A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective

Authors:

Seong-Kyu Kim, Jun-Ho Huh

Date Submitted: 2018-09-21

Keywords: smart grid security, smart grid, advanced metering infrastructure (AMI), market operation with demand response, Blockchain, ICT (information and communication technology) solutions for demand response, Java implementation, Rainbowchain, Computer Architecture

Abstract:

Interest in green energy has increased worldwide. Therefore, smart grid projects to form a more efficient and eco-friendly intelligent grid by combining information technology (IT) technology with the existing grid are actively being conducted. In Korea, a national-level smart grid project road map has been confirmed, and an action plan has been prepared. Despite such actions, there may appear various threat scenarios in the application of the IT to the grid as a reverse function. Security technology is a measure to respond to such threats effectively. The security technology of a smart grid is an important factor that is directly related to the success or failure of the smart grid project. A smart grid is a new type of next-generation grid born of the fusion with IT. If the smart grid, the backbone of the power supply, is damaged by a cyberattack, it may cause huge damage, such as a nationwide power outage. In fact, there is an increasing cyberattack threat, and the cyber security threat to the smart grid is not insignificant. Furthermore, the legal system related to information protection is also important in order to support it systematically. In this paper, the necessity of the smart grid is examined, and the industry's initiative toward the smart grid security threat and threat response is examined. In this paper, we also suggest a security plan of applying Rainbowchain, the Blockchain technology, to the smart grid and energy exchange. We propose achieving superior performance and security functions by using Rainbowchain, which contains seven authentication techniques among existing Blockchain technologies, and propose the ecosystem and architecture necessary for its application.

DOI of Published Version: https://doi.org/10.3390/en11081973 *energies*

MDPI

Article

A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective

Seong-Kyu Kim [1,2,3] and Jun-Ho Huh [4,*]

[1] School of Electronic and Electrical Engineering, Sungkyunkwan University, Seoul 110-745, Korea; guitara7@skku.edu
[2] Mytsystem, Seoul 06149, Korea
[3] Puroom, Seoul 06149, Korea
[4] Department of Software, Catholic University of Pusan, Busan 46252, Korea
[*] Correspondence: 72networks@pukyong.ac.kr or 72networks@cup.ac.kr

Received: 10 July 2018; Accepted: 24 July 2018; Published: 30 July 2018

check for updates

Abstract: Interest in green energy has increased worldwide. Therefore, smart grid projects to form a more efficient and eco-friendly intelligent grid by combining information technology (IT) technology with the existing grid are actively being conducted. In Korea, a national-level smart grid project road map has been confirmed, and an action plan has been prepared. Despite such actions, there may appear various threat scenarios in the application of the IT to the grid as a reverse function. Security technology is a measure to respond to such threats effectively. The security technology of a smart grid is an important factor that is directly related to the success or failure of the smart grid project. A smart grid is a new type of next-generation grid born of the fusion with IT. If the smart grid, the backbone of the power supply, is damaged by a cyberattack, it may cause huge damage, such as a nationwide power outage. In fact, there is an increasing cyberattack threat, and the cyber security threat to the smart grid is not insignificant. Furthermore, the legal system related to information protection is also important in order to support it systematically. In this paper, the necessity of the smart grid is examined, and the industry's initiative toward the smart grid security threat and threat response is examined. In this paper, we also suggest a security plan of applying Rainbowchain, the Blockchain technology, to the smart grid and energy exchange. We propose achieving superior performance and security functions by using Rainbowchain, which contains seven authentication techniques among existing Blockchain technologies, and propose the ecosystem and architecture necessary for its application.

Keywords: smart grid security; smart grid; advanced metering infrastructure (AMI); market operation with demand response; Blockchain; ICT (information and communication technology) solutions for demand response; Java implementation; Rainbowchain; Computer Architecture

1. Introduction

The size of the smart grid has been increased, and various ICT (information and communication technology) technologies have been installed into the existing grid. Various devices for the smart grid form the Internet of Things (IoT) via the internet connection, and it creates optimal power consumption and efficient power generation [1–3].

The term "smart grid" is a combination of "smart", which means brilliant, and "grid", which means electric and gas supply network. It is also referred to as the "next-generation grid" and the "intelligent grid". It is a "next-generation grid by adding smart grid to existing ICT, the power production and consumption information are given and taken in two-way at real time to enhance energy efficiency". That is to say, the smart grid is a service for more effective electrical supply management by providing electricity user information both to the supplier and producer. By using electricity and IT technology, the grid is intelligent and advanced enough to provide high-quality power service and to maximize energy use efficiency.

Every year, it seems that the earth is becoming hotter. We have begun inventing new words for extreme weather, such as "fire hot weather" and "worst cold". The records for the hottest day and the coldest day are broken every year. Due to such weather fluctuation, the power usage fluctuates. Rapid temperature changes cause difficulties in power supply and management. The government has responded by instituting a maximum recommended setting during the winter for public institutions, department stores, and store facilities. In addition, the government recommends that large office buildings reduce their power consumption by 10%. Apartment management offices are also advising their tenants to save energy.

Due to global warming, the world is paying attention to green growth. Many countries are searching for new energy sources and are developing renewable energies, such as solar power and water power. At the same time, technologies to enhance energy efficiency are being explored with greater urgency.

The smart grid is a technology and energy policy that is derived from such issues. The United States (US) recently announced a national vision called "Grid 2030" for the purpose of achieving an economic boost through the modernization of aging grids and has promoted the modernization of the grid and distribution of smart meters. However, security problems can also occur in the smart grid system, which currently take place in the online environment, by connecting devices to the internet. Thus, this study aims to develop a stable transaction system by block chaining and distributing a ledger considering advanced metering infrastructure (AMI), the key to a smart grid and various environments between power exchanges.

In addition, P2P (Peer-to-Peer) transactions should always be performed along with existing B2B (Business-to-Business) and B2G (Business-to-Government) for the energy-trading method using the Blockchain. To do that, integrity is always important.

In order to deal with energy electricity, we propose a Rainbowchain that is one step further upgraded from the existing Blockchain authentication method by using the smart contract function, which always has high integrity, and using Blockchain.

2. Related Research

2.1. Smart Grid

The smart grid is a next-generation power grid for optimizing energy production and consumption through the real-time information exchange between the supplier and consumer by combining IT technology with a supplier-focused power supply structure [3–6]. Furthermore, as shown in Figure 1, power production and consumption information are managed, and distributed resources are efficiently managed, by introducing sensor and computing technologies and two-way communication, which are important ICT technologies, to the power grid.

The most important thing for electricity trading is verification work that the energy transaction is accurate and transparent, because energy trading is now monopolized by the central government or large corporations.

For the most part, government agencies or big corporations can be trusted, but they can be neutralized by hackers or other attacks. Therefore, it is necessary to make electricity trading transparent by using the distributed ledger of the Blockchain for power trading and to improve reliability through seven different certifications by using the Rainbowchain among the necessary Blockchain technologies.

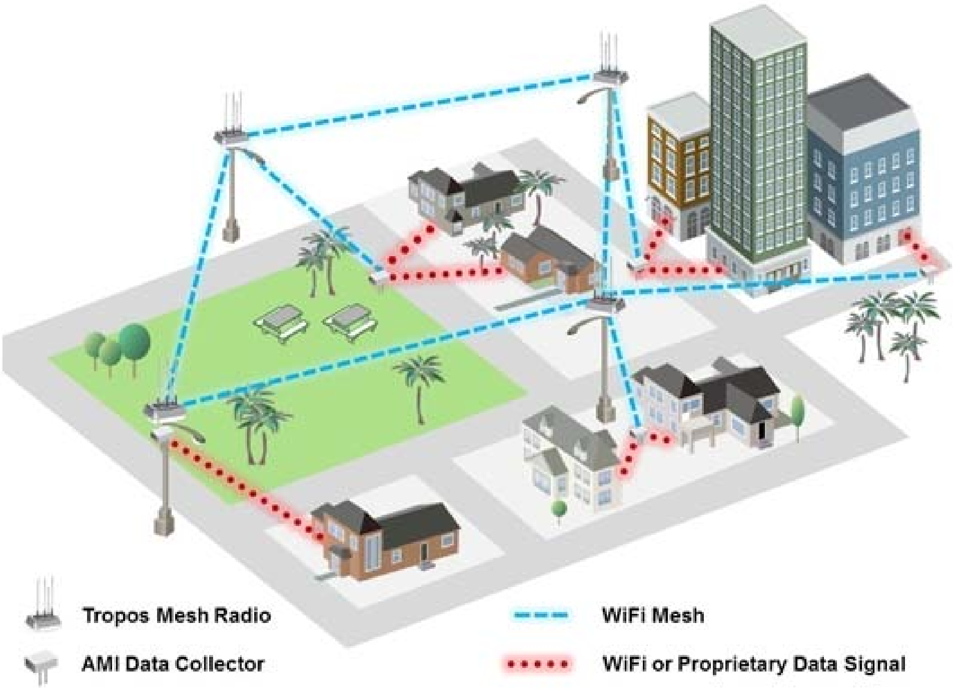


Figure 1. Diagram of smart grid.

It applies a differentiated power rate system by power supply and demand condition in order to distribute power consumption. It also shows the usage and power rate in real time in order to induce consumers to save energy voluntarily. The power producer can also enhance the stability of the grid and reduce costs through remote automatic metering. As such, it increases operational efficiency and reduces the investment of the power plant due to the reduction of the maximum power demand. Consumers may charge power to the energy storage device during the time when the power rate is low. Conversely, they sell electricity at times when demand is high. As such, they become prosumers.

In the first power layer, the distributed power source system connection and intelligence transmission system development take attention. The intelligent transmission network contains an intelligent power device, such as a smart meter to control the transmission network efficiently through the automatic restoration function by the grid operator, and it is expected that a distributed transmission network and distributed power to the customer system, a high-pressure direct current transmission system (HVDC3), a flexible transmission system (FACTS), and an auto recovery function will be introduced. In the second communication layer, it is necessary to use the existing communication network and to develop a new communication infrastructure for two-way communication between the power producer and consumers. The third layer can use power line communication and wireless local area network. The fourth layer, the application layer, can use applications, such as remote advanced metering infrastructure (AMI), consumption reaction, power storage, and electric car.

2.2. Blockchain

Blockchain technology can shift the current centralized ledger system to a distributed ledger due to the public key algorithm. It also has encryption technology and ensures low costs due to the distribution processing structure. Blockchain technology is the biggest threat to the payment settlement intermediary system [6–9]. This is because P2P financial transaction is possible via the internet without the intervention of a financial institutions or a trusted third party (TTP). Blockchain is the infrastructure security technology that serves as the foundation for "Bitcoin", which is the most widely used virtual currency. The Blockchain technology in Bitcoin is a kind of distributed digital ledger that saves the transfer history of Bitcoin value and is issued periodically. This ledger is produced with encrypted technology to prevent forgery. The digital ledger to record transactions of encrypted money publicly to transfer the ownership of Bitcoin also starts from a genesis block. The chain containing an individual block contains information of the previous block and Blockchain, which means that all transaction information starts from storage and management by distribution into various nodes (Figure 2 [10–12]).

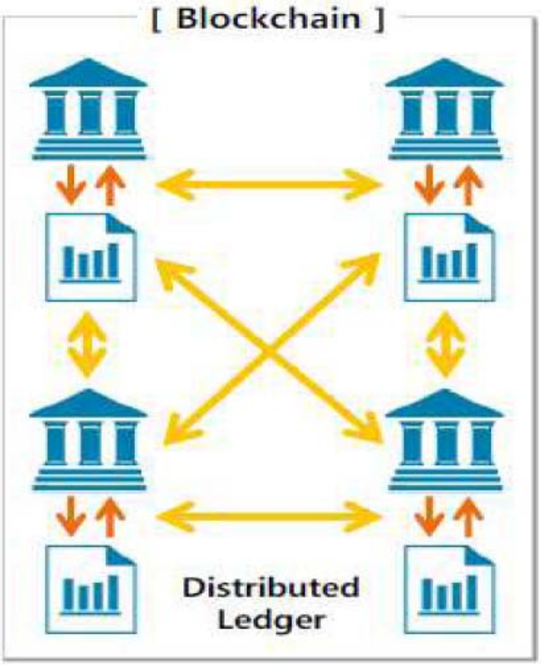


Figure 2. Diagram of Blockchain.

Blockchain can be explained in three forms, including public, private, and consortium (Table 1). As for public Blockchain, if all participants verify the transaction details, it may be helpful for integrity, but it may cause privacy problems. Also, there is information, such as internal information and trade secrets that must be hidden in the capital market. Private Blockchain is a method to fill the realistic need in the actual operation by securing high privacy. Finally, the consortium is a half centralized Blockchain that is composed of a consortium of various institutions. As pre-selected nodes have rights, the N number of institutions operate one node each, and a transaction takes place if there is consent among the nodes in each institution. The right to read the records of the Blockchain is granted to all participants, or to select institutions only, to disclose to specific personnel through API (application programming interface).

Table 1. Type of Blockchain.

Items	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 known in advance	Transaction verification is made by central institution	Transation verifier is known through cetification transaction verification and block

Various technologies are used for device certification. The most powerful technology for security is a certification system using a device certificate under the public key infrastructure (PKI), which has the highest safety and device identification function. Republic of Korea's KEPCO (Korea Electric Power Corporation), in the AMI security public hearing in June 2015, announced AMI security technology and policy using the PKI-based certificate. The PKI-based certification system is composed in the form of hierarchy by application [13–15]. It consists of a registration server (RA) that checks the certification requester face-to-face, a certification server (CA) that issues a certificate, and an OCSP (online certificate status protocol) server that verifies the certificate online. However, with the existing certification method, the central CA server plays that role, and it follows the central concentration method. For the sake of convenience, there is an increasing number of cases of new systems and services to which it can be applied besides Bitcoin. For example, it includes a certifying system of ownership by digitalizing certification information and assets of bank customers by distribution storage of financial transaction details and a certifying system of the existence by verifying data, such as registration or certification [16–19]. Recently, as a concept verification to connect with the IoT internet, Samsung Electronics and IBM (International Business Machines Corporation) announced a system called ADEPT (autonomous decentralized peer-to-peer telemetry). However, the smart grid system adopts a device certification method using Blockchain technology rather than a centralized certification method [20–25]. Energy division is another industry where real-time and mass transactions are made physically and financially with the power transaction at its center. With specialty and technical ability, large power companies and energy companies monopolize this industry. However, with the recent development of ICT, mobile, AI (artificial intelligence), and big data, Blockchain technologies are being introduced to the energy market. However, close cooperation with security technology is required due to ceaseless attacks by hackers.

In this paper, we can deal with power trading automatically by sharing power transaction information between the energy supplier and consumer of energy Blockchain.

3. Design and Implementation of Smart Grid Security Performance and Blockchain Smart Grid Perspective

3.1. Issue Raising

Smart grid is a next-generation grid born of the fusion with IT technology. If the smart grid, the backbone of the power supply, is damaged by cyberattack, it may cause huge damage, such as nationwide power outages. In fact, there is an increasing cyberattack threat, and the cyber security threat to smart grid is not insignificant. Therefore, this study examines the cyber security threat against the smart grid and also examines efforts to strengthen the cyber security of the smart grid domestically and internationally. The cyber security coordination task group (CSCTG) of NIST (national institute of standards and technology), a security standardization group in the US, an advanced country with respect to the smart grid (Figure 3), also raised the need for enhanced cyber security. Security measures are critical to prevent any national disaster due to the breakdown of the grid. Therefore, it is necessary to consider the international standard ISO 27001 [15] and Korea's Information Security Management System (ISMS) to reestablish security as a distributed concept using Blockchain technology. Accordingly, this study suggests Blockchain as a security system for domestic and international smart grids.

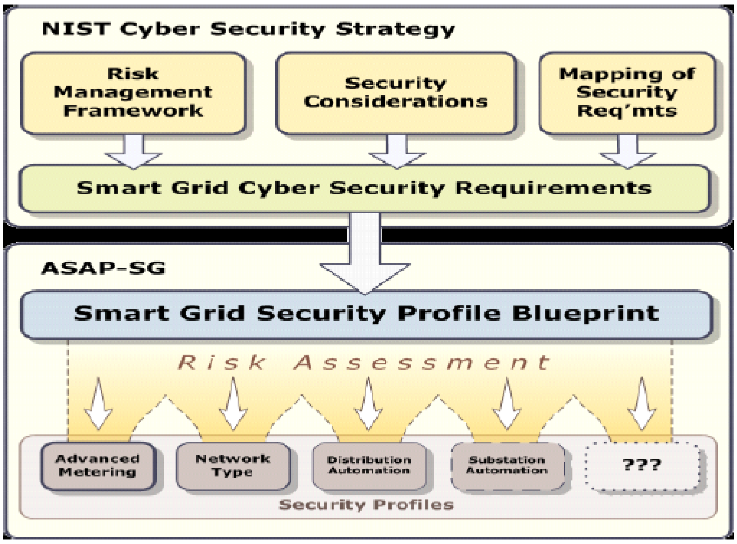

NIST Cyber Security Strategy
Risk Management Framework
Security Considerations
Mapping of Security Req'mts
Smart Grid Cyber Security Requirements
ASAP-SG
Smart Grid Security Profile Blueprint
Risk Assessment
Advanced Metering
Network Type
Distribution Automation
Substation Automation
???
Security Profiles

Figure 3. NIST Cyber Security Strategy. ASAP-SG: advanced security acceleration project for smart grid; NIST: national institute of standards and technology.

3.2. Research Methodology

Rainbowchain is a Blockchain technology that induces symmetric compensation through dual chains on a consent algorithm. It certifies seven categories to enhance the reliability of Blockchain through mutual competition and symmetry, considering the case of the transferable efficiency through the branch sequence randomizing method.

As the block verification and consent in the existing P2P network is not a chain technology that considers the limit of consent delay, it needs a method to overcome this. Proof-of-work of a node that participates in block verification does not consider the proportionate increase of a block transaction.

For a typical chain, it is advantageous to verify it in sequence by typifying the block structure for a chain. An atypical chain has an architecture that is not in a fixed structure of a block using an atypical chain. This means that the attributes that form the block are not structured. Because the existing blockchain is made of structured serial bits, it presents a limit regarding its use in the energy management system and smart grid system.

Elements forming such an atypical chain use a hash algorithm considering the extend chain in order to avoid using the fork method, and it also has a point. A hash point is a structure that connects with another chain, allowing the expansion of the existing structure. If an existing Blockchain exchanges a block through a fork as a P2P independent chain structure, the atypical chain structure does not create complete consent between the two peers due to unstable network suspension behavior through the fork. Thus, it designs a method to maintain the connection link using expansion.

However, expanding an atypical chain also has limits. Thus, the existing database has the capacity for addition and modification of the field and table. Like the addition of the field to refer to the table index, Rainbowchain is designed to expand by using a hash pointer to the format element that forms a block.

Such expansion can make a process for interlocking various servers, as the node in the central network can apply the naturally generated expansion. Thus, it can be flexible. If the length of an existing block is settled in a typified size, the atypical chain can have variable block lengths. Accordingly, Rainbowchain is designed to expand from an existing Blockchain.

Also, Rainbowchain provides seven authentication algorithms. It is a Blockchain technique to increase the reliability of a Blockchain through mutual competition and mutual consideration considering the possibility of relocating through seven authentication chains for the consensus algorithm and transferability through the branch sequential random verification method.

Block verification and agreement in the existing P2P network is not a chain technique considering the limit of delay of consensus, so a method to overcome this is necessary.

The proof-of-work of the nodes participating in the verification of the block does not take into account the proportional increase of the transactions in the block, so a Rainbowchain technique is needed.

3.3. Smart Grid Security Performance and Blockchain Smart Grid Perspective

This study uses Blockchain in the share method structure used in the existing Blockchain and structured seven new chain methods using Rainbowchain including Blockchain.

If the certificate method is a centralized structure where CA and Roof-CA play an important role in the center, Rainbowchain verifies seven safe share methods escaping the first share method through seven various kinds of verification methods of Blockchain.

This is because security issues can arise with respect to a Blockchain due to the development of quantum computing. As for the competition of compensation, the transaction recorded on the block through reasonable decision-making can have an individual node. The problem is that the individual node must have synchronized to disperse risks. The resource retention of participating nodes wants all compensation. It is necessary to announce the most suitable purpose of compensation, and it must be shared reasonably. It is therefore necessary to provide compensation for competitive participation. Further, the information path is not a right in a specific place; it is owned by the subject creating information. If the subject creating information is recorded on a specific platform as a value of information and if the compensation is given through the value of the relevant record, it can be said that the value attribution is transferred. The problem is that it is difficult to verify that the value transfer is not an initiated value. Thus, Rainbowchain was proposed.

Blockchain is confirmed through the verification of Rainbowchain (Figure 4). The Rainbowchain architecture is a tool to assist in rational decision-making. In addition, rational physicians will try to distinguish between meaningfulness and connectivity, and the transactions recorded in the blocks are held separately for each node. The problem is to distribute the risk by synchronizing all the nodes in each group. All you have to have is a book on individual transactions. It is important that you keep your books on individual transactions in hand. This should lead to the transaction of the node, whose verification of the block has been confirmed.

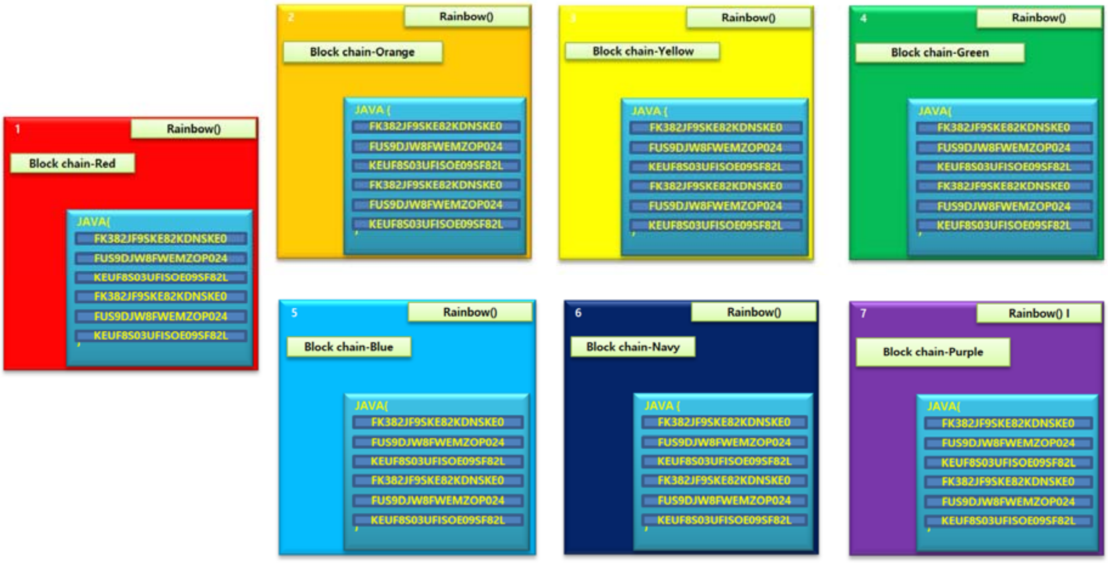


Figure 4. Rainbowchain architecture.

All the resource holding behaviors of the participating rainbow nodes want compensation. It is necessary to publicize what is most suitable for compensation during the resource maintenance act and share it reasonably. In order for this rational sharing to be undermined, we must determine the reasonable price for compensation that has a positive impact through the Rainbowchain theory. However, such a reasonable price decision should make the mode node fall into a prisoner's dilemma. Here, the goal is to prevent the actors in the prisoner's dilemma from making dangerous—though rational—decisions that will ultimately have negative implications for all the actors involved, and instead to reduce the risk of bad decision-making so that choices can be made that provide the best benefit. Thus, we need a game to encourage competitive participation.

These measurements serve to extract information about the process of the transaction. The path of information is not the right of a specific place but of the subject who created it. If the subject who created the information is recorded on a specific platform with the value of this information and wants to be compensated through the value of the record, the attribute of the value can be said to have been transferred. The problem is that it is difficult to prove that the transfer of these values is their leading value. It can also be a Byzantine process to compare whether values interpretations are favorable.

We assume that the rainbow nodes are *A*, *B*, *C*, *D*, *E*, *F*, and *G*. *B*, *C*, *D*, *E*, *F*, and *G* are allowed to participate in the probability that "0" will be generated according to the degree of difficulty of the hash of transaction of node *A*. We also assume that the following are true:

- This participation is not necessary.
- This participation must be rewarded.
- This participation is granted at random.

In this paper, we propose a new method for selecting random nodes in order to reduce the number of random nodes.

Random nodes do a PoW (Proof of Work) to produce a result whereby the hash of the transaction is "0" according to the difficulty of the transaction. If a nonce is found to be "0", it compensates according to the nascent value criterion constant from the first node to the last node that is found or not found.

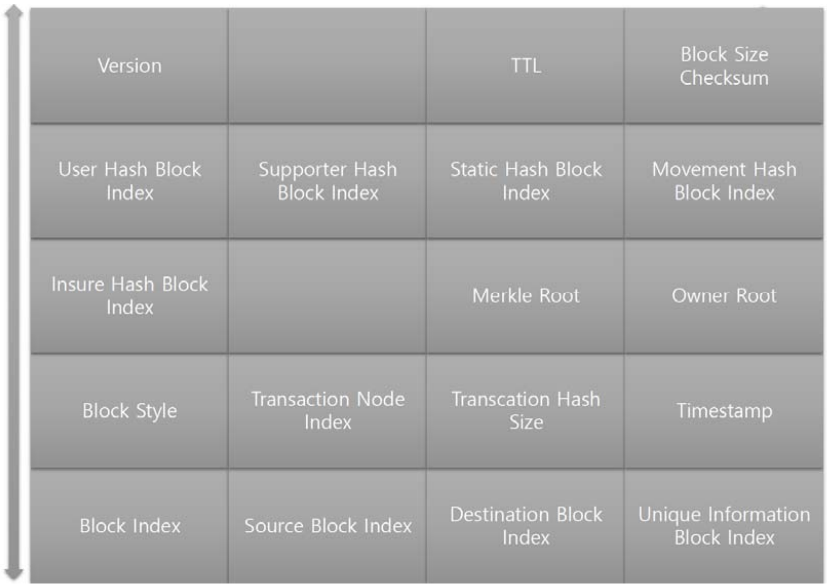
The nonce of the first node that found the nonce is written to the block.

The node *A* does not participate in the operation of the next node *A* in order to prevent the one-way hash of the node from increasing. However, if it is not an operation of node *A*, participation is possible, and the possibility is low. Also, we want to eliminate random node operation and irrationality.

The following is a description of node creation of Rainbowchain (Figure 5):

- How to create a block;
- Information to put in a block;
- Rainbow chain trust credentials (trust: trust of business relationship, trust of time);
- Unstructured blockchain: proof-of-work;
- Orthogonal Whitechain: proof of block;
- Increased reliability, increased security, increased availability;
- Unstructured Blockchain;
- Orthopedic Whitechain;
- Based on Whitechain nodes through physical information.

Rainbowchain and the work node are determined by adjusting the block difficulty according to the participation rate and the coin trading volume. The difficulty determination is based on the acceleration of the traffic limit curve. In order to prevent infinite increases of the transaction compensation by the seismic cancellation rate, the addition of the previous block is calculated based on the increase/decrease ratio of the previous block based on the limit model. The difficulty constant of the traffic limit curve in the difficulty determination model is called the limited ovarian number threshold multiplier.



Version		TTL	Block Size Checksum
User Hash Block Index	Supporter Hash Block Index	Static Hash Block Index	Movement Hash Block Index
Insure Hash Block Index		Merkle Root	Owner Root
Block Style	Transaction Node Index	Transcation Hash Size	Timestamp
Block Index	Source Block Index	Destination Block Index	Unique Information Block Index

Figure 5. Rainbowchain node. TTL: Talent Tech Lab.

Also, the informal chain means that the structure of one block is not defined. This means that the attributes that make up the block are not structured. The existing Blockchain is structured with continuous bits, which is a limitation for application to the smart grid energy.

The elements constituting the informal chain have hash points considering extended chains in order to avoid using the fork method. The hash point is a structure for linking other chains considering that the existing chain structure should be extended. If the existing Blockchain is an independent chain structure of P2P and the block is exchanged through the fork, the unstructured chain structure we have devised is a way to maintain a connection link that utilizes extensions in view of the inability to create a full agreement between peers due to unstable network suspension behavior through these forks.

In addition to adding fields and adding and modifying tables in existing databases, you can extend them with a hash pointer to the element of the formatting block, just as you would add a field to the reference 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. Because the length of the variable block can extend infinitely, the concept of time to limit it is applied to induce a marginal block increase, thereby preventing the transaction from overflowing.

Trust in a Rainbowchain also means that transactions and time must at least have synchronous time intervals. The criterion for determining that the time interval is synchronous is that the process of confirming when the transaction has occurred should be through the Rainbowchain. The block transmitted through the Rainbowchain is time-sensitive considering the network transmission state of not exceeding 255 TTL: Talent Tech Lab (transactions that have gone to the router with time to live) is generated.

The trust to be described here is that transactions and time must have at least synchronous time intervals. The criterion for determining that the time interval is synchronous is that the process of confirming the point in time of the transaction should be through the Rainbowchain, and the blocks transmitted through the Rainbowchain should be transmitted over a network transmission rate not exceeding 25 TTL (10% of 255). This means that the time recognition considering the state has occurred.

The chain that maintains the trust is called the verification chain. In order to derive the agreement of the unstructured block, the hash of the previous block and the verification block are concurrently referenced so that the time information has the attribute of consensus.

In addition, it provides the trust of the generated block. It means to contain all the transaction information in 3 s, because it is an irregular block. It means to solve the situation where the false information in the Byzantine problem is not reached within a certain time. All block generation takes place every 3 s, and all transaction information should be contained within the 3 s interval, after which the block verification and time synchronization should be done.

You also have to define a hash function as follows:

- Hash, Key, Index;
- Hash pointer;
- Block pointer;
- Atypical structures are treated in a json manner and logo.

The cipher block of the data created by applying the value of the specific header must be verified by using the block information of the Whitechain.

To prove a block, the role of the RainbowChain has an approver (intermediary) function that creates a block with a structured structure and generates the next block using the hash of the pointer issued by the chain. This sequence of information allows the next block to determine the degree of difficulty. The formula (*t*) block generation method for the hash generation cycle is reflected through the API relation used in the authentication and transaction process.

Finally, the intermediary role determines the hash difficulty based on the number of occurrences (frequency) of the transactions and the information associated with the previous block, and the next block is spontaneously generated every second. If no transaction occurs, a block is created. Therefore, users can create the difficulty and hash code generated in the previous block in the trusted role. The hash code is used to generate code that is interpreted based on the CPU (central processing unit), and it plays a role of maintaining the compensation of the block as long as the participation in the block continues. In addition, the role that maintains the block is maintained as an open pool of P2P, and the private key can be maintained over the broadcast network defined by the unstructured Blockchain.

The architecture is defined as a Rainbowchain architecture for smart grid measurements. It is proved from the creation of Rainbowchain. Each block has the hash of the previous block and the level of difficulty needed to contain a rapid transaction, to compete, and to compensate the transaction. With this level of difficulty, the number of "0" s generated to the block is found. Such verification is made through all nodes, which enables enhanced reliability.

A block quickly contains transactions, and it has reliability of transaction in terms of confidentiality, usability, functionality, and interoperability (Figure 6). To prove integrity and to prevent denial, the transaction does not use saved nodes but provides random rights to other participating nodes. In this way, it forms a consent structure that verifies through the outcome of "0" in a specific time. Such a system is applied to the smart grid system and the energy exchange in order to design the systematization of power exchange and energy exchange.

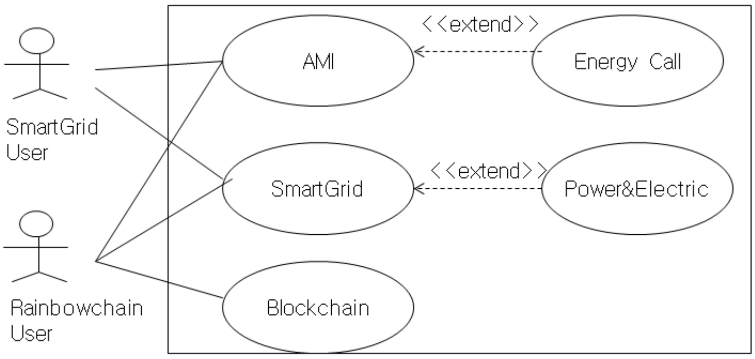


Figure 6. Rainbowchain use-case diagram.

Also, see the class diagram using Rainbowchain among the Blockchains (Figure 7). We designed the Rainbowchain class using power, AMI, and an instruction table. We also designed a diagram of the Rainbowchain security scheme (Figure 8).

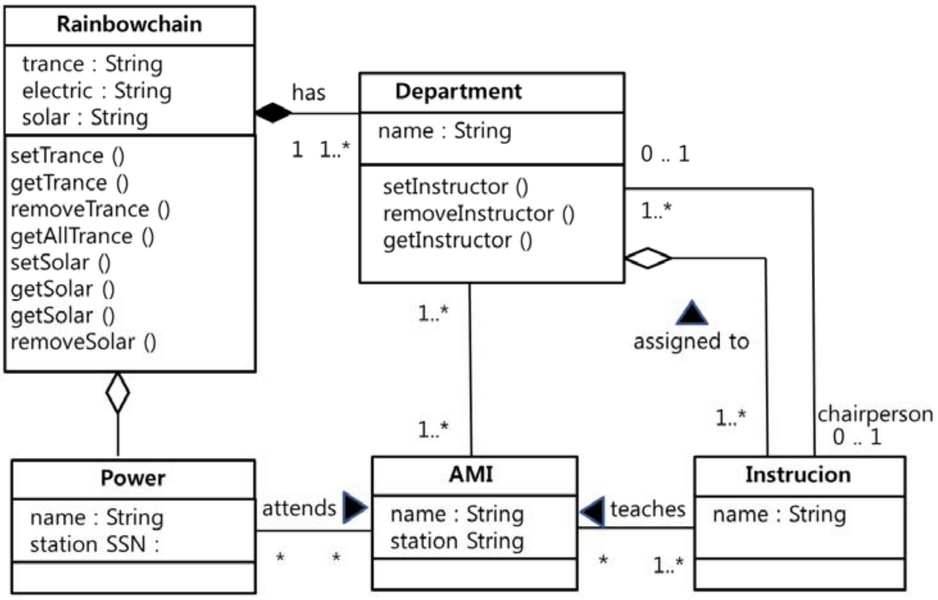


Figure 7. Rainbowchain class diagram. *: routine.

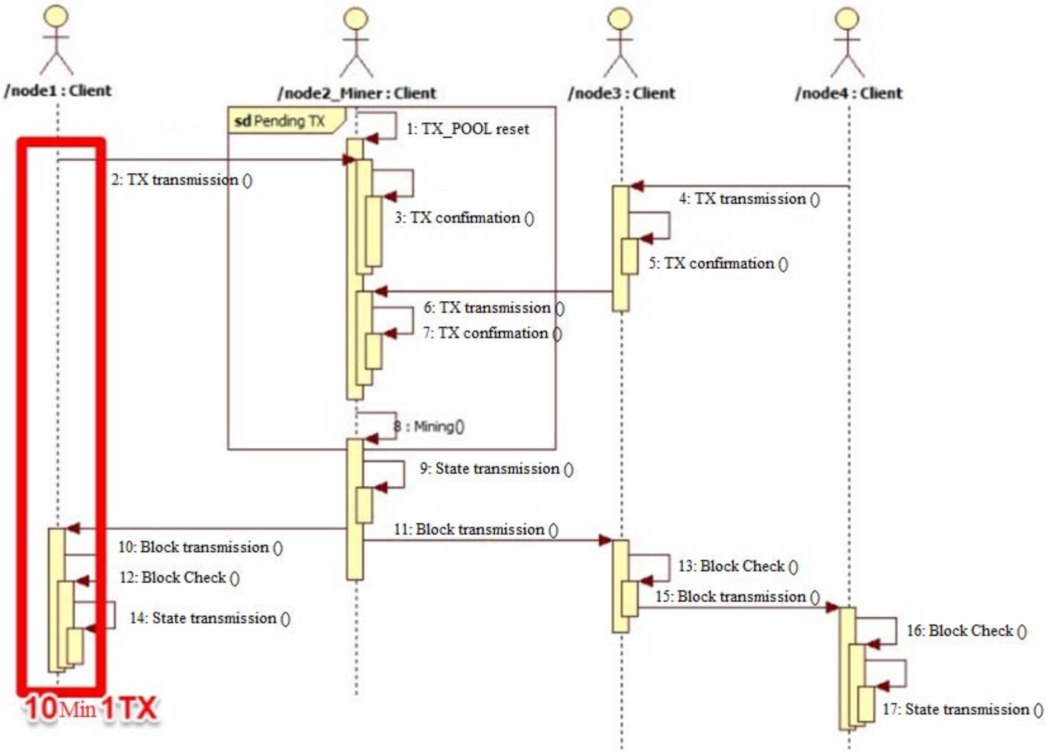


Figure 8. Rainbowchain Architecture Conclusion. TX: transaction.

If the trajectory in the X direction of the end-effector is to be generated by reflecting location, velocity, and acceleration by making use of the Rainbowchain, then the trajectory can be expressed in the five-level polynomial equation about time, t, as follows:

$$S(t) = At^5 + Bt^4 + Ct^3 + Dt^2 + Et + F \tag{1}$$

$$\dot{\mathrm{S}}(t) = 5At^4 + 4Bt^3 + 3Ct^2 + 2Dt + E \tag{2}$$

$$\dot{\mathrm{S}}(t) = 20At^3 + 12Bt^2 + 6t + 2DS \tag{3}$$

The above Equations (1)–(3) show six unknown numbers of A, B, C, D, E, and F, so we need six equations to obtain each of them.

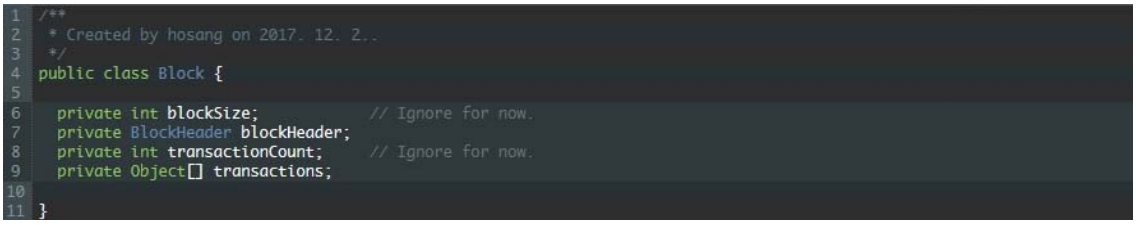
If the value t = 0 and the value t = T are as shown above, we have three initial conditions in Equation (4) and three final conditions, so we can obtain A, B, C, D, E, and F, the coefficients of the polynomial equation. If t = 0, then S(0) = F = S_0, and F will be found by linear simultaneous equations. Therefore, if put in the format of a matrix, then it will appear as follows:

$$\begin{gathered} s(t) = Re\left\{ \left\{ \sum_{i=\frac{N_s}{2}}^{\frac{N_s}{2}-1} d_i + \tfrac{N_s}{2} \exp\left(j2\pi \left(f_c - \tfrac{i+0.5}{T} \right) (t - t_s) \right) \right\}, t_s \leq t \leq t_s + T \right. \\ s(t) = 0, t < \ t_s \ \hat{} \ \ t \ > t_s + T \end{gathered} \tag{4}$$

In the equation used to obtain A, B, C, D, E, and F, as shown in Equation (5), if the inverse matrix of the 6 × 6 matrix is multiplied on both sides, you will find that security is more enhanced than when we use Rainbowchain by creating a speed profile.

$$\begin{bmatrix} S_0 \\ S_T \\ \dot{S}_0 \\ \dot{S}_T \\ \ddot{S}_0 \\ \ddot{S}_T \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ T^5 & T^4 & T^3 & T^2 & T & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 5T^4 & 4T^3 & 3T^2 & 2T & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 20T^3 & 12T^2 & 6T & 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \\ D \\ E \\ F \end{bmatrix} \tag{5}$$

In pseudo Java code, a block is an individual unit constituting a Blockchain, and each block is connected to form a Blockchain. The key component of the block is the previous block's hash information and transactions that are needed for the Blockchain connection. Each block has a value of the previous block hash in the block header, parent block. In this way, going back to the parent block, you will see the first block that can no longer find the parent, which is called the genesis block (Figure 9).



```
/**
 * Created by hosang on 2017. 12. 2..
 */
public class Block {

  private int blockSize;              // Ignore for now.
  private BlockHeader blockHeader;
  private int transactionCount;       // Ignore for now.
  private Object[] transactions;

}
```

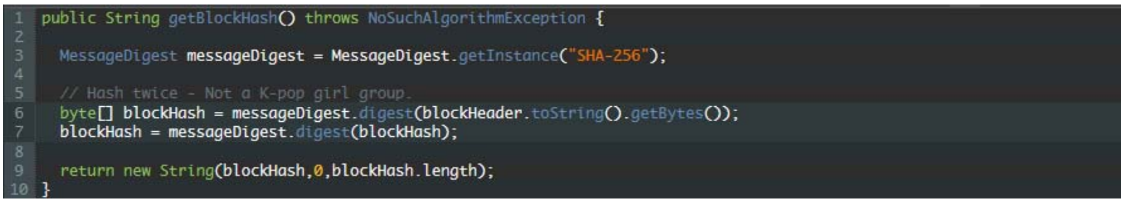
Figure 9. Rainbowchain equations.

Also, the block size, block header, transaction counter, and transaction information is defined as follows:

- Block size: The block size is the size of the data except this field is expressed in bytes.

- Block header: The block header is an object that contains the metadata of the block.
- Transaction count: This field stores the number of transactions.
- Transaction: A collection containing transaction information.

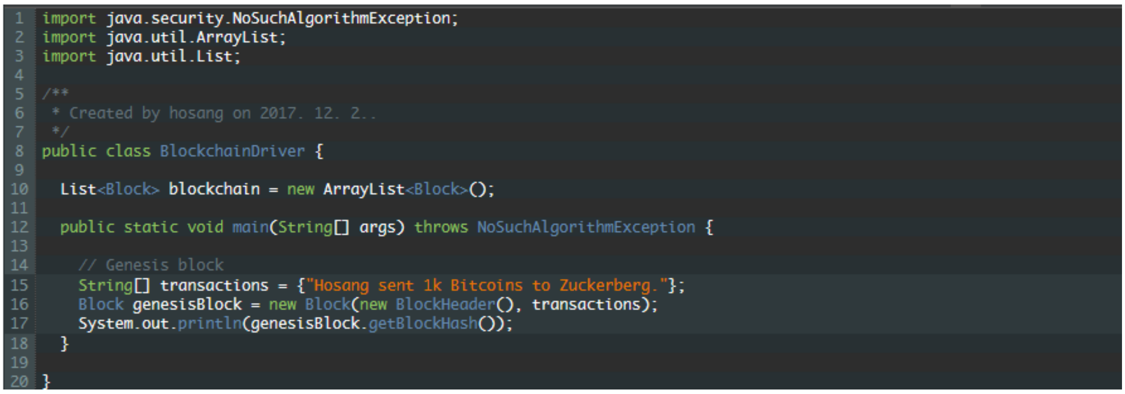
Now, in order to create a new block using the verification method of seven techniques of Rainbowchain, a hash value of a previous block to which a corresponding block is to be connected is set. The block hash value is not stored in the form of data in the block. Figure 10 is a code that applies the above-described "Rainbow SHA-256" algorithm by adding the get block hash method to the block class to quickly perform block hash computations on the node.



```java
public String getBlockHash() throws NoSuchAlgorithmException {

  MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

  // Hash twice - Not a K-pop girl group.
  byte[] blockHash = messageDigest.digest(blockHeader.toString().getBytes());
  blockHash = messageDigest.digest(blockHash);

  return new String(blockHash,0,blockHash.length);
}
```

Figure 10. Computation of block hash using the rainbow SHA (secure hash algorithm)-256.

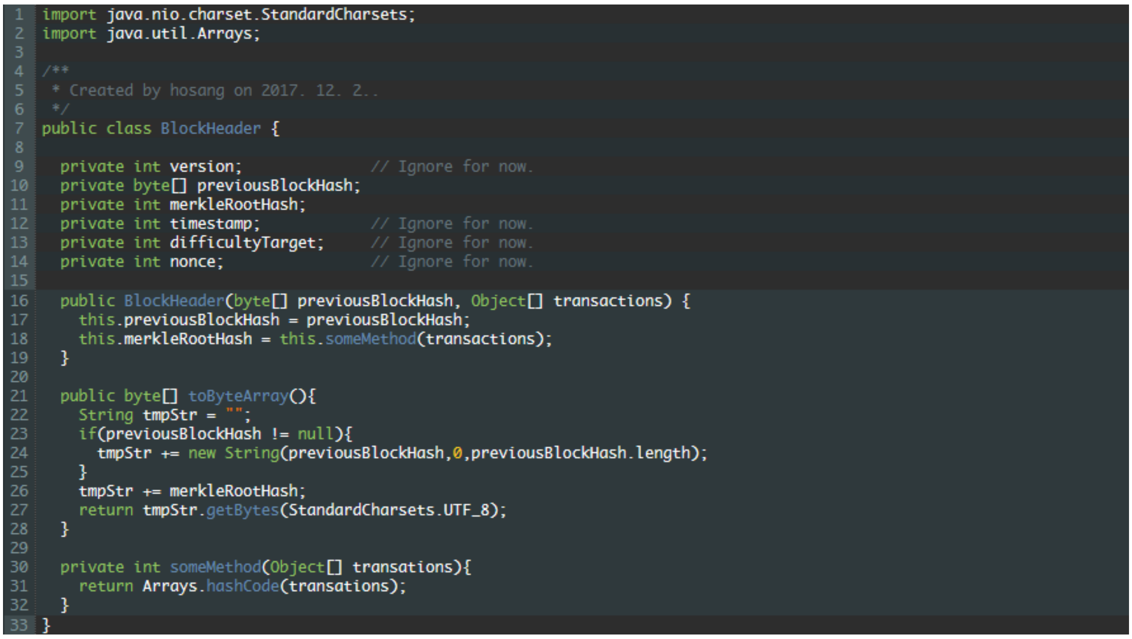
In Figure 11, you can see some strange occurrences in that the value of the block hash does not change even if the contents of the transactions are modified. If the transaction is forged, the value of the block hash is changed. Therefore, the previous block of the connected block does not match the previous hash value of the connected block. However, this code does not change the value of the block hash even if the array of transactions is changed. This is because the transaction history does not affect the block header data, while minimizing code writing to understand the concept. In the real Blockchain implementation, the contents of the block header are changed because the transaction details affect the Merkel root hash value in the block header. That is, the value of the block hash created through the data of the block header is also changed.



```java
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

/**
 * Created by hosang on 2017. 12. 2..
 */
public class BlockchainDriver {

  List<Block> blockchain = new ArrayList<Block>();

  public static void main(String[] args) throws NoSuchAlgorithmException {

    // Genesis block
    String[] transactions = {"Hosang sent 1k Bitcoins to Zuckerberg."};
    Block genesisBlock = new Block(new BlockHeader(), transactions);
    System.out.println(genesisBlock.getBlockHash());
  }

}
```

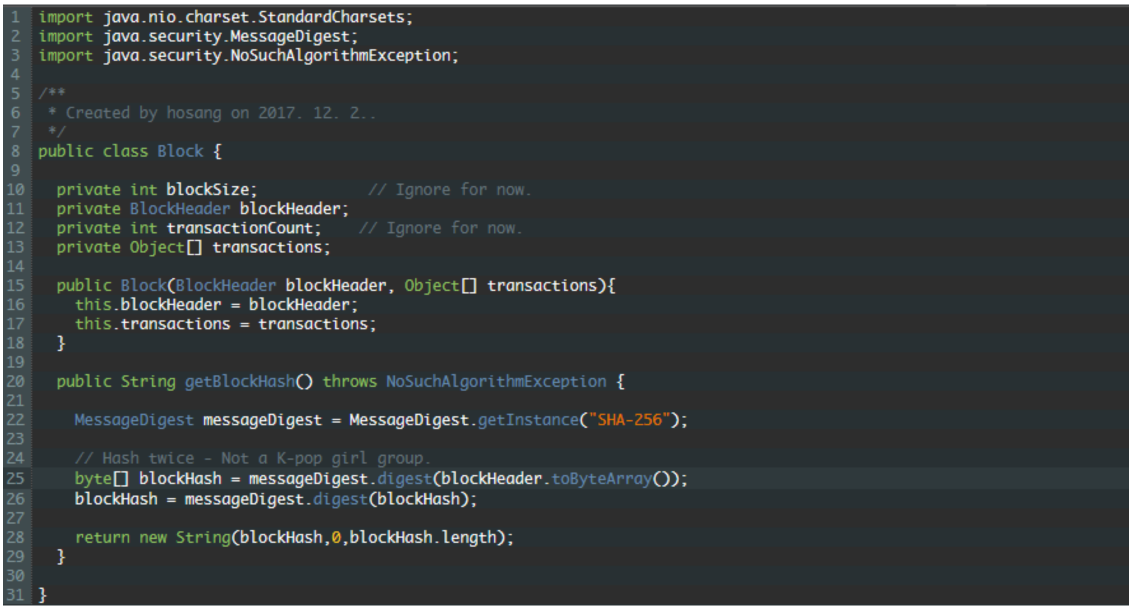
Figure 11. Generation of original block (genesis block) and output of the block hash value.

This being so, we will modify the code slightly so that the value of the block hash can be changed when the transaction is forged. First, in order to make the transaction history affect the block header data, after receiving the transaction details as a factor of the block header constructor, we modify the code to calculate this data by using a certain method (someMethod). Figures 12 and 13 show an implementation in this content, and the computation logic of the actual muckle hash value is omitted.



```java
import java.nio.charset.StandardCharsets;
import java.util.Arrays;

/**
 * Created by hosang on 2017. 12. 2..
 */
public class BlockHeader {

  private int version;              // Ignore for now.
  private byte[] previousBlockHash;
  private int merkleRootHash;
  private int timestamp;            // Ignore for now.
  private int difficultyTarget;     // Ignore for now.
  private int nonce;                // Ignore for now.

  public BlockHeader(byte[] previousBlockHash, Object[] transactions) {
    this.previousBlockHash = previousBlockHash;
    this.merkleRootHash = this.someMethod(transactions);
  }

  public byte[] toByteArray(){
    String tmpStr = "";
    if(previousBlockHash != null){
      tmpStr += new String(previousBlockHash,0,previousBlockHash.length);
    }
    tmpStr += merkleRootHash;
    return tmpStr.getBytes(StandardCharsets.UTF_8);
  }

  private int someMethod(Object[] transations){
    return Arrays.hashCode(transations);
  }
}
```

Figure 12. Constructor of the block header.

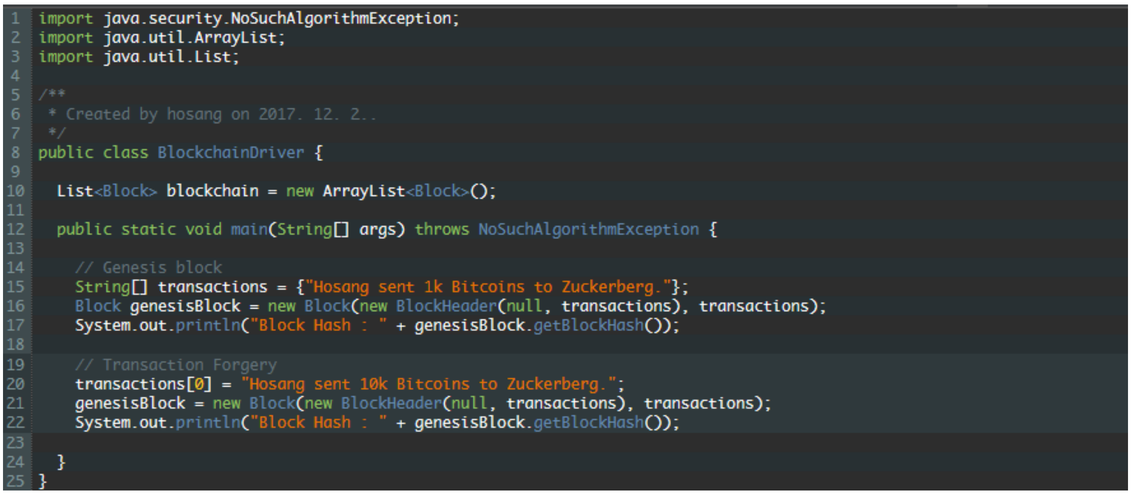


```java
import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

/**
 * Created by hosang on 2017. 12. 2..
 */
public class Block {

  private int blockSize;            // Ignore for now.
  private BlockHeader blockHeader;
  private int transactionCount;    // Ignore for now.
  private Object[] transactions;

  public Block(BlockHeader blockHeader, Object[] transactions){
    this.blockHeader = blockHeader;
    this.transactions = transactions;
  }

  public String getBlockHash() throws NoSuchAlgorithmException {

    MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

    // Hash twice - Not a K-pop girl group.
    byte[] blockHash = messageDigest.digest(blockHeader.toByteArray());
    blockHash = messageDigest.digest(blockHash);

    return new String(blockHash,0,blockHash.length);
  }

}
```

Figure 13. Block hash calculation.

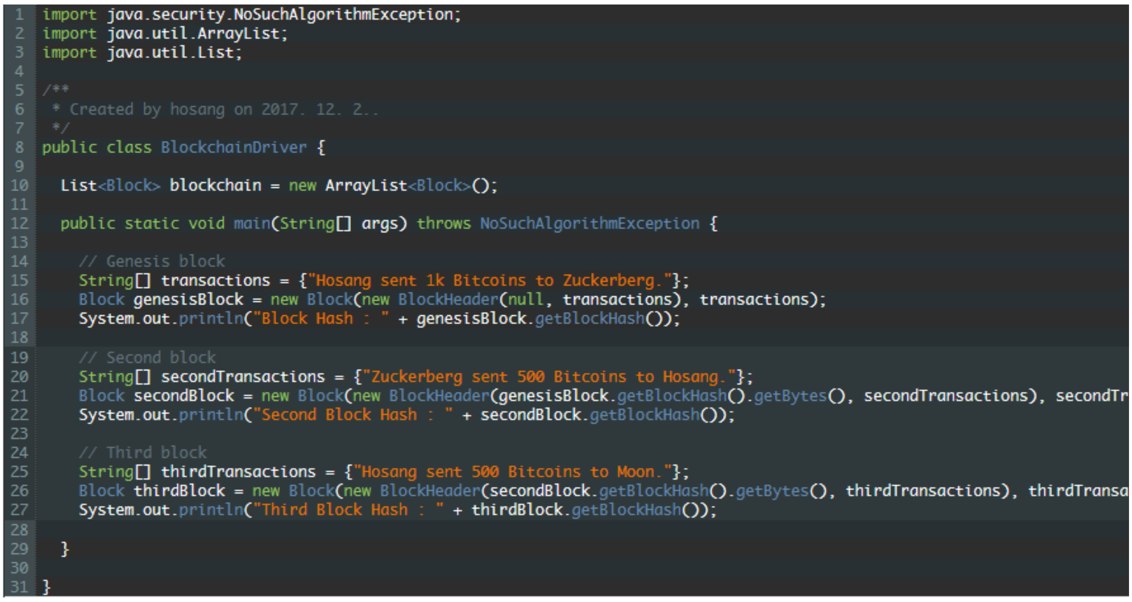
The output code of the first block generation and block hash is now shown in Figure 14. It can be seen that the change in the transaction details affects the value of the actual block hash.

Now that we have completed the creation of the initial block and the output test of the block hash, we will see how the Blockchain operates by creating two additional blocks and concatenating them to the original block. Figure 15 generates two blocks and sets the hash value of the previous block to the previous block hash value of the linked block. Here, we confirm that when changing the floor value of the previous block, not only the hash value of the corresponding block, but also the hash value, is changed. However, if the transaction details of the second block are modified, there is no change in the hash value of the first block.



```java
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

/**
 * Created by hosang on 2017. 12. 2..
 */
public class BlockchainDriver {

  List<Block> blockchain = new ArrayList<Block>();

  public static void main(String[] args) throws NoSuchAlgorithmException {

    // Genesis block
    String[] transactions = {"Hosang sent 1k Bitcoins to Zuckerberg."};
    Block genesisBlock = new Block(new BlockHeader(null, transactions), transactions);
    System.out.println("Block Hash : " + genesisBlock.getBlockHash());

    // Transaction Forgery
    transactions[0] = "Hosang sent 10k Bitcoins to Zuckerberg.";
    genesisBlock = new Block(new BlockHeader(null, transactions), transactions);
    System.out.println("Block Hash : " + genesisBlock.getBlockHash());

  }
}
```

Figure 14. Modification of block hash calculation code.



```java
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

/**
 * Created by hosang on 2017. 12. 2..
 */
public class BlockchainDriver {

  List<Block> blockchain = new ArrayList<Block>();

  public static void main(String[] args) throws NoSuchAlgorithmException {

    // Genesis block
    String[] transactions = {"Hosang sent 1k Bitcoins to Zuckerberg."};
    Block genesisBlock = new Block(new BlockHeader(null, transactions), transactions);
    System.out.println("Block Hash : " + genesisBlock.getBlockHash());

    // Second block
    String[] secondTransactions = {"Zuckerberg sent 500 Bitcoins to Hosang."};
    Block secondBlock = new Block(new BlockHeader(genesisBlock.getBlockHash().getBytes(), secondTransactions), secondTr
    System.out.println("Second Block Hash : " + secondBlock.getBlockHash());

    // Third block
    String[] thirdTransactions = {"Hosang sent 500 Bitcoins to Moon."};
    Block thirdBlock = new Block(new BlockHeader(secondBlock.getBlockHash().getBytes(), thirdTransactions), thirdTransa
    System.out.println("Third Block Hash : " + thirdBlock.getBlockHash());

  }

}
```

Figure 15. Generation and connection of second and third block using hash value.

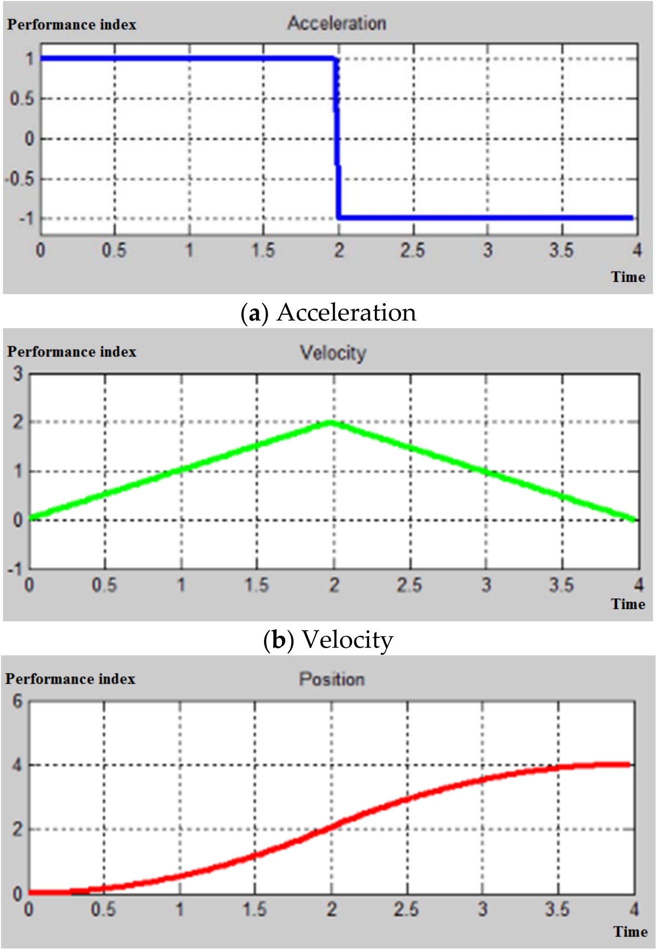
If you actually run this code, you can see that when you change the transaction history (string) of the previous block, the hash value of the block, as well as the hash value of the next block to be linked, are changed. Because of this chain effect, to change the transaction history of one of the blocks constituting the Blockchain, all the blocks associated with the block must be recalculated.

So far, we have implemented the structure of Java code to advance the security performance through the implementation of the data structure of the block constituting the Blockchain and the operation method of the Blockchain through the Java code.

We also show that the performance is improved when we derive the result using Rainbowchain using MATLAP using the blockchain algorithm.

We define the security performance, defense rate, and TPS (transactions per second) performance of the Rainbowchain as three values: acceleration, velocity, and position.

Also, measuring the security performance of Rainbowchain using MATLAP (Figure 16) proves that the security is excellent.



(**a**) Acceleration

(**b**) Velocity

(**c**) Position

Figure 16. Rainbowchain MATLAP performance data. (**a**) Acceleration; (**b**) Velocity; (**c**) Position.

We have simulated the security protection performance of the existing smart grid network by defining maximum concurrent, real-world traffic throughput, and HTTP (Hyper Text Transfer Protocol) response time.

The above graph shows the existing smart grid network (Figure 17) and maximum concurrent (after generating a normal HTTP session, sending an exploit packet will result in a nonstateful).

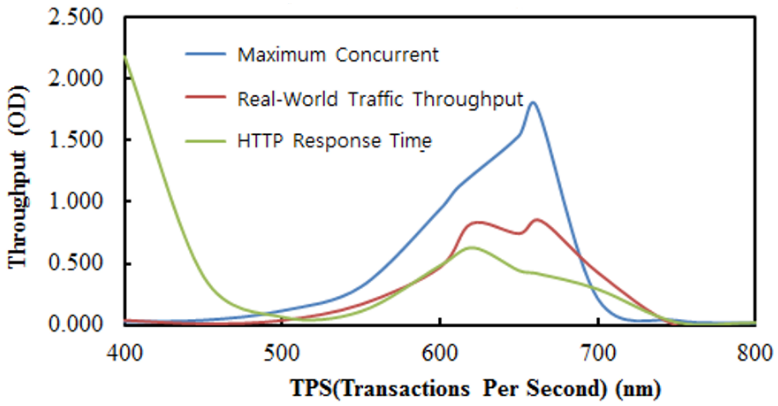


Figure 17. Default smart grid security performance.

HTTP response time (44 KB, 21 KB, 10 KB, 4.5 KB, and the maximum throughput for HTTP response size of 1.7 KB) and the real-world traffic throughput (Figure 18) show that the TPS and throughput values are slightly higher when the test data are simulated. Therefore, security performance is improved.

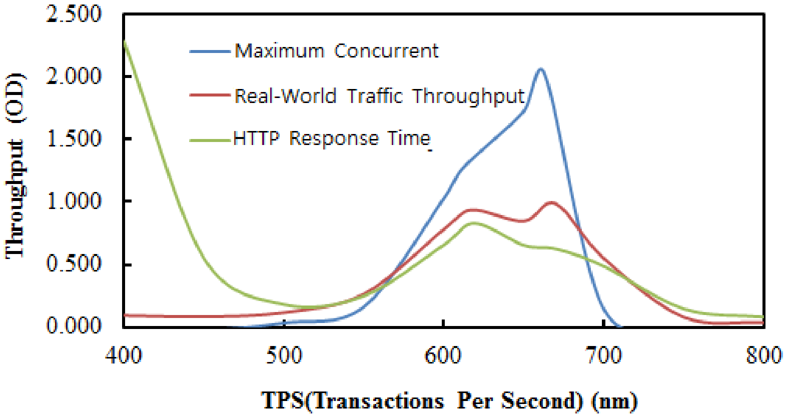


Figure 18. Smart grid security performance with Blockchain.

As a result, when we simulate using Rainbowchain, we can see that the maximum concurrent, which is the security performance, is increased as shown in Figure 17.

4. Discussion

This study continues to review considerations such as security threats that can take place through the Blockchain service development and security functions. For example, as a response measure to the reduction of usability, when it applies “restriction of validity verification participant” or “selective transaction information save”, it may cause additional security threats. As new developments and improvements to the security technologies for Blockchain are expected, it is necessary to review the latest security technology research trends. In particular, in preparation for the commercialization of quantum computing technology, it is necessary to review safe key creation technology and related trends in quantum computing.

Also, the structure for Blockchain authentication of the power data of the smart grid is drawn below (Figure 19).

To apply the Rainbowchain to the smart grid, the static model structure mainly identifies data, structures, and class structures. Looking at the dependency graph between package modules, we can see that the wallet depends on the primitive information below.

Other important packages are as follows:

- RPC: Sends commands or data between Blockchain network participants.
- Consensus: manages the Merkle tree and handles consensus among participants, and Mercury Protocol summarizes transactions and manages encrypted hash values.

The primitive package defines the structure of the block and transaction, which is the core of the Blockchain, and manages block chaining and transaction information. The Blockchain index that connects the blocks is defined as follows in the CBlockIndex class (Figure 20).

CBlockIndex is the base class of CBlock, and the structure of the connecting chain of blocks is managed by using a hash map and block index, which have block information as the following class diagram. The actual Blockchain data is stored on a disk and serialized to memory as needed (Figure 21).

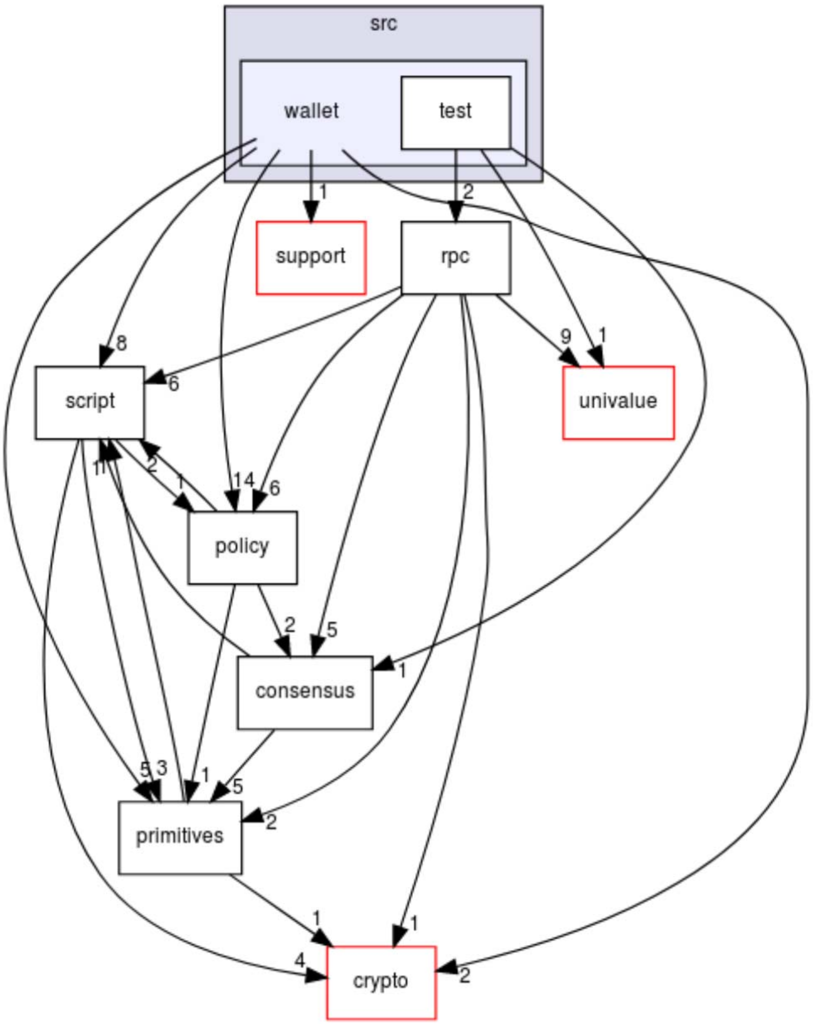


Figure 19. Smart grid of static Rainbowchain.

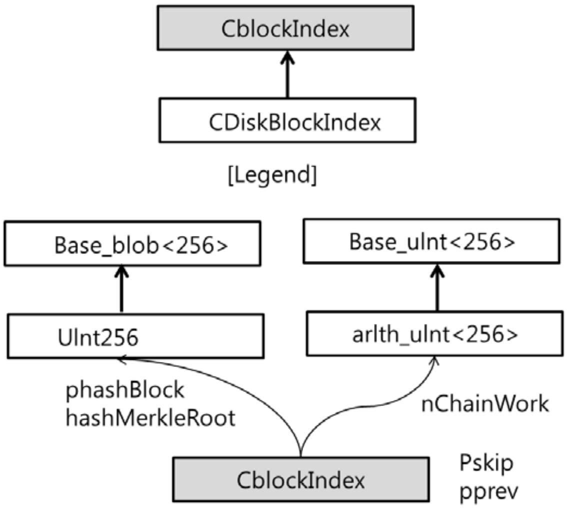


Figure 20. CBlockIndex.

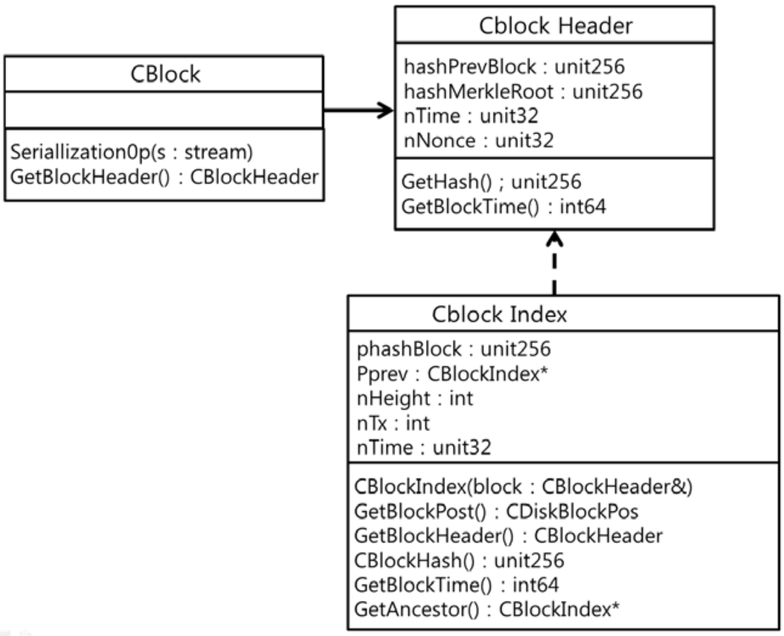


Figure 21. CBlock class.

The method of securing the reliability and traceability of the block information is that the Blockchain holds the hash and the transaction history. The hash generation uses the SHA (secure hash algorithm)-256 function as in the below call graph.

The following is a very brief summary of the structure of the smart grid-based rainbow chain information model analyzed so far (Figure 22).

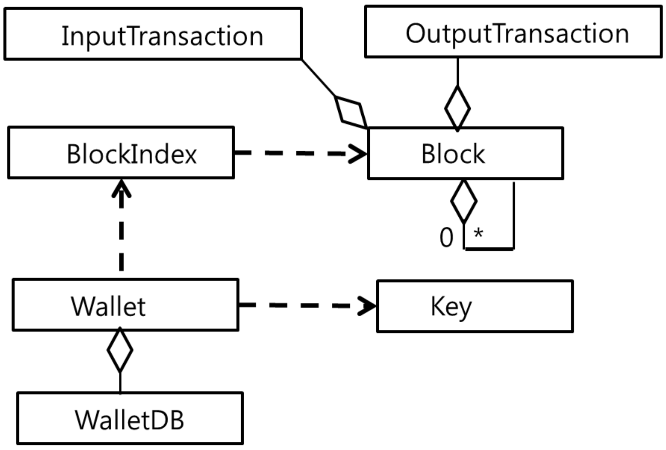


Figure 22. CBlock static model.

Accordingly, this study suggests seven verification methods that are more powerful in the first certification of the existing Blockchain technology.

5. Conclusions

Recently, Goldman Sachs announced a cost reduction case through Blockchain. It is estimated that Blockchain can be applied strongly in various areas of the smart grid. This proves that Blockchain technology can be sufficiently used in a smart grid and energy management exchange. It attempts to overcome the technical limits of blockchain.

In this paper, we design a smart grid based on the power trading system and Blockchain technology using Rainbowchain. (Figure 23).

It also maps and uses essential data based on smart grid data and Rainbowchain methodology.

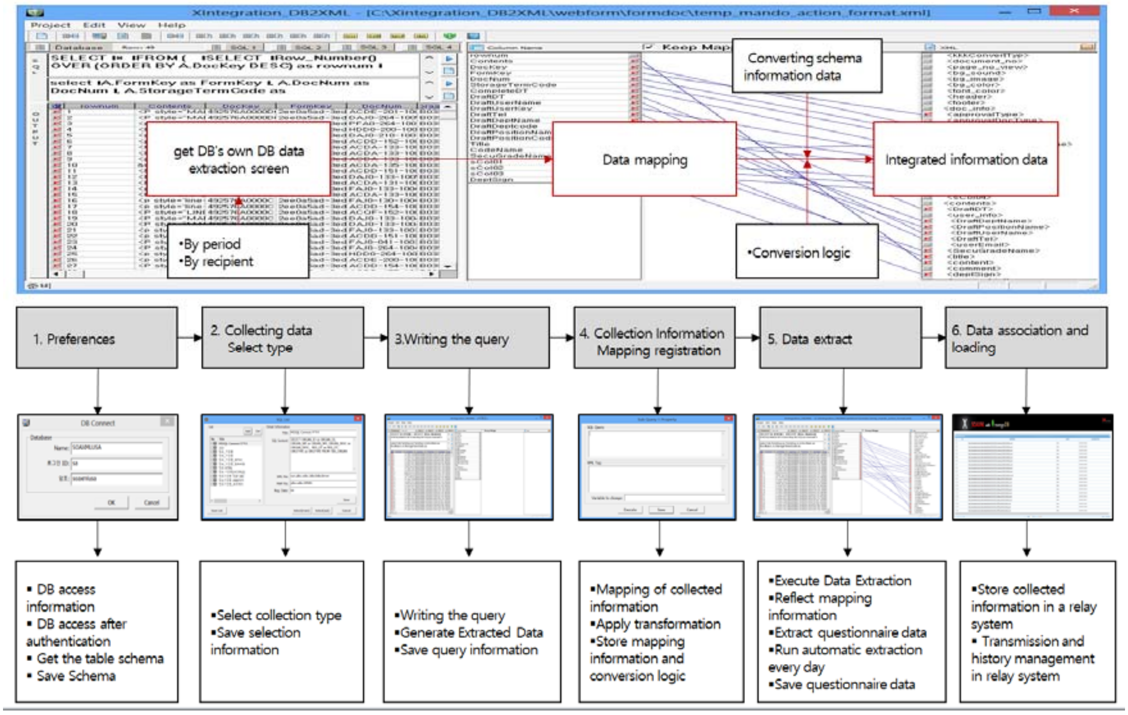

XIntegration_DB2XML
Converting schema information data
get DB's own DB data extraction screen
Data mapping
Integrated information data
•By period
•By recipient
•Conversion logic
1. Preferences
2. Collecting data Select type
3.Writing the query
4. Collection Information Mapping registration
5. Data extract
6. Data association and loading
▪ DB access information
▪ DB access after authentication
▪ Get the table schema
▪ Save Schema
▪Select collection type
▪Save selection information
▪Writing the query
▪Generate Extracted Data
▪Save query information
▪Mapping of collected information
▪Apply transformation
▪Store mapping information and conversion logic
▪Execute Data Extraction
▪Reflect mapping information
▪Extract questionnaire data
▪Run automatic extraction every day
▪Save questionnaire data
▪Store collected information in a relay system
▪ Transmission and history management in relay system

Figure 23. Rainbowchain data mapping method.

It provides an architecture for stable P2P transactions for intermediate smart contract functions to stably trade power data of an existing smart grid (Figure 24).

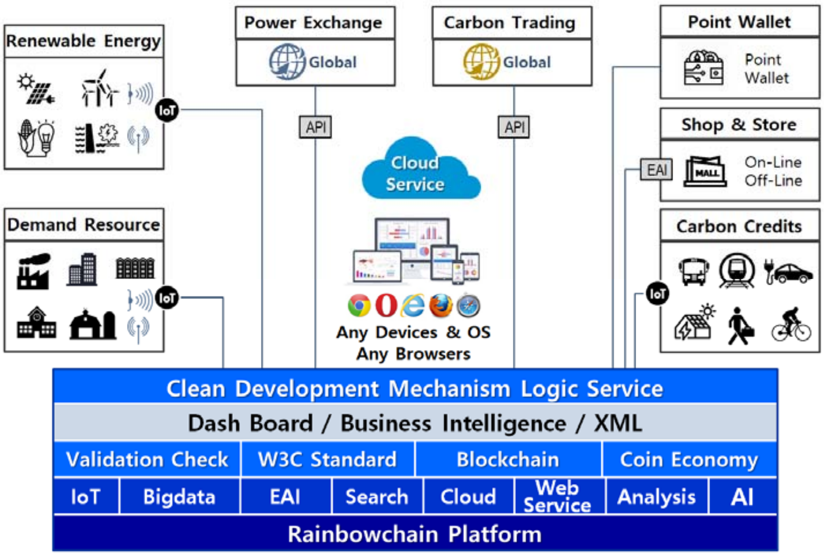


Figure 24. Rainbowchain platform.

We also present an empirical model that can be seen by individuals and companies through GUI (graphical user interface) screens and dashboards that are clearly used as user bases (Figure 25).

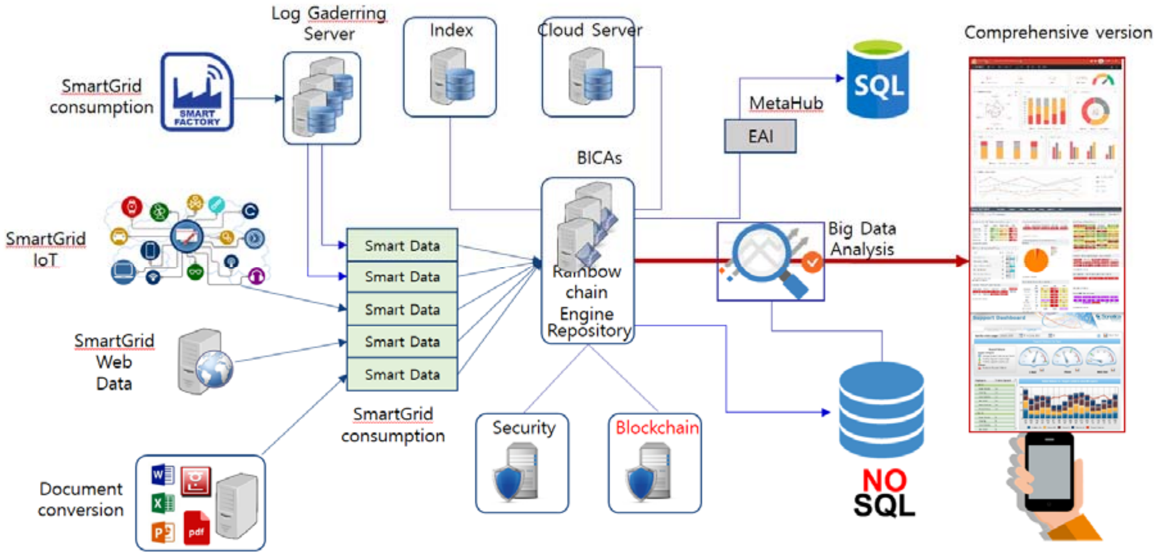


Figure 25. Rainbowchain architecture.

In this study, as a solution for security threats, which are a barrier to the expansion of the smart grid, this study proposes a smart grid Rainbowchain verification method using Blockchain that can be operated at a low cost and with more efficiency than the existing system. Also, it models Rainbowchain for test device verification, and it confirms the possibility of the application of Blockchain to the smart grid.

Blockchain has been studied continuously since its inception, and application cases appear in various areas. While more time may be necessary to expand Blockchain technology due to technical issues, such as a lack of related laws and regulations, due to the processing speed and storage capacity, it has a high operating efficiency over cost in a large system like the smart grid. Therefore, it is expected that the technical development of Blockchain would benefit the smart grid. Further studies on Blockchain protocol and a consent algorithm to apply Blockchain technologies to various areas of the smart grid are required. In particular, this study suggests Rainbowchain, an algorithm for international law and related certification with security issues.

Author Contributions: Conceptualization, S.-K.K.; Formal analysis, S.-K.K.; Funding acquisition, J.-H.H.; Investigation, S.-K.K.; Methodology, S.-K.K.; Project administration, J.-H.H.; Resources, J.-H.H.; Software, S.-K.K. and J.-H.H.; Supervision, J.-H.H.; Validation, J.-H.H.; Visualization, S.-K.K. and J.-H.H.; Original draft preparation, S.-K.K. and J.-H.H.; Review and editing of the manuscript, J.-H.H.

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

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

References

1. 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]
2. Chen, Y. Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Bus. Horiz.* **2018**, *61*, 567–575. [CrossRef]
3. Kshetri, N. Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]
4. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]

5. Savelyev, A. Copyright in the blockchain era: Promises and challenges. *Comput. Law Secur. Rev.* **2018**, *34*, 550–561. [CrossRef]
6. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038.
7. Levin, R.B.; Waltz, P.; LaCount, H. Chapter 9—Betting Blockchain Will Change Everything—SEC and CFTC Regulation of Blockchain Technology. Available online: https://www.sciencedirect.com/science/article/pii/B9780128122822000097 (accessed on 18 August 2017).
8. Prybila, C.; Schulte, S.; Hochreiner, C. Webe, I. Runtime verification for business processes utilizing the Bitcoin blockchain. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
9. 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]
10. Mansfield-Devine, S. Beyond Bitcoin: Using blockchain technology to provide assurance in the commercial world. *Comput. Fraud Secur.* **2017**, *2017*, 14–18. [CrossRef]
11. 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]
12. 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]
13. Wang, H.; He, D.; Ji, Y. Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
14. Löbbe, S.; Hackbarth, A. Chapter 15—The Transformation of the German Electricity Sector and the Emergence of New Business Models in Distributed Energy Systems. Available online: https://www.sciencedirect.com/science/article/pii/B9780128117583000152 (accessed on 19 May 2017).
15. Huh, J.-H. *Smart Grid Test Bed Using OPNET and Power Line Communication*; IGI Global: Hershey, PA, USA, 2017.
16. 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]
17. Livieratos, S.; Vogiatzaki, V.-E.; Cottis, P.G. A Generic Framework for the evaluation of the benefits expected from the smart grid. *Energies* **2013**, *6*, 988–1008. [CrossRef]
18. Park, L.; Jang, Y.; Bae, H.; Lee, J.; Park, C.Y.; Cho, S. Automated energy scheduling algorithms for residential demand response systems. *Energies* **2017**, *10*, 1326. [CrossRef]
19. Kessels, K.; Kraan, C.; Karg, L.; Maggiore, S.; Valkering, P.; Laes, E. Fostering residential demand response through dynamic pricing schemes: A behavioural review of smart grid pilots in Europe. *Sustainability* **2016**, *8*, 929. [CrossRef]
20. Hassan, N.U.; Pasha, M.A.; Yuen, C.; Huang, S.; Wang, X. Impact of scheduling flexibility on demand profile flatness and user inconvenience in residential smart grid system. *Energies* **2013**, *6*, 6608–6635. [CrossRef]
21. Boroojeni, K.G.; Amini, M.H.; Iyengar, S.S. *Smart Grids: Security and Privacy Issues*; Springer International Publishing: Cham, Switzerland, 2017.
22. 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 (PerCom Workshops), Kona, HI, USA, 13–17 March 2017.
23. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Commun. Surv. Tutor.* **2017**. [CrossRef]
24. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.; Sun, Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Intern. Things J.* **2017**. [CrossRef]
25. Huh, J.-H.; Seo, K. Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. *J. Supercomput.* **2018**, 1–17. [CrossRef]