a certificate that the server trusts. It then goes through the encrypt connection step Figure 6.

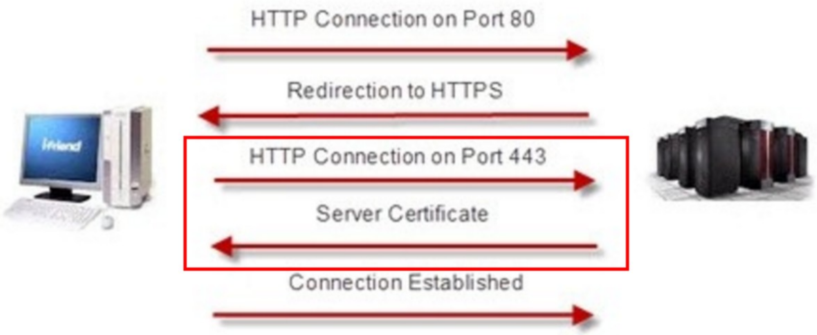


Figure 6. Receved by HTTP protocol.

(1) Color Spectrum Chain Architecture Design

Typical storage system Figure 7.

—Uses a proprietary PCIe optical interface card.

—Eliminates the extra memory buffering behavior for interfaces to the storage media termination.

—Uses multi-channel PCIe optical interface card to improve Input/Output Operations Per Second (IOPS) performance (SPC1).

—Has improved throughput performance (SPC2) (single bus interface from PCIe to the storage media termination).

—Has high performance with "All-Flow PCIe".

Super-IO storage system Figure 8.

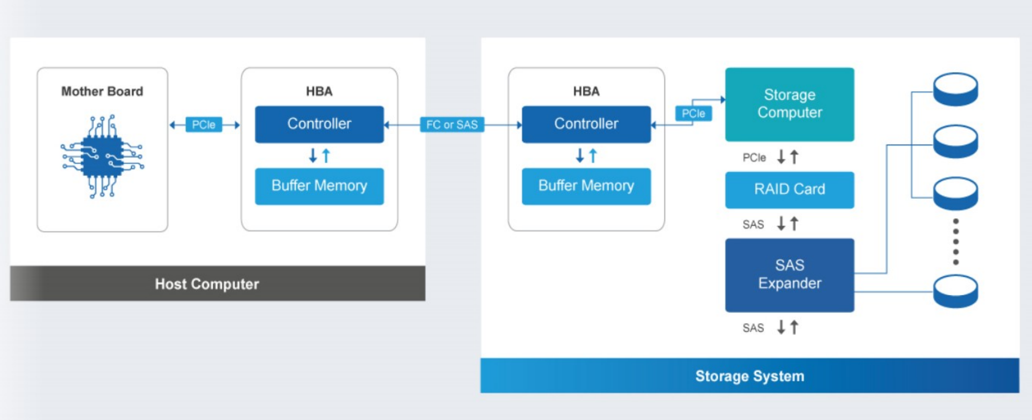


Figure 7. Typical storage systems architecture.

—Uses HBA card that requires memory buffering such as Fiber Channel and Infiniband—Performance degradation.

—Uses multi-channel HBA card to improve IOPS performance (SPC1).

—Has throughput performance (SPC2) improvement constraint (heterogeneous bus Host Bus Adapter (HBA) card).

—Has high performance with "All-Flash Storage".

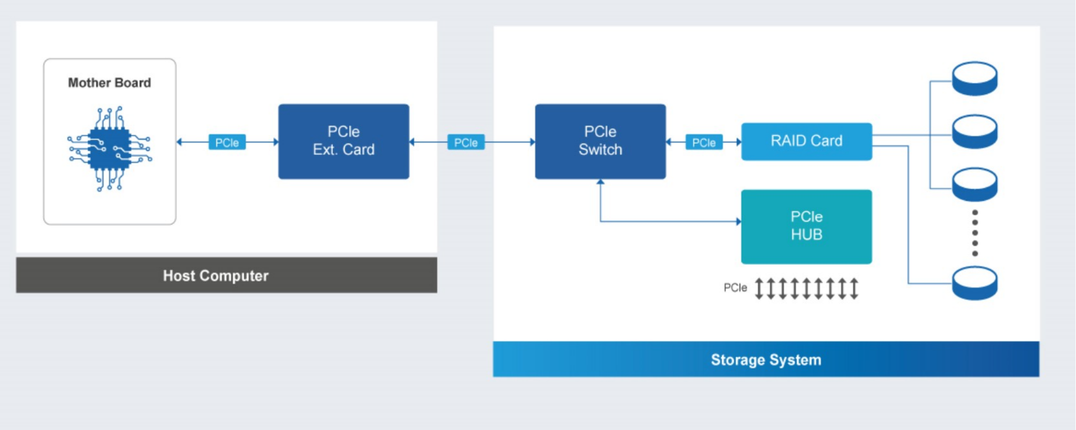


Figure 8. Super-IO storage systems architecture.

The fact that Alice sends $ 100 to Bob is recorded in the blockchain. To prove that this transaction is true, Alice's purse must be verified through the entire node of the blockchain. Whether Bob's wallet is correct is checked as well through the entire node of the blockchain. It also records the hash value S9H8FDFJH89FSFDSAFKLJFLDSJALKJDF for the transaction information as No. 2 (assumed) block-chaining transaction and randomly selects a server to participate in to prove to all nodes that the transaction recorded in No. 2 is a normal transaction.

If the total blockchain has three nodes (A, B, and C), the transaction recorded in blockchain 2 of A will participate in the verification of B and C nodes, which compete for verification. This competition generates compensation. The competition chain is the color spectrum chain. The block proven through the competition provides compensation to the node that proves the transaction size according to the proportion. To prove the transaction, all nodes have a public key. This public key is used to verify that the transaction is complete. The nonce of the block is performed according to the degree of difficulty, so the operation leading to 0 must be carried out through the public key.

The color spectrum chain uses multiple nodes, excluding its own node, to prove that it is the blockchain. This node does not have verification authority. Randomly select the nodes to participate in the verification, and then request verification. The hash of the color spectrum chain is rebased to all nodes to have a hash of the verified transaction block.

The blockchain is also established through the proof of the color spectrum chain. This establishment is confirmed through the creation of a whitechain.

The block has hash as well as the previous block's difficulty of containing fast transactions and for competition and trade compensation. Through such difficulty, the proving of the block is verified through the occurrence of "0"; thus, the reliability can be improved Figure 9.

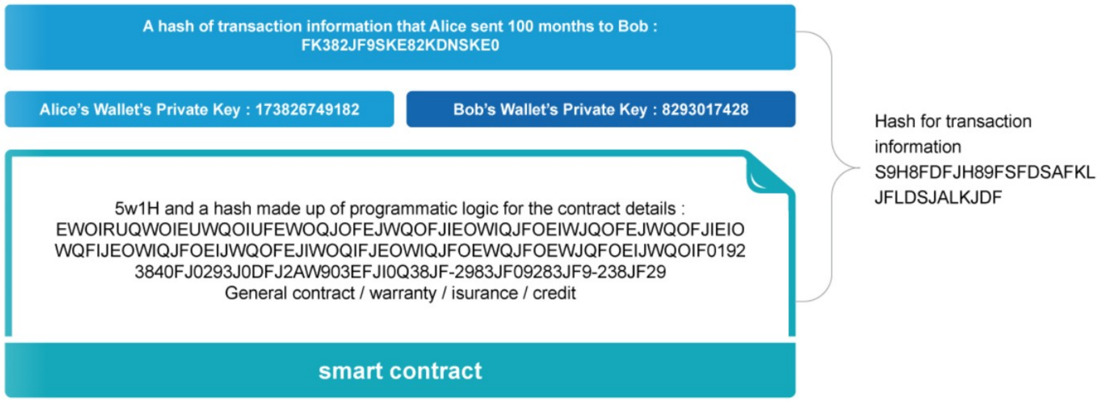

A hash of transaction information that Alice sent 100 months to Bob :
FK382JF9SKE82KDNSKE0
Alice's Wallet's Private Key : 173826749182
Bob's Wallet's Private Key : 8293017428
5w1H and a hash made up of programmatic logic for the contract details :
EWOIRUQWOIEUWQOIUFEWOQJOFEJWQOFJIEOWIQJFOEIWJQOFEJWQOFJIEIO
WQFIJEOWIQJFOEIJWQOFEJIWOQIFJEOWIQJFOEWQJFOEWJQFOEIJWQOIF0192
3840FJ0293J0DFJ2AW903EFJI0Q38JF-2983JF09283JF9-238JF29
General contract / warranty / isurance / credit
smart contract
Hash for transaction
information
S9H8FDFJH89FSFDSAFKL
JFLDSJALKJDF

Figure 9. Color spectrum chain hash architecture.

To capture transactions (confidentiality, availability, functionality, and interoperability aspects) quickly and to prove that the transaction is trustworthy (integrity, non-repudiation), the block provides random rights to other nodes that participate without using the node containing the transaction. By doing so, a consensus structure is created for the nodes participating according to how many "0 s" have occurred for a certain time Figure 10.

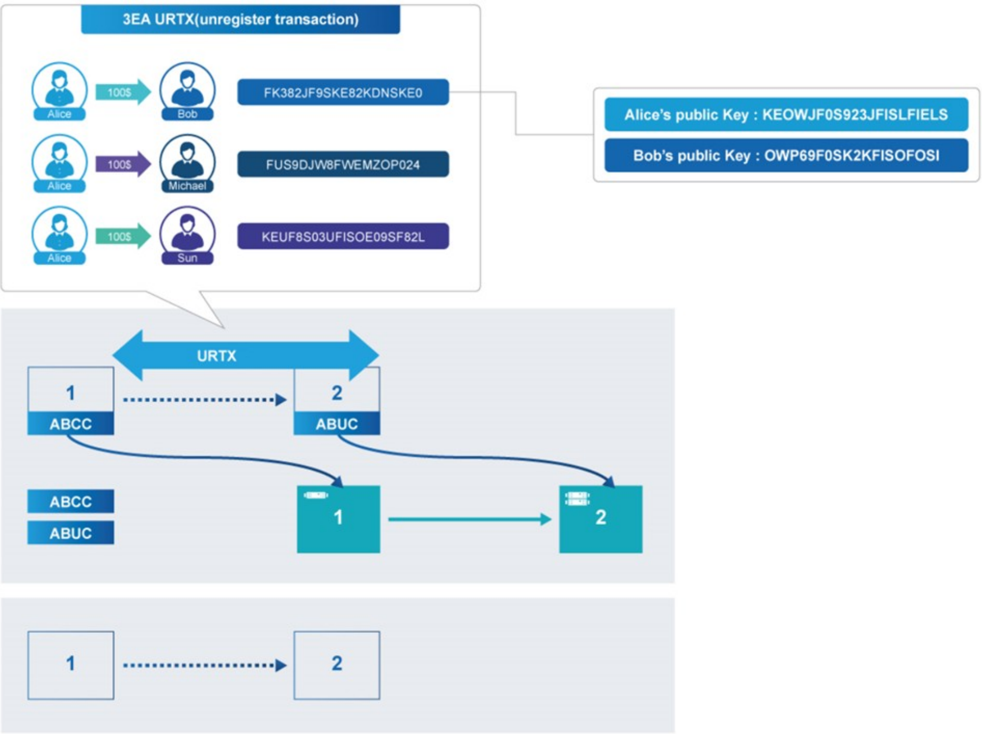


Figure 10. Color spectrum chain hash throw architecture.

In addition the blockchain technology has advantages of reducing transaction costs and preventing forgery of data and it can be combined with various industries to increase efficiency and create new economic value. In addition it is possible to support real-time autonomous collaboration between Internet devices without human intervention based on a smart contract through autonomous collaboration between IoT devices. Moreover, blockchain technology to enable comparative analysis between blockchain technologies. We propose an evaluation system that can objectively verify the reliability and performance of platform service (distributed app).

(2) Color Spectrum Chain Performance comparison with Existing Blockchain

In the Color spectrum chain each block is stored as a timestamp and an optional index. It also has a self-identifying hash to each block to ensure integrity throughout the blockchain.

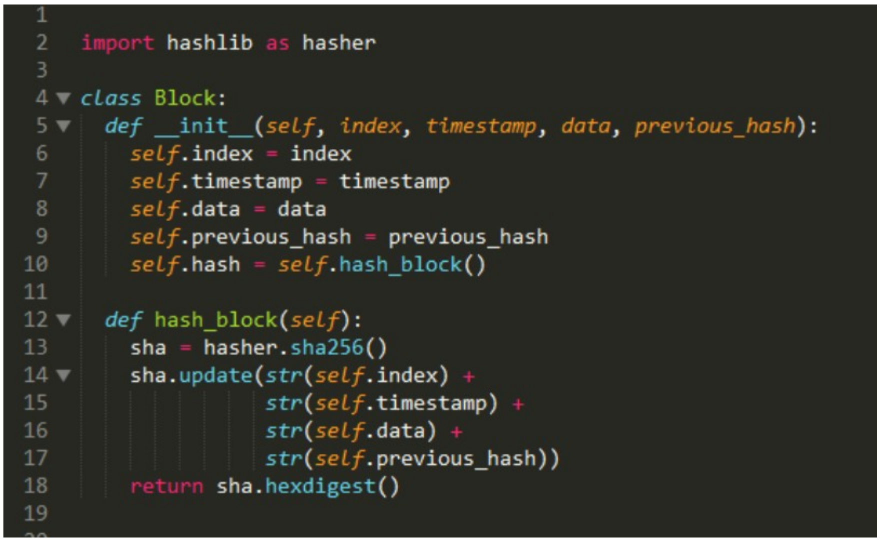
As with the bitcoin, the hash of each block is a hash that encrypts the index of the block, the timestamp, the data, and the hash of the previous block Figure 11.

Once the block structure is created as in the code, the next step is actually adding the block to the chain. As mentioned earlier, each block needs information on the previous block.

The first block, the genesis block, is a special block unlike ordinary blocks. Usually, it needs to be added manually or by using a unique logic.

The index of this block is 0, returning an arbitrary data value and an arbitrary value for the "previous hash" parameter Figure 11.

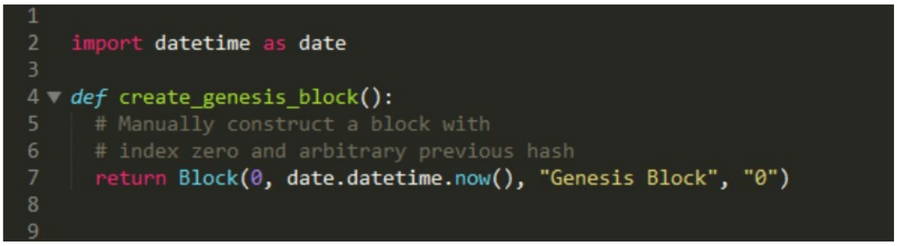
This function creates data of the block to be newly created by using the previous block as a parameter in the color spectrum chain structure, and returns a new block with the corresponding data Figure 12.



```
import hashlib as hasher

class Block:
    def __init__(self, index, timestamp, data, previous_hash):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.hash = self.hash_block()

    def hash_block(self):
        sha = hasher.sha256()
        sha.update(str(self.index) +
                   str(self.timestamp) +
                   str(self.data) +
                   str(self.previous_hash))
        return sha.hexdigest()

```

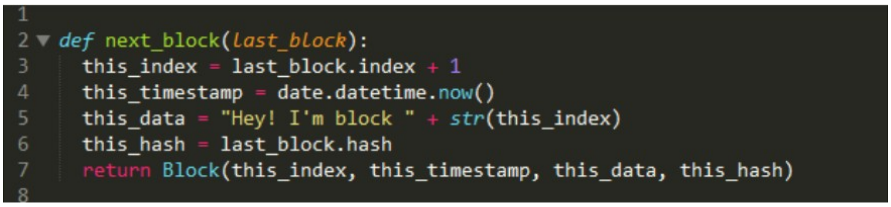
Figure 11. Color spectrum chain code generation.

When a new block hashes the information of the previous block, the integrity of the Blockchain increases each time a new block is created. By using this structure, we will be able to defend our blockchain in the replacement (collapse) of the chain structure due to the "modification of the past information" which may originate from an external intruder such as a hacker. Therefore, this color spectrum chain acts as proof of encryption and can not be replaced or removed once the block is added to the blockchain Figure 13.



```
import datetime as date

def create_genesis_block():
    # Manually construct a block with
    # index zero and arbitrary previous hash
    return Block(0, date.datetime.now(), "Genesis Block", "0")

```

Figure 12. Color spectrum chain replacement code.



```
def next_block(last_block):
    this_index = last_block.index + 1
    this_timestamp = date.datetime.now()
    this_data = "Hey! I'm block " + str(this_index)
    this_hash = last_block.hash
    return Block(this_index, this_timestamp, this_data, this_hash)
```

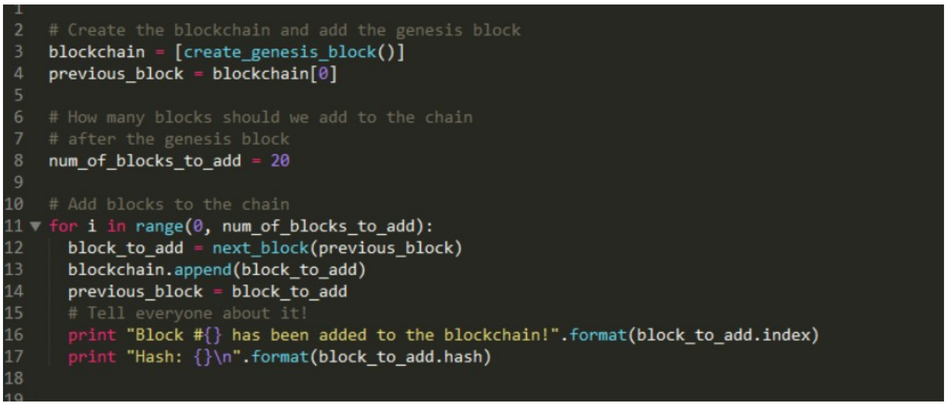
Figure 13. Color spectrum chain block.

This function creates the data of the new block to be created by using the previous block as a parameter in the color spectrum chain structure and returns a new block with the corresponding data Figure 12.

When a new block hashes the information of the previous block, the integrity of the blockchain increases each time a new block is created. By using this structure, we will be able to defend our blockchain in the replacement (collapse) of the chain structure caused by the "modification of past information," possibly by an intruder such as a hacker. Therefore, this color spectrum chain acts as proof of encryption; it cannot be replaced or removed once the block is added to the blockchain Figure 13.

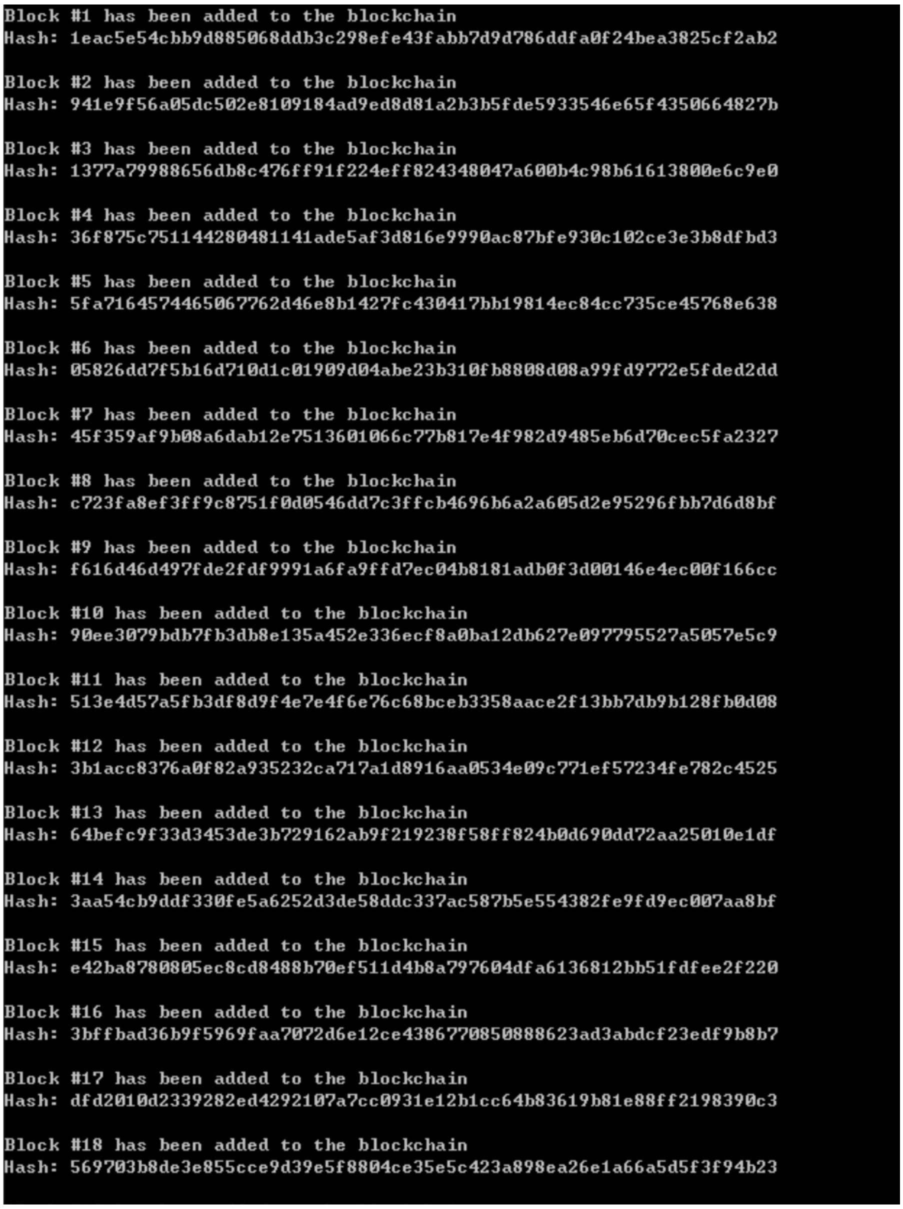
By complete the code above, a blockchain can be built. The color spectrum chain itself is a simple Python list whose first element is the origin block. Naturally, the next block needs to be added.

Because it is a color spectrum chain Figure 14, add 20 new blocks Figure 15.



```

# Create the blockchain and add the genesis block
blockchain = [create_genesis_block()]
previous_block = blockchain[0]

# How many blocks should we add to the chain
# after the genesis block
num_of_blocks_to_add = 20

# Add blocks to the chain
for i in range(0, num_of_blocks_to_add):
  block_to_add = next_block(previous_block)
  blockchain.append(block_to_add)
  previous_block = block_to_add
  # Tell everyone about it!
  print "Block #{} has been added to the blockchain!".format(block_to_add.index)
  print "Hash: {}\n".format(block_to_add.hash)

```

Figure 14. Color spectrum chain block replace.



```
Block #1 has been added to the blockchain
Hash: 1eac5e54cbb9d885068ddb3c298efe43fabb7d9d786ddfa0f24bea3825cf2ab2

Block #2 has been added to the blockchain
Hash: 941e9f56a05dc502e8109184ad9ed8d81a2b3b5fde5933546e65f4350664827b

Block #3 has been added to the blockchain
Hash: 1377a79988656db8c476ff91f224eff824348047a600b4c98b61613800e6c9e0

Block #4 has been added to the blockchain
Hash: 36f875c751144280481141ade5af3d816e9990ac87bfe930c102ce3e3b8dfbd3

Block #5 has been added to the blockchain
Hash: 5fa716457446506776 2d46e8b1427fc430417bb19814ec84cc735ce45768e638

Block #6 has been added to the blockchain
Hash: 05826dd7f5b16d710d1c01909d04abe23b310fb8808d08a99fd9772e5fded2dd

Block #7 has been added to the blockchain
Hash: 45f359af9b08a6dab12e7513601066c77b817e4f982d9485eb6d70cec5fa2327

Block #8 has been added to the blockchain
Hash: c723fa8ef3ff9c8751f0d0546dd7c3ffcb4696b6a2a605d2e95296fbb7d6d8bf

Block #9 has been added to the blockchain
Hash: f616d46d497fde2fdf9991a6fa9ffd7ec04b8181adb0f3d00146e4ec00f166cc

Block #10 has been added to the blockchain
Hash: 90ee3079bdb7fb3db8e135a452e336ecf8a0ba12db627e097795527a5057e5c9

Block #11 has been added to the blockchain
Hash: 513e4d57a5fb3df8d9f4e7e4f6e76c68bceb3358aace2f13bb7db9b128fb0d08

Block #12 has been added to the blockchain
Hash: 3b1acc8376a0f82a935232ca717a1d8916aa0534e09c771ef57234fe782c4525

Block #13 has been added to the blockchain
Hash: 64befc9f33d3453de3b729162ab9f219238f58ff824b0d690dd72aa25010e1df

Block #14 has been added to the blockchain
Hash: 3aa54cb9ddf330fe5a6252d3de58ddc337ac587b5e554382fe9fd9ec007aa8bf

Block #15 has been added to the blockchain
Hash: e42ba8780805ec8cd8488b70ef511d4b8a797604dfa6136812bb51fdfee2f220

Block #16 has been added to the blockchain
Hash: 3bffbad36b9f5969faa7072d6e12ce43867708508886 23ad3abdcf23edf9b8b7

Block #17 has been added to the blockchain
Hash: dfd2010d2339282ed4292107a7cc0931e12b1cc64b83619b81e88ff2198390c3

Block #18 has been added to the blockchain
Hash: 569703b8de3e855cce9d39e5f8804ce35e5c423a898ea26e1a66a5d5f3f94b23
```

Figure 15. Color spectrum chain result.

As shown in the Figure 15, a hash block can be divided into 1 to 18 blocks to obtain a unique hash value. Hashes are also widely used in the security field. Because there is no direct relationship between the key and the hash value, it is difficult to restore the key with the hash value alone. In addition, the hash function can generate a constant length output for input data having different lengths, and can also perform a "data reduction" function. However, almost all hash functions developed so far have been confirmed to cause hash collisions. Of course, it would also make sense to reduce the hash collision itself, but the important thing is that hash collisions occur evenly across the hash value. In the above diagram, if the unique values of all the hashes are mapped to the same hash value, the inefficiency is increased when accessing the data, the security is weak (the same hash value even though the key is different) There is no reason to manage it. So from 1 to 18 hash values are put in different blocks to show the value that enhances security function.

The results verified using the colored spectrum chain are compared and verified with the existing data. The figure shows the blockchain performance data using the existing blockchain Figure 16.

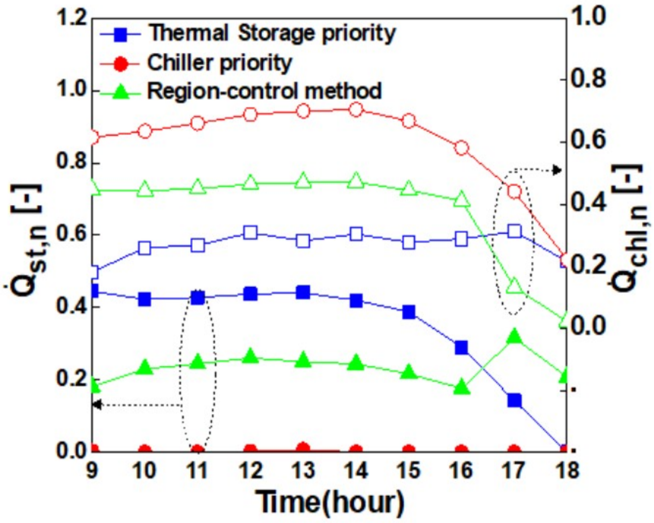


Figure 16. Basic blockchain data.

The color spectrum chain is used to compare and verify Thermal priority and Chiller priority Figure 17.

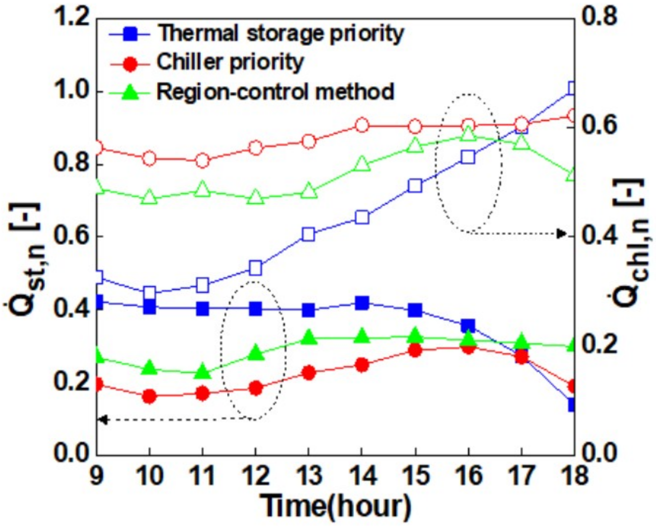


Figure 17. Color spectrum chain results.

Figure 16 above compares the existing block-chain platform with the IOTA's "Tangle" platform, which uses block chains of existing IOT data. IOTA discusses innovative approaches. This approach is applied to a virtual currency called iota, which is specially designed for the current IoT industry. In this paper, we compare the general characteristics of Tangles, discuss the problems that arise when removing blockchains and maintaining distributed trading books, and comparing them with color spectrum chains. The specific implementation method of the Iota protocol is compared. In general, Tugle-based virtual currency works as follows. Instead of a global block chain, there is a directed acyclic graph (DAG) called a tang. The transactions requested by the nodes constitute a set of sites in the Tangle graph, which is a transaction book that stores transactions. The edge set of the tangles is obtained by the following method. When a new transaction arrives, it must approve two previous transactions 2. These approvals are expressed as directed edges. If there is no directional line between the transaction and the transaction, but there is a directed path from a minimum of two to a long, we indirectly acknowledge (or refer to) the transaction. There is also a "genesis" transaction that is directly or indirectly approved by all other transactions. The genesis transaction is explained as follows. In the early days of Tangles, there were addresses that had all the tokens, and these tokens were sent to the addresses of other "founders" through genesis transactions. Emphasize that all the tokens here are generated from the Genesis transaction. In the future, tokens will not be created, and there will be no mining such that the jugglers will receive financial compensation from the air. The key idea of Tangle is as follows. To request a transaction, users must work to approve other transactions. Thus, users requesting transactions contribute to the security of the network. The nodes are assumed to verify that the authorized transaction is not conflicting. If a node finds that a transaction conflicts with a toggle, the node will not directly or indirectly approve the conflicting transaction. In this paper, we compare the performance of the IoT sensor based block chain with the color spectrum chain.

And IoT data can be seen that the performance value is staggered when the performance value is compared with the conventional blockchain and the color spectrum chain which can be verified with high degree. These values can never be determined to be significant values. Finally it can be said that the Capital expenditures (CAPEX) and Operating Expenditure (OPEX) values have grown.

In the graph, Qst, n represents the performance data value, Qchl, n is quality data values. In this comparison table, the performance data and the quality data scale were calculated in proportion to the time value. Performance can be improved by considering data processing speed (TPS), data processing process, etc. In some cases, performance degrades due to the data model structure, and inevitably degrades in performance due to large data size. In addition, there are cases where performance is deteriorated due to index creation without sufficiently considering index characteristics. In this paper, performance refers to performance of data retrieval. and infrequent, and there is a lot of single-item processing, whereas data retrieval is repetitive, frequent, and many cases are processed. This characteristic is that the nature of a general transaction has a pattern of inquiry, and in some cases, the performance of input/modification/deletion is important. Moreover, Qchl, n is the quality data, and it can be defined as securing the latestness, accuracy, and interconnection of data and giving it useful value to users. Systematic management and activities are required to continuously maintain or improve such data quality from the user's point of view. Therefore, "Data Quality Management" is defined as "a set of activities such as quality goal setting, quality diagnosis and improvement to secure data quality, and related tools to support it". In general, data quality management has been recognized as a task performed in the operation and utilization phase since data construction. However, the cause of major quality issues is found in the absence of quality management activities in the information system construction stage including data operation and utilization stages have. Therefore, the superiority of security is simulated by giving time value to the relationship between performance and quality. We compare the construction cost with the operation cost. Now, we compare the block chain of the internal sensor network with the method of constructing the block chain in the external cloud against the actual construction cost as follows.

(1) Direct costs associated with operating a block-chain server: IT, power, volume, storage and management of such resources.
(2) Indirect costs of operating a block-chain server: IT operations for network and storage infrastructure and general infrastructure management.
(3) Block chain server holding overhead: Needless to say, critical resources in scarcity, procurement and accounting workforce: IT management and processing.

The benefits of OPEX aspects of block-chain computing should be based on a clear understanding of CAPEX within the enterprise. Firms are limited in the amount of capital investment possible by the stock market. Even in the case of a private company, it must be restricted by financial institutions. Because CAPEX is limited, companies usually want to direct their investments to monetization activities. Many companies prefer renting rather than buying real estate because they do not want to keep valuable capital in liquid assets. Rightly or wrongly, there are many companies that see IT as an investment of the latter, so they endeavor to minimize this cost. This is why IT departments report to Chief Financial Officer (CFO)s in many companies. A financial consultant said IT was "a guy who poured in unexplained jargon and demanded a huge amount of cash," he said. From that point of view, it is easy to understand why the idea of cutting down on capital expenditures and turning it into a more cost-effective operating cost is so appealing to those who hit the abacus. Given all these factors, attempts to block cloud computing by comparing costs based on block-chain clouds versus internal block-chain server operating costs are not feasible. Unless cloud figures increase significantly, cloud economics has a myriad of attractive elements that top management can deserve. Therefore, the trade-off point between CAPEX and OPEX values was selected and designed.

4. Discussion

The colored spectrum chain is used A service model is highly necessary to keep a generated electronic document in a reliable third party and to check the authenticity of the electronic document stored in it for the purpose of dealing with the dispute or legal effect.

Note, however, that most service models related to electronic documents do not include the verification information of the signer in the digitally signed electronic document, and a separate document format such as an information package that can supplement the verification information is created. Signed electronic documents are transformed into a regulated format for long-term archiving; even when distributing electronic documents, a separate document format is used, which requires a very complicated process and costs a lot.

In particular, there are no technical specifications or verification methods for long-term verification in the certified electronic document repository. In long-term verification, the verification information included in the information package is used, so it is troublesome since many processes must be reversed. In addition, electronic documents stored on a long-term basis are not matched with the provisions of the RFC standard or the domestic electronic signature law. Therefore, there is a need for a method of efficiently securing the integrity of electronic documents for the long-term verification of electronic documents stored on a long-term basis.

The method proposed in this paper secures the authenticity of the electronic document itself. Even though it is changed to various forms such as document, image, or other multimedia according to the needs of the service provider, the integrity of the final version can be ensured by digital signatures with simple procedures and functions. Therefore, it can be applied to any type of service such as electronic notarization and electronic seal.

We compared the long-term verification service model based on the existing certified electronic document repository with the long-term verification model proposed in this paper.

Using the proposed model, the validity of the digital signature can be verified even after the expiration of the validity period of the certificate. Even if the validity period of the certificate expires, the certificate validation service can be provided by keeping the revocation information of expired certificates. The certification authority (CA) should ideally maintain the revocation information of expired certificates and provide the certificate verification service, and the retention period of the revoked certificate information should be determined by the policy. For long-term verification in particular, it is necessary to retain revoked certificate information permanently. Modification must also be made so that the archive cutoff field—which is an optional extension field—can be used to compare and verify Thermal priority and Chiller priority.

The mechanism for block-chain hacking is solved by using a color spectrum chain. We want to use blockchain technology to prevent many different hacking attacks. Moreover, blockchain technology is a technique that comes from a block-chain concept that prevents it from various hacks.

The blockchain protects the block from the risk of hacking through various methods and it automatically protects the block every time the block is created. This method is automatically created through various methods of generating through multi-level security Figure 18.

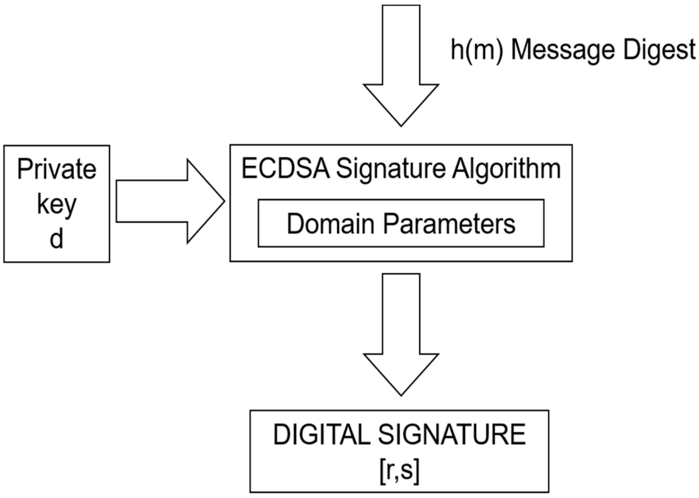


Figure 18. Transaction of blockchain.

When creating a transaction in a blockchain, it is passed to each node, including the digital signature. In this standard, ECDSA is used as the algorithm for signature generation, and the ID and IP of the object Internet device and resources are used for the signature creation message. ECDSA is an elliptic curve digital signature algorithm, and the existing digital signature generation algorithm has a merit that it can be implemented much faster using shorter key length than RSA, DSA, Diffie–Hellman etc. The existing RSA cryptosystem requires about 15,000 bits to provide similar security as the 512-bit ECDSA. Each node generates its own private key and public key, and generates an electronic signature by encrypting the private key and the generated IP address, port number, and ID in message form. The generated signature is attached to the transaction and sent to the other node, and the generated public key is also attached to the transaction. The node receiving the transaction can decrypt the encrypted signature using the enclosed public key and verify that the received transaction and signature are valid when a true return value is derived.

The problem of security that can occur in an existing naming system can be solved by the digital signature of blockchain. Digital signatures are used to identify the subject who created the information, and have the function of blocking information transformation and the intervention of malicious nodes.

The first step is to verify that the user is a legitimate user by using authentication. The digital signature generated by this standard is information that is encrypted by using the private key that only the owner can know, and it is confirmed that the signature is valid by using the public key. In the case of IP spoofing, a malicious node performs an action of changing an IP address, thereby causing a problem of receiving erroneous data if requesting an ID when searching for a resource stored in a blockchain. The problem of the security aspect can be solved by authenticating the user through the process of verifying the validity of the digital signature.

Second, the use of non-repudiation prevents users from denying that they have generated information. When generating a digital signature, it generates its own private key that no other user knows, so it can not deny that it created a transaction. In the case of a cybil attack, a single node masquerades as multiple nodes and uses malicious information to change data maliciously. When a single node masquerades as a global NRS server, a local NRS server, an OID server, and several nodes, the naming system data is maliciously changed and data reliability problems arise. In this standard, each node generates a digital signature using its own private key, so it cannot be deined that one node has generated the information and prevents it from being disguised as another node.

Third, use data integrity to ensure that the stored data is not corrupted/tampered with. By checking the block hash included in the blockchain, it is possible to check whether the information of the transaction included in the block is modified. The block contains a hash of the transaction, and adds the previous block hash to the block header. If the transaction information of a block is maliciously transformed, information of the block hash is transformed. If the block hash is different from the block owned by another node, it is determined that the data is falsified and the corresponding block is removed. Also, as the number of blocks connected to a blockchain increases, the amount of data to be changed maliciously increases, which further reduces the possibility of data overmodulation. If the root hash information is changed and the root hash is different from the block owned by another node, it can be judged that the data is falsified. Therefore, when the transaction information inside the block is converted maliciously, Configure the correct blockchain.

5. Conclusions and Future Work

We have proposed an authentication protocol to improve the efficiency and stability in the IoT environment.

In the IoT network domain, a session key is generated based on ID-based encryption between the access network and the core server, the device and the gateway are verified by using the generated session key, and a new identification value is given. The identification value is also updated automatically by adding an update protocol in the identification value.

The existing IoT environment is vulnerable to physical attack on vulnerability, compromise of credentials, attack through modification, protocol attack, attack on core network, and attack on user data and privacy. Moreover, intelligence communication devices are rapidly developing and becoming smaller. Therefore, we have designed an ID-based encryption authentication protocol that is lighter and more secure than the existing PKI-based authentication technology. We have implemented the proposed authentication protocol and compared the efficiency and stability with the existing IoT communication technology and PKI-based authentication technology. In terms of efficiency, the device registration rate is 185.7% faster, and the overall operation system is 83% faster than the existing PKI-based authentication technology. In the future, we need to study a wide range of authentication protocols to apply to various object communications.

There is a need for research on the authentication protocol for the authentication of devices collected by the IoT gateway through a local network rather than a device with the activated IoT function proposed in this study. It is also necessary to study the attack types by analyzing the types of attacks that are yet to be known and the dangers of rapidly developing IoT communications. Finally, we suggest block-based and IoT-based authentication using the color spectrum chain.

In this paper, the node that generates the information to be written in the blockchain transmits to the other nodes participating in the blockchain with the specified information storage type (transaction), and the node receiving the transaction performs the block hash algorithm and generates a block. The node that generated the block propagates the fact to another node, and the receiving node connects to the blockchain that it had after block verification and stores the information. Therefore, it is possible to create a platform structure that does not require a centralized database. The object Internet device and resource search framework proposed in this standard can solve security vulnerabilities of existing centralized NRS or OID server. The subject Internet device and resource search framework consists of the object Internet devices and resources constituting the block-chain network, namely the representative and participant node, and the authentication server.

The existing NRS service is a method of assigning IDs to the Internet devices, services and resources connected to network devices such as gateways and routers, and searching for the necessary IDs from the NRS server to find and connect IPs. In the case of OID, object ID is assigned to the object Internet device and resource to identify object.

Both of these two approaches present a hacking vulnerability problem in the central server. This standard defines a way to solve the problems of OID and NRS services and apply the functions to a distributed database using blockchains. The user who retrieves the ID can obtain the IP mapped with the corresponding ID by checking the hash of the blockchain owned by each node instead of the NRS server or the OID interpretation server.

Objects define the search framework components and requirements based on blockchain technology that ensures security functions such as authentication/non-repudiation/data integrity when searching for devices and resources based on the identity on the Internet, Figure 19.

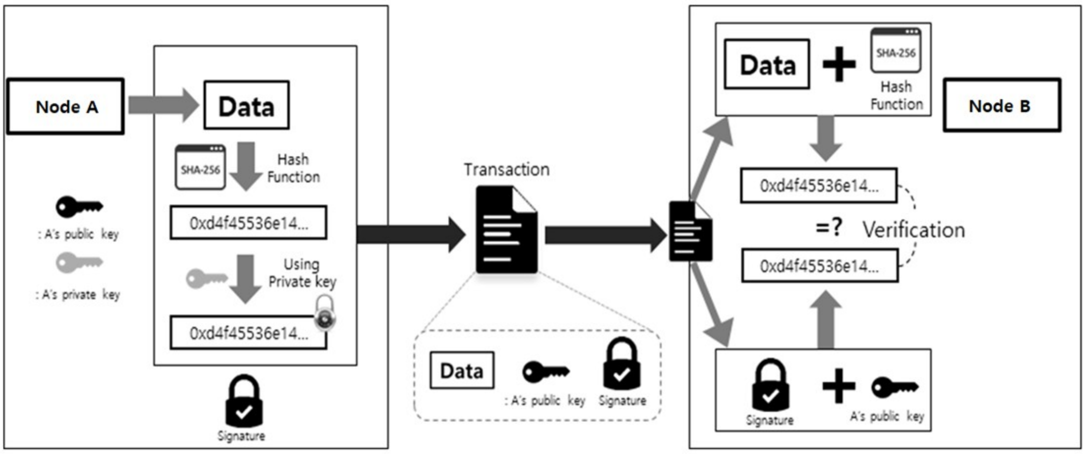


Figure 19. Generate signature blockchain.

The process of creating a transaction and generating an electronic signature in a blockchain network constituting the framework of this paper is as follows. It is a process of generating a transaction that generates information constituting a single block and a digital signature generation process used for transaction verification.

In the framework, the representative node and participant node records their ID, IP and port number in the transaction. The information stored in the transaction is as follows:

(1) When a participating node is connected to a representative node (e.g., a stuff Internet gateway) and generates a transaction by storing the device ID and IP address information.
(2) When participating nodes and representative nodes generate ID and IP address information, respectively, to create a transaction.

In the above two cases, the representative node and the participating node connected to the network are each a node participating in the blockchain and the node generating the transaction is transmitted to all the nodes participating in the blockchain. In the smart home/building, the IP and port number information of the nodes participating in the blockchain are all owned by the IP list and are transmitted to the nodes included in the IP list at the time of transaction creation or block generation. Each time the blockchain is updated, the corresponding IP list is stored in the form of a table in which the ID and the IP are mapped, and it is utilized at the time of ID search later. When the transaction is transmitted, the electronic signature and the public key generated using the private key of ECDSA are attached and transmitted. The node receiving the transaction first determines the validity of the transaction using the attached signature and public key, and when the decryption result of the signature is "true", it stores the transaction information and performs the block generation process. Therefore, the authentication and non-repudiation prevention of the transaction creator is confirmed through the decryption process of the digital signature.

In addition, the standard classifies object Internet devices and resource nodes participating in a blockchain into two types. The first is a representative node, which has sufficient storage space and is easy to store the blockchain and data, and has a relatively high computing power. Next, the participant node is basically defined as a blockchain node participating in the block generation process, while the block power is less than that of the representative node and the storage space is small, and the blockchain and the high-load data are not stored.

This standard defines two cases in which a representative node performs a consensus protocol in case of including a simple object Internet sensor that only generates data and a case in which a representative node and a participant node both execute a consensus protocol.

This also covers information exchange overhead costs. The information exchange overhead can be thought of as the "RAM" of the ethernet network's "GAS" fee EOS network. These etherium and EOS network group projects are considered to be the most widely used information exchange overheads in many dApp ecosystems that currently use block chains. This information exchange overhead is ultimately linked to the blooming economy. In addition, the complexity of the application of the framework. In addition, if the quality of the software is determined according to the capability of the developer according to the capability of the developer, the standard framework upgrades the developers so as to reduce the risk of business. By reusing proven technology structures and infrastructure services, developers can standardize development environments, application execution environments, and operator operating environments, thereby improving development productivity and reducing risk. In addition, quality and productivity are improved through the development of proven standard programs and templates, and all developers use the same platform, which enables them to build systems that ensure performance and stability through unified platform. In the event of a total system failure except for individual program failures, fault resolution can be facilitated through framework-based tracking and batch tuning becomes possible. This can improve overall development productivity, reduce operational efficiency, reduce IT costs and improve security.

Author Contributions: Conceptualization, S.-K.K.; Data curation, S.-K.K. and J.-H.H.; Formal analysis, S.-K.K.; Investigation, S.-K.K. and U.-M.K.; Methodology, S.-K.K. and J.-H.H.; Project administration, U.-M.K. and J.-H.H.; Resources, U.-M.K. and J.-H.H.; Software, U.-M.K. and J.-H.H.; Supervision, U.-M.K. and J.-H.H.; Validation, J.-H.H.; Visualization, J.-H.H.; Writing—original draft, S.-K.K. and J.-H.H.; Writing—review and editing, U.-M.K. and J.-H.H.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. 2017R1C1B5077157).

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

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdfpp1-9 (accessed on 1 June 2018).
2. Huh, J.-H.; Seo, K. Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. *J. Supercomput.* **2018**, 1–17. [CrossRef]
3. Huh, J.-H.; Otgonchimeg, S.; Seo, K. Advanced metering infrastructure design and test bed experiment using intelligent agents: Focusing on the PLC network base technology for Smart Grid system. *J. Supercomput.* **2016**, *72*, 1862–1877. [CrossRef]
4. Chen, Y. Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Bus. Horiz.* **2017**, *61*, 567–575. [CrossRef]
5. Kshetri, Y.N. Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–82. [CrossRef]

6. Savelyev, A. Copyright in the Blockchain era: Promises and challenges. *Comput. Law Secur. Rev.* **2018**, *34*, 550–561. [CrossRef]
7. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]
8. Kim, S.-K.; Huh, J.-H. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* **2018**, *11*, 1. [CrossRef]
9. Levin, R.B.; Waltz, P.; LaCount, H. Betting Blockchain Will Change Everything—SEC and CFTC Regulation of Blockchain Technology. In *Handbook of Blockchain, Digital Finance, and Inclusion*; Elsevier: New York, NY, USA, 2017; pp. 187–212.
10. Bank of Korea. Development strategy of digital innovation and payment service. In *Bank of Korea*; Bank of Korea: Seoul, Korea, 2016; pp. 1–23.
11. Seo, Y.-S.; Bae, D.-H. On the value of outlier elimination on software effort estimation research. *Empir. Softw. Eng.* **2013**, *18*, 659–698.
12. Gartner (2016). Available online: http://www.gartner.com/events/na/orlando-symposium/ (accessed on 1 June 2018).
13. Antonopoulos, A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*; O'Reilly Media Inc.: Sevastopol, CA, USA, 2014; pp. 1–73.
14. Beverly, Y.; Garcia-Molina, H. PPay: Micropayments for peer-to-peer systems. In Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, 27–30 October 2003; pp. 300–310.
15. Yoo, H.W. *Implementation and Performance Improvement Plan of Blockchain-Based Electronic Ballot System*; Graduate School of Information and Communication, Ajou University: Suwon, Korea, 2016; pp. 1–34. (In Korean)
16. Park, J.; Seo, Y.-S.; Baik, J. A comparative analysis of reliability assessment methods for web-based software. *Int. J. Softw. Innov.* **2013**, *1*, 31–44. [CrossRef]
17. Cheon, I.G. *Android Programming, Easy Explanations with Pictures*; Life and Power Press: Seoul, Korea, 2015. (In Korean)
18. Peters, G.W.; Panayi, E.; Chapelle, A. Trends in crypto-currencies and Blockchain technologies: A monetary theory and regulation perspective. *J. Financ. Perspect* **2015**, *3*, 1–43. [CrossRef]
19. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 3–16.
20. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
21. Huh, J.-H.; Seo, K. Design and test bed experiments of server operation system using virtualization technology. *Hum. Centric. Comput. Inf. Sci.* **2016**, *6*, 1–21. [CrossRef]
22. Huh, J.-H. PLC-based design of monitoring system for ICT-integrated vertical fish farm. *Hum. Centric. Comput. Inf. Sci.* **2017**, *20*, 1–19. [CrossRef]
23. Moon, S.-Y.; Park, J.-H. Efficient hardware-based code convertor of a quantum computer. *J. Converg.* **2016**, *7*, 1–9.
24. Nagaraju, S.; Parthiban, L. Trusted framework for online banking in public cloud usingmulti-factor authentication and privacy protection gateway. *J. Cloud Comput. Adv. Syst. Appl.* **2015**, *4*, 1–23. [CrossRef]
25. Massias, H.; Avila, X.S.; Quisquater, J.-J. Design of a secure timestamping service with minimal trust requirements. In Proceedings of the 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, 27–28 May 1999; pp. 1–8.
26. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
27. Bayer, D.; Haber, S.; Stornetta, W.S. Improving the efficiency and reliability of digital timestamping. In *Seq II: Methods in Communication, Security, and Computer Science*; Springer: Berlin, Germany, 1992; pp. 329–334.
28. Haber, S.; Stornetta, W.S. Secure names for bit-strings. In Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, 1–4 April 1997; pp. 28–35.
29. Muzammal, M.; Qu, Q.; Nasrulin, B. Renovating blockchain with distributed databases: An open source system. *Future Gener. Comput. Syst.* **2019**, *90*, 105–117. [CrossRef]

30. Prybila, C.; Schulte, S.; Hochreiner, C.; Webe, I. Runtime verification for business processes utilizing the Bitcoin Blockchain. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
31. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
32. Saberi, S.; Kouhizadeh, M.; Sarkis, J. Blockchain technology: A panacea or pariah for resources conservation and recycling? *Resour. Conserv. Recycl.* **2018**, *130*, 80–81. [CrossRef]
33. Huh, J.-H. Server Operation and Virtualization to Save Energy and Cost in Future Sustainable Computing. *Sustainability* **2018**, *10*, 1919. [CrossRef]
34. Qin, B.; Huang, J.; Wang, Q.; Luo, X.; Liang, B.; Shi, W. Cecoin: A decentralized PKI mitigating MitM attacks. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
35. Wang, H.; He, D.; Ji, Y. Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
36. Löbbe, S.; Hackbarth, A. Chapter 15: The Transformation of the German Electricity Sector and the Emergence of New Business Models in Distributed Energy Systems. In *Innovation and Disruption at the Grid's Edge*; Sioshansi, F.P., Ed.; Elsevier: Amsterdam, The Netherlands, 2017; pp. 287–318.
37. Huh, J.-H. *Smart Grid Test Bed Using OPNET and Power Line Communication*; IGI Global: Hershey, PA, USA, 2017; pp. 1–425.
38. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized Blockchain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
39. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162. [CrossRef] [PubMed]
40. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerComWorkshops), Kona, HI, USA, 13–17 March 2017.
41. Underwood, S. Blockchain beyond bitcoin. *Commun. ACM* **2016**, *59*, 15–17. [CrossRef]
42. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Self-managed and Blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany, 12–16 September 2016; pp. 137–140.
43. Pass, R.; Shi, E. Fruitchains: A fair Blockchain. In Proceedings of the ACM Symposium on Principles of Distributed Computing, Washington, DC, USA, 25–27 July 2017; pp. 315–324.
44. Karame, G. On the security and scalability of bitcoin's Blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1861–1862.
45. Kiayias, A.; Koutsoupias, E.; Kyropoulou, M.; Tselekounis, Y. Blockchain mining games. In Proceedings of the 2016 ACM Conference on Economics and Computation, Maastricht, The Netherlands, 24–28 July 2016; pp. 365–382.
46. Hori, M.; Ohashi, M. Adaptive Identity Authentication of Blockchain System-the Collaborative Cloud Educational System. In *EdMedia+ Innovate Learning*; Association for the Advancement of Computing in Education (AACE): Waynesville, NC, USA, 2018; pp. 1339–1346.
47. Lee, S.; Huh, J.H. An effective security measures for nuclear power plant using big data analysis approach. *J. Supercomput.* **2018**, 1–28. [CrossRef]
48. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. *IJ Netw. Secur.* **2017**, *19*, 653–659.
49. Eom, S.; Huh, J.H. Group signature with restrictive linkability: Minimizing privacy exposure in ubiquitous environment. *J. Ambient Intell. Humaniz. Comput.* **2018**, 1–11. [CrossRef]
50. Huh, J.-H. Implementation of lightweight intrusion detection model for security of smart green house and vertical farm. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1–11. [CrossRef]
51. Seo, Y.-S.; Bae, D.-H.; Jeffery, R. AREION: Software effort estimation based on multiple regressions with adaptive recursive data partitioning, Information and Software technology. *Inf. Softw. Technol.* **2013**, *55*, 1710–1725. [CrossRef]
52. Jabbar, K.; Bjørn, P. Growing the Blockchain information infrastructure. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017; pp. 6487–6498.

53. Tsiropoulou, E.E.; Baras, J.S.; Papavassiliou, S.; Qu, G. On the Mitigation of Interference Imposed by Intruders in Passive RFID Networks. In Proceedings of the International Conference on Decision and Game Theory for Security, New York, NY, USA, 2–4 November 2016; pp. 62–80.
54. Sagduyu, Y.E.; Ephremides, A. A game-theoretic analysis of denial of service attacks in wireless random access. *Wirel. Netw.* **2009**, *15*, 651–666. [CrossRef]
55. Babaioff, M.; Dobzinski, S.; Oren, S.; Zohar, A. On Bitcoin and red balloons. In Proceedings of the 13th ACM Conference on Electronic Commerce, Valencia, Spain, 4–8 June 2012; pp. 56–73.