Blockchain Application in Internet of Things for Securing Transaction in Ethereum TestNet

by Endah Setyaningsih

Blockchain Application in Internet of Things for Securing Transaction in Ethereum TestNet

Joni Fat[1]*, Henry Candra[2]
[1]Department Electrical of Engineering, Faculty of Engineering UniversitasTarumanagara
[2]Department Electrical of Engineering, Faculty of Industrial and Technology, UniversitasTrisakti

* jonif@ft.untar.ac.id

Abstract. This system is designed by using Lolin D32 as the processor dan MPL3115A2 for the sensors. This system is designed to show that devices that based on Internet of Things (IoT) could be secured by using blockchain technology. The blockchain technology is based on Ethereum which will be tested in Ropsten Testnet network. Processor module connects to Internet through WiFi module which is one of the Lolin D32 features. This WiFi module connects to router which is used for designing and testing the system. This system wants to prove that the data which are acquired from sensor module MPL3115A2 (altitude, temperature and pressure) and positioning data could be sign and verify within the processor Lolin D32. Before sending the data, the data will be formatted. Data will be stored in smart contract. The smart contract is an Ethereum program which is written using Solidity language. This smart contract is delployed into Ropsten network. The numbers of testing that have been carried out are 516 times. These testings proved as success. The data which were sent to Ropsten network could be proved that they were recorded successfully. These are done by checking through etherscan.io.

1. Introduction

Microcontroller is the main part of Internet of Things (IoT) system, because all processes are started by microcontroller. Sensors and actuators are connected with the microcontroller. Microcontroller obtains and processes data from those devices and then dispatches the data to network which is connected to the microcontroller. The conclusion is that all the processes in IoT are started from microcontroller. Thus, securitization is the process of securing data in the microcontroller [1]. So, the aplication of blockchain in IoT in this design is about signing data in the microcontroller [2].

IoT as a new wave of Internet has a main problem in security. With the blockchain technology, this problem should be resolved. In this design, the focuses are:

1. Could a transaction signing be conducted in the microcontroller?
2. Could the transaction be processed in Ethereum Virtual Machine?
3. Could the transaction be verified?

This design uses Remote Procedure Call (RPC) from Infura. It also uses etherscan.io for checking whether a transaction is verified by a node in a blockchain network. The data which are acquired from sensor are height, temperature, pressure and position. As for the advantages from blockchain technology, there are disadvantages also. The disadvanteges are length of time that is needed to complete a transaction, a fee to process each transaction, and this technology is still in a development stage.

2. Method

2.1. Block Diagram

Client module is a microcontroller module which could do a signing process for a transaction to a node. For the sake of interaction to Ethereum Network, this process empowers RPC. The RPC that is used in this system is Infura. Infura will relay data from client module to Ethereum Network. This transaction data will be verified by Ethereum Virtual Machine (EVM). EVM will be located in TestNet of Ethereum Network, i.e. Ropsten. This verification result could be monitored through etherscan.io. Figure 1 shows the block diagram of this system.

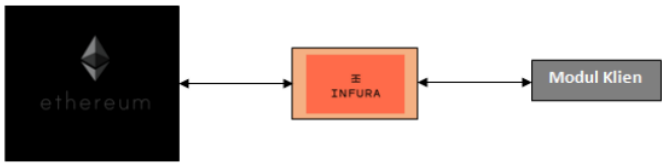

Figure 1. Block Diagram

2.2. System Architecture

Figure 2 shows the system architecture. This architecture consists of two parts, i.e. external and internal part. External part consists of infura.io and etherscan.io. Infura is used to connect IoT module (hardware) to EVM by using RPC. Etherscan.io is a website that is used to monitor the verification process by EVM. Internal part consists of IoT module and smart contract which is deploy in EVM.

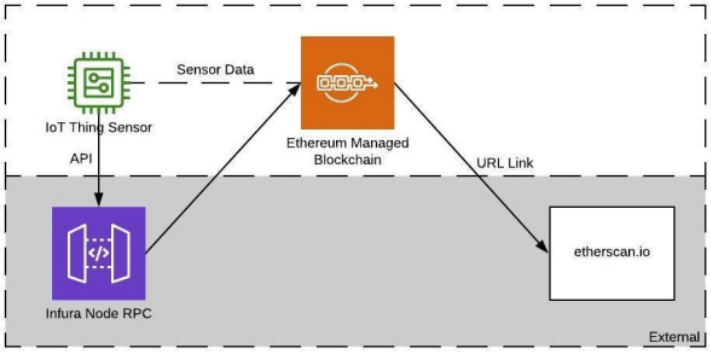

Figure 2. System Architecture

2.3. System Environment

Figure 3 shows the system environment. In this figure, client or system designer or user interacts by using etherscan.io to check the validation of a transaction. Client will input a transaction hash as an identification of a transaction or client could input smart contract address if the client want to verify all transactions. This is the only interaction between system and client.

As stated in Figure 1, the internal part in this system environment is called acquisition system. It consists of hardware and software. The hardware is microcontroller module which

uses Lolin D32. The software is a program which creates transactions. This system will relay a transaction to infura.io by using RPC with a link that is hardcoded.

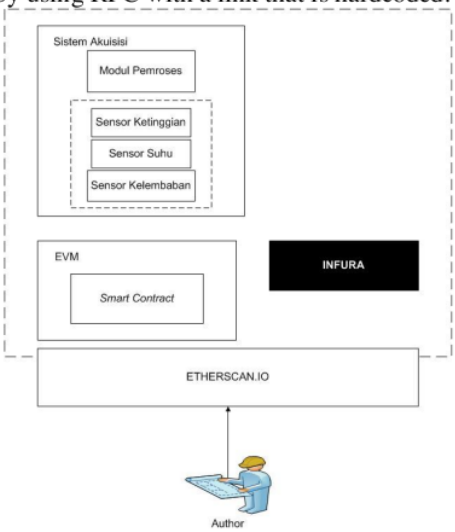

Figure 3. System Environment

2.4. Activity Diagram

Figure 4 shows activity diagram for this system. The process is started by client which initiates signing process. *Signer* subsystem will take over the process by conducting *Connecting*, *Initiating*, *Getting Information*, *Prepairing* and *Sending Transaction*.

After these processes are done, *Verifier* subsystem will be activated to verify the transaction. The result will be returned to the Client for checking. This will complete the whole cycle of the system.

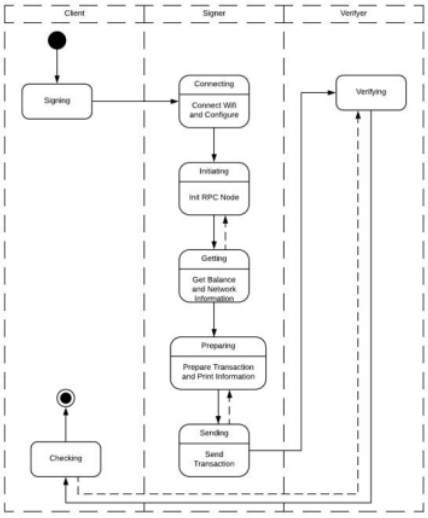

Figure 4. Activity Diagram

3. Results and discussion

Figure 5 shows the result of integration testing by using Zerinth console. Data which were used for testing are position (connected = 1), height (38.5625 m = 0x26), pressure (100 kPa = 0x64), and temperature (28.125°C = 0x1C). These data were formatted before sending to the network. After formatting, the data were 0x011C6426. The transaction hash for this testing is 0x85c012cc0c43a49331ea523a3d29deffe9c41de5d4ea604f28c5498fbfb4f47d. The result could be checked through etherscan.io. Wallet address which was used to process the transaction was 0x81b7e08f65bdf5648606c89998a9cc8164397647.

The testing result could be shown in Figure 6. From this figure, it could be concluded that the transaction was successfully processed to EVM. The data was completely secure according to blockchain method. From this figure, it was stated that the process needed 0,000000018000000017 ETH as a processing fee.

```
Begin of Sensor Initialization for modul MPL3115A2..

Sensor Initialized and Ready to Use...
Begin to Initiating Network Driver...
Driver initialized...
Connecting to WiFi...
WiFi Connected to  3Com
Asking ethereum...
Begin of Initiating of the RPC Node..
Initiating RPC Node Success..
Begin of Getting Information..
Getting of the Ethereum Ballance in Wallet..
Balance: 0x26e704247c3389c8  in Wallet Address  0x9Ad8Ee5E185455D6E7205bF63cE3808EDa44A2Ff
Success in Retrieving Ballance..
Getting off Gas Price to Process a Transaction..
Gas Price: 1000000000
Gas Price Acquired..
Getting of the Transaction Count or Nonce..
TCount: 516
Chain: 3
Success in Retrieving Transaction Count..
Getting Information is Done Successfully..
Altitude:  38.5625 meter  [ 0x26 ]
Pressure:  100 kPa  [ 0x64 ]
Temperature:  28.125 Celcius  [ 0x1C ]
Begin of Prepairing Transaction Object..
Setting wei..
WEI Price:  0
WEI Value Set..
Setting GAS Price..
GAS Set..
Setting Smart COntract Address..
Wallet Address for Transaction:  0x81b7e08f65bdf5648606c89998a9cc8164397647
Address Set..
Setting Up Data for Transaction..
Data to be sent: 0x011C6426
Data Set Up Done..
Setting Nonce..
Nonce  516
Nonce Set..
Object Prepairing Done..
Signing Completed...
Begin of Sending Value..
Sending values... [ 0x011C6426 ]
Sending Completed..
Monitor your transaction at:
https://ropsten.etherscan.io/tx/0x85c012cc0c43a49331ea523a3d29deffe9c41de5d4ea604f28c5498fbfb4f47d
Sent!
```

Figure 5. Testing Code

Transaction count or nonce was 516. This show that the testing was conducted for 516 times through the blockchain network. The testing was carried out in every 30 seconds. This length of time is also the length of time which is needed for completing one process cycle. So, in one day there should be 2.880 data which will be processed to the network.

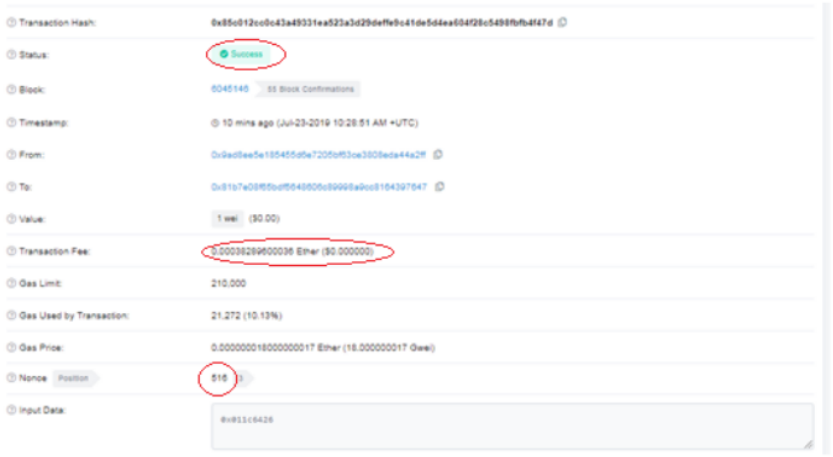

Figure 6. Verification in etherscan.io

4. Conclusion

This system design proves that data in IoT system could be securitized by using blockchain technology. The testings which have been conducted were 516 times (according to nonce field in etherscan.io). These proved that the data were successfully recorded to state variables.

5. References

[1] P. Danzi, et. al., *Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices*, IEEE International Conference on Communications (ICC), 2018.

[2] K. K. Patel and S. M. Patel, *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges*, IJSEC, vol. 6, no. 5, ISSN: 2321 3361, 2016, pp. 6122-6131.

[3] L. Atzori, A. Iera, and G. Morabito, *Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm*, Ad Hoc Networks, vol. 56, pp. 122-140, 2017.

[4] L. Srivastava and T. Kelly, *The internet of things*, International Telecommunication Union, Tech. Rep, vol. 7, 2005.

[5] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, *IoT Middleware: A Survey on Issues and Enabling Technologies*, IEEE Internet of Things Journal, vol. 4, pp. 1-20, 2017.

[6] R. C. Merkle, *A digital signature based on a conventional encryption function*, in Conference on the Theory and Application of Cryptographic Techniques. Springer, 1987, pp. 369–378.

[7] U. Guin, P. Cui and A. Skjellum, *Ensuring Proof-of-Authenticity of IoT Edge Devices using Blockchain Technology*, The 2018 IEEE International Conference on Blockchain, 2018.

Blockchain Application in Internet of Things for Securing Transaction in Ethereum TestNet

ORIGINALITY REPORT

13%	13%	13%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	"Preface", IOP Conference Series: Materials Science and Engineering, 2020 Publication	6%
2	eprints.uthm.edu.my Internet Source	4%
3	Matza Gusto Andika, Bambang Kismono Hadi, Rianto Adhy Sasongko. "A study on the response of high aspect ratio composite wing structures due to gust load", IOP Conference Series: Materials Science and Engineering, 2020 Publication	2%
4	www.coursehero.com Internet Source	1%
5	www.tandfonline.com Internet Source	1%
6	vdoc.pub Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		