Reliability Analysis of Iot Device with Block-Chain

Yo-Han Choi, Seung-hwan Ju, Hee-Suk Seo

Abstract**: *As sensor devices become diverse and prices fall, we develop diverse systems that use sensors. The integrity of the data used is critical to the value of these systems. A system using data generated at a sensor device must be able to obtain reliable data from the sensor device. They are design/develop general sensor devices for their purpose and their functions are limited. In order to overcome the limitation of performance of the sensor device, a collector node located in the local area and a Blockchain for ensuring the integrity are used. This is to increase the value of the system. When data of a sensor device located at a remote site is used, it is difficult to guarantee the integrity of the transmitted data. In this paper, we use a Blockchain as a method to store data and a collector node to manage the sensor device and to secure the integrity of data. It manages the data generated by the sensor node through the collector node and calculates the hash value to ensure the reliability of the data. Through the nodes constituting the block-chain, the node records the computed hash value in the block. When using data in the main system server, the integrity of the data can check using the hash value stored in the block-chain, and the reliability of the system can increase. This paper presents a method for securing data reliability by using a collector node and a Blockchain when generating in a sensor device However, the disadvantage of utilizing the data in the main system server according to the block generation rate is that it has a delay time. Future research will explore a Blockchain system suitable for sensor devices. Although this paper focuses on data generated in sensor devices, it can secure the reliability of objects by recording information such as digital documents and programs in a block-chain.***

Index Terms**: *Blockchain, Sensor Device, Data processing, Responsibility, Security.***

I. INTRODUCTION

Bitcoin is significant in that it is the first platform to exchange personal cryptography using block-chain technology, which is almost impossible to forge or modify in a distributed environment [1]. However, Bitcoin has a design with a focus on maintaining information related to each individual transaction, and there are limitations in developing various services using a Blockchain. To solve these limitations, a block-chain platform such as Ethereum, ripple, etc. has been developed [2]. In addition, various block-chain platforms such as Bitcoin and researches utilizing them have received attention. Along with the Blockchain, sensor devices and network technology have greatly improved. Industrial development has reduced the size and price of various sensors and controllers. With the advancement of network technology, various sensor devices connect to the network, and the user can monitor the status of the sensor device at a remote location. Using this environment, we can remotely control electronic devices and perform various IoT services such as smart home [3]. The data collected through the sensor device is very large and can cause fatal damage to the user when using the wrong data. It is possible to secure the confidentiality and reliability of data by encrypting the data transmitted by the sensor device, but it is difficult to perform such additional operation due to limitations of the H/W performance of the sensor device. Therefore, separate system is a need to process the data collected and generated by the sensor device. There is a need for a system that can detect data forgery or correction during data transmission. This paper proposes a method and data transfer structure for securing reliability of data transmitted from sensor devices using Raspberry Pi and block-chain.

II. MATERIALS AND METHODS

This paper proposes to use Blockchain as a method to guarantee the reliability of data generated and transmitted by IoT devices. It describes a typical block-chain platform and describes the features that store and process data on each platform. Describes Raspberry Pi, a microprocessor that performs the role of collecting data generated by sensor devices.

A. Block-Chain Platform Features and Data Storage Methods

The block chain is a platform for maintaining and managing transaction information. The block chain stores information sets of information such as sender and receiver information, transaction amount, and message in 'block'. A node is a system (object) that creates, stores, and utilizes blocks. Each block maintains a chain-like structure including information on the previous block (block hash value).

In the process of creating a block and propagating it to another node, another node (in another region) can create a new block before arriving at all nodes due to a network error or a geographical problem. If a branch occurs in the block list, the node adopts a block list with a longer block length. Each block refers to the hash value of the previously generated block, and the node must newly create all

Revised Manuscript Received on May 22, 2019.

Yo-Han Choi, ESS & Microgrid Engineering Team, Power System PU, Hyosung Heavy Industries Corp., Seoul, Republic of Korea

Seung-hwan Ju, Researcher, Electrical Standard Center, Korea Testing Laboratory, Ansan-si, Republic of Korea.

Hee-Suk Seo, Professor, School of Computer Science and Engineering, Koreatech, Cheonan-si, Republic of Korea.

blocks after the block whose information has been changed. Therefore, the node has a block of short length, and the node does not adopt the block list.

Blockchain provides compensation (coins used in blocks) to the nodes that create the new block. When a node generates a block, it gets an incentive. The node gets the incentive only if the list contains the block that it created. Therefore, the compensated node tries to connect the blocks generated by the block list. As a result, it is possible to prevent the malicious node from changing the information in the block in the middle of the block list and influencing the generated block later.

B. Bitcoin

Bitcoin is a cryptographic transaction system using the first block chain. Nakamoto Satoshi (pseudonym) first announced it in October 2008 [4]. In January 2019, it has attracted great attention by implementing the Bitcoin system himself.

The Bitcoin replaces the hash value by assigning a random value to the Nonce field in the block to create a new block. If the computed hash value is smaller than the difficulty goal set in the block, the block creation succeeds. This process is called mining. A successful miner obtains the transaction fee recorded in the corresponding block along with a fee for the production of a certain amount of blocks. The block chain uses the Difficulty target value as a role to control the generation rate of the new block. The smaller the value set for the difficulty target, the lower the probability of finding a hash value of a block smaller than the target value. Therefore, the system requires more computation, which increases the generation time of the block. The bitcoin is automatically adjusted so that the generation interval of the block is about 10 minutes.

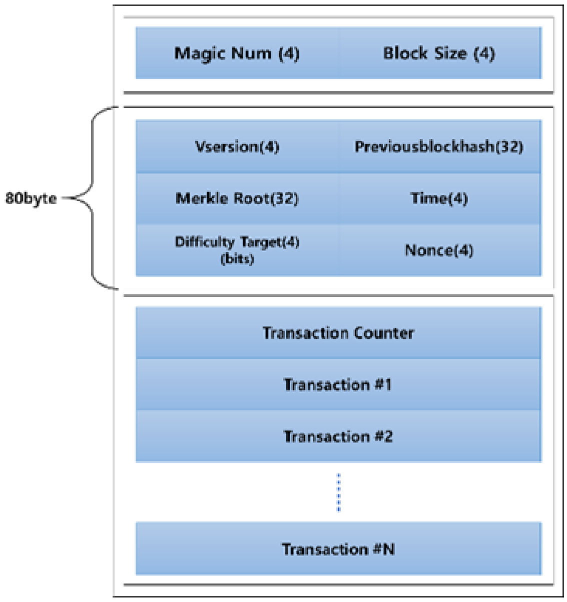
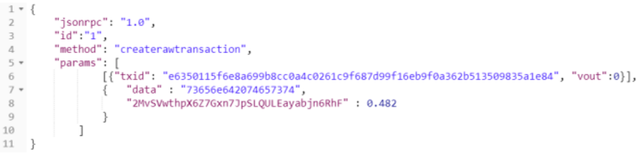


Figure 1. Bitcoin Block Structure

The block structure of the Bitcoin is shown in [Figure 1]. Version records the version of the block. Previous Block Hash records the hash value of the previous block so that the blocks form a 'chain' structure. Record a single-line summary of the transactions recorded in the Merkle Root block. Record the Unix time as a time when the miner tries to mince the block. Bits is the difficulty target value of the block. The miner repeats the process of finding the hash value of the block smaller than the bits while arbitrarily changing the value of the Nonce field. Bitcoin developed as a system for trading passwords over P2P networks. It is possible to conduct a direct transaction between a sender and a receiver without involvement of an intermediary. However, there is no way to record other information besides information for transaction (sender / recipient address, remittance amount, etc.), and limited function.

While many studies have verified the reliability of block chains, users wanted to record messages in addition to transaction information within Bitcoin blocks [5]. Users have used a method of recording a message in a block in such a way as to include the information of the message instead of the recipient address information in order to record the message.

Since then users have been asking for more requests and added OP_RETURN function to record messages from Bitcoin core 0.9.0 (current Bitcoin core version is 0.17.1) [6]. As shown in [Figure 2], the system can record a message in the Data parameter during the transaction. The message can record data at a maximum size of 80 bytes, but the size of the data that can stably maintain is 40 bytes.



```
{
    "jsonrpc": "1.0",
    "id":"1",
    "method": "createrawtransaction",
    "params": [
            [{"txid": "e6350115f6e8a699b8cc0a4c0261c9f687d99f16eb9f0a362b513509835a1e84", "vout":0}],
            {   "data" : "73656e642074657374",
                "2MvSVwthpX6Z7Gxn7JpSLQULEayabjn6RhF" : 0.482
            }
        ]
}
```

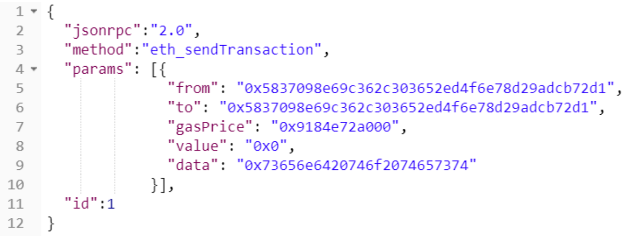
Figure 2. Bitcoin ‘createrawtransaction’ json message

C. Ethereum

Ethereum is a Blockchain platform proposed by Vitalik Buterin in 2013. Unlike the Bitcoin, which simply keeps transaction information, it is developed to include various information such as contract contents in the Blockchain. It provides a platform for creating web frameworks and extended distributed applications by implementing a programmable Blockchain [7]. Ethereum can program contracts through Smart contract. It has the advantage of automating transactions based on specific conditions using smart contracts. [8].

Ethereum supports smart contracts so that messages can delivered. However, a smart contract must execute to deliver or verify the message. User can use the data parameter to write the message directly into the block. The original purpose of the data parameter is to record the compiled smart contract code or hash value of the invoked method signature and encoded parameters. The message can encode in the encoding format defined in the data parameter and included in the block as shown in [Figure 3].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



```
{
  "jsonrpc":"2.0",
  "method":"eth_sendTransaction",
  "params": [{
              "from": "0x5837098e69c362c303652ed4f6e78d29adcb72d1",
              "to": "0x5837098e69c362c303652ed4f6e78d29adcb72d1",
              "gasPrice": "0x9184e72a000",
              "value": "0x0",
              "data": "0x73656e6420746f2074657374"
            }],
  "id":1
}
```

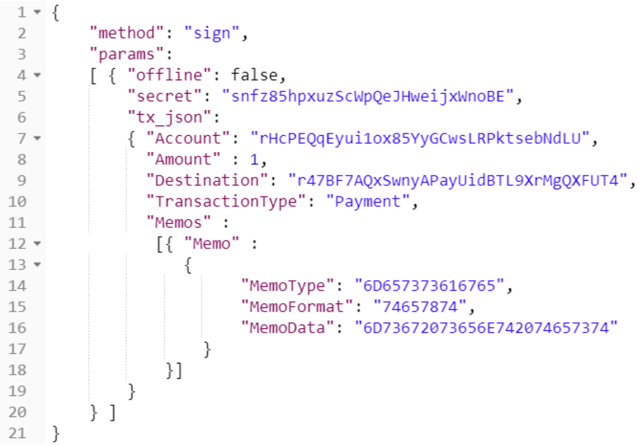
Figure 3. Ethereum 'eth_sendTransaction' json message

D. Ripple

Ripple is a Blockchain platform jointly developed by Chris Larsen and Jed McCaleb in 2013 and currently operated by RippleLabs. Ripple was developed for the purpose of replacing SWIF, an international remittance fund, unlike other Blockchain platforms whose main purpose is to trade coins in the block chain [9].

Ripple is a private Blockchain, and only nodes approved by RippleLabs can participate in the blockchain. Accordingly, it is not necessary to provide a negotiation process or a compensation scheme for blocking malicious users and securing the reliability of a Blockchain. When a node has created a new block, the verification nodes determine the contents of the block and decide whether to approve or not. If more than 80% of the verification nodes approve the block, the block is included in the block-chain. Verification nodes that have been thoroughly qualified can generate blocks and increase processing speed.

Since Ripple is developed to replace SWFT, various information related to the transaction can be included in the block. There is also a memos field for recording messages, and multiple memos can be recorded [9]. To record data in the memo, record type, format, and data separately as shown in [Figure 4].



```
{
     "method": "sign",
     "params":
     [ { "offline": false,
         "secret": "snfz85hpxuzScWpQeJHweijxWnoBE",
         "tx_json":
         { "Account": "rHcPEQqEyui1ox85YyGCwsLRPktsebNdLU",
           "Amount" : 1,
           "Destination": "r47BF7AQxSwnyAPayUidBTL9XrMgQXFUT4",
           "TransactionType": "Payment",
           "Memos" :
            [{ "Memo" :
                {
                      "MemoType": "6D657373616765",
                      "MemoFormat": "74657874",
                      "MemoData": "6D73672073656E742074657374"
                }
            }]
         }
     } ]
}
```

Figure 4. Ripple 'sign' json message

E. Features of the Blockchain platform

[Table 1] is a comparison of Bitcoin, Ethereum, and Ripple. Bitcoin is the first P2P trading system using Blockchain and has the longest service period. However, since the block generation period is long and the block size is limited to 1 MB, the transaction speed is very slow compared with other Blockchains. Since Bitcoin and ether use the negotiation algorithm of the work proof (POW) method (a method of generating a block and recognizing / approving a generated block), the last generated block can be replaced with another block. It takes time until the transaction recorded in the block is less likely to change. The Bitcoin is regarded as a confirmed transaction when six blocks are added after the block in which the transaction is recorded, and the Ripple is confirmed when 25 blocks are added. Therefore, the time required to approve the transaction is 1 hour for Bitcoin and 5 minutes for Ripple. Ripple, on the other hand, has defined nodes that can generate blocks. When the nodes generate a block, the transaction recorded in the block is determined as a transaction that confirmed immediately.

Table 1. Features of the Blockchain platform

	Bitcoin	Ethereum	Ripple
Features	First trading system using Blockchain	Smart contracts, DApp	Purpose of replacing SWIFT
Agreement algorithm	POW (Proof of Work)	POW -> POS (Proof of Work)	Ripple Transaction Protocol
The time period for generating the block	about 10 Min	about 12 Second	-
Transaction speed(Transaction Per Second)	7 TPS	25 TPS	1500 TPS
Payment time	about 1 Hour	about 5 Min	About 4 Second
Service validity time	9 Years	2Years	5Years

III. RASPBERRY PI

This paper simulates Blockchain technology in Raspberry Pi based. Raspberry Pi is a tiny, ultra-low-cost computer designed and developed as part of an educational project at the Raspberry Pi Foundation in the UK. The Raspberry Pi 3 Model B + supports 1.4GHz CPU and 1GB RAM, 2.4GHz and 5GHz wireless LAN and Gigabit Ethernet pods. It can run Linux OS, can use various accessories, and has high utilization. In addition, various sensors can be controlled via GPIO port [10]. The sensor device contains only minimal functions to accomplish its purpose. Therefore, it is difficult to process the data acquired from the sensor device itself and to transmit it to the outside. In this paper, we refer to Raspberry pi as Collector node and connect it with many sensor devices. The Collector node collects data generated from connected sensor devices for a certain period. It collects the data collected from the Collector node and removes the anomaly data.

In order to overcome the limitation of the HW performance of the sensor device, the information generated by the sensor device is firstly managed through the collector node.

IV. MATH RESULTS AND DISCUSSION

block-chain The time required to create a new block for each platform and the computing resources required are different. The public block chain cannot guarantee that the user will create a new block at a desired point in time. In addition, the size of data that the block-chain can include in the public block-chain is limited, and the cost of generating the block also increases when the size of the data increases.

This paper proposes a system structure as shown in [Figure 5] in order to efficiently and reliably transfer data collected through various sensors using a block-chain.

- The Main System Server is a system that collects and generates data from sensor nodes.
- block-chain node is a node that assures the reliability of data collected and generated through sensor node and collector node. It connect with other block-chain nodes and maintains block-chain by sharing generated block information.
- The Collector node manages the sensor nodes, collects data from the sensor nodes, and creates a DataSet of a certain size. Reducing the load that can occur when managing sensor nodes directly from the main system server.
- The sensor node collects basic data.

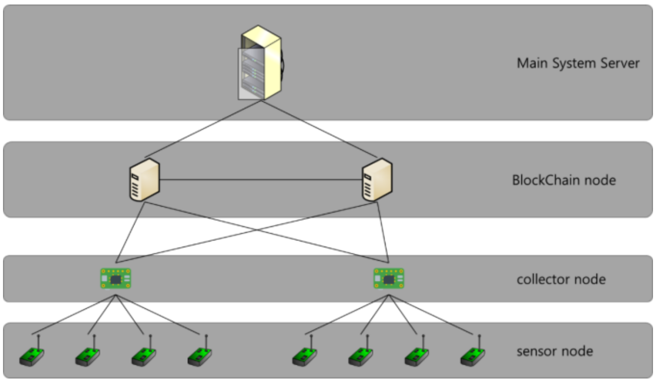


Figure 5. System Structure

[Figure 6] shows how the data collected and generated by the sensor nodes are transferred and utilized in the main system. When each sensor node acquires and generates data, it is delivered to the higher-level collector node. The collector node does not directly send data collected by the sensor node to the Main System Server, but creates a DataSet for the collected data for a certain period of time. After acquiring a DataSet over a period of time, calculate the hash value for the DataSet. Pass the computed hash value to block-chain node. block-chain node inserts the hash value received by the collector node into block and attempts to create the block. If the block containing the hash value is successfully generated, the corresponding block information is transmitted to the collector node. When the Collector node receives block information containing the hash value from block-chain node, it sends the collected data set to the main system server, the hash value of the data set, and the block information in which the hash value is recorded to the main system server.

When the main system server receives the relevant data information from the Collector node, it requests to check whether the hash value is included in the corresponding block. block-chain node checks whether block contains a hash value and returns the result to the main system server. When the main system server confirms that the hash value from block-chain node is included in the block, it determines that the corresponding DataSet is the data normally received from the sensor node and uses it as data of the service provided by the main system server.

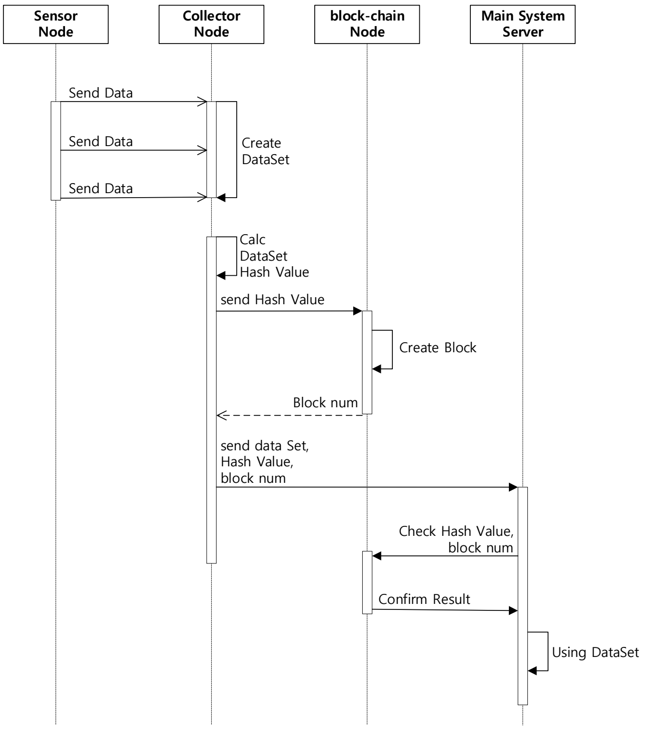


Figure 6. data flow sequence

V. CONCLUSION

In this paper, we study Blockchain such as Bitcoin, Ethereum, and Ripple, and describe how to write data to each Blockchain.

This paper proposes a method for securing the reliability of data generated by sensor nodes and collector nodes by using block-chains. The system structure and data flow using the proposed method are verified by the operation of the system. The proposed method collects data from the sensor node and generates a DataSet of a certain size. Thereafter, time is delayed until the data is used by the main system by registering the information in the corresponding data set in the block-chain and transferring the data to the main system server.

In this paper, we propose a method of securing reliability by using block-chain for data generated by sensor nodes and apply it to various data. In the future, we plan to extend this study to apply performance tests to large systems, and to minimize the time required to generate a DataSet.

ACKNOWLEDGMENT

This paper was supported by Education and Research promotion program in 2019

REFERENCES

1. Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review, 2016 june; 2.
2. John P Conley. Blockchain and the economics of crypto-tokens and initial coin offerings. Vanderbilt University Department of Economics Working Papers, 2017 June;VUECON-17-00008
3. Ali Dorri, Salil S Kanhere, Raja Jurdak, Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, 2017 Mar; DOI:10.1109/PERCOMW.2017.7917634
4. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008 Oct; Available from:https://bitcoin.org/bitcoin.pdf
5. Zikratov I, Kuzmin A, Akimenko V, Niculichev V, Yalansky L. Ensuring data integrity using blockchain technology. 2017 20th Conference of Open Innovations Association. 2017 Apr; DOI:10.23919/FRUCT.2017.8071359
6. Massimo Bartoletti, authorLivio Pompianu. An analysis of Bitcoin OP_RETURN metadata. International Conference on Financial Cryptography and Data Security. 2017 Nove;
7. Wood, Gavin. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. 2014 Available from:http://gavwood.com/paper.pdf
8. Nicola Atzei, Massimo Bartoletti, Tiziana Cimoli. A survey of attacks on Ethereum smart contracts (SoK). International Conference on Principles of Security and Trust. 2017 Mar;
9. Frederik ArmknechtGhassan O. KarameEmail authorAvikarsha MandalFranck YoussefErik Zenner. Ripple: Overview and outlook. International Conference on Trust and Trustworthy Computing. 2015 Aug;
10. Priyanka Roy, Pritam Roy, Abhijit Chakrabarti. Modified shuffled frog leaping algorithm with genetic algorithm crossover for solving economic load dispatch problem with valve-point effect. 2013 Nov;13(11). DOI:https://doi.org/10.1016/j.asoc.2013.07.006
11. Maksimović M, Vujović V, Davidović N, Milošević V, Perišić B. Raspberry Pi as Internet of things hardware: performances and constraints. IcETRAN 2014. 2014 Jun; 3(8)

AUTHORS PROFILE

Yo-Han Choi is a Ph.D. Candidate at the Interdisciplinary Program in Creative Engineering from Korea University of Technology and Education in 2019, Cheonan, Korea. He is now Assistant Manager of Hyosung Heavy Industries Corp. ESS & Microgrid Engineering Team

Seung-hwan Ju has a Ph.D. in Computer Engineering from Korea University of Technology and Education and currently works as a researcher at the Korea Testing Laboratory. He studies energy-IoT and information assurance.

Hee-Suk Seo is now a Professor in Department of Computer Science and Engineering, Korea University of Technology and Education, Korea.
His research interests include malicious code analysis, modeling & simulation, network security and intelligent system.