EasyChair Preprint

№ 595

Demo Abstract: Blockchain enabled Internet-of-Things Service Platform for Industrial Domain

Chanhyung Lee, Nak-Myoung Sung, Lewis Nkenyereye and Jaeseung Song

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

October 29, 2018

Demo Abstract: Blockchain enabled Internet-of-Things Service Platform for Industrial Domain

ChangHyung Lee,[1] NakMyoung Sung,[2] Lewis Nkenyereye,[1] and JaeSeung Song[1]*

[1]Department of Computer and Information Security
Sejong University, Seoul, Republic of Korea
[2]Department of IoT Convergence
Korea Electronics Technology Institute, Sungnam, Republic of Korea
Email: wwoorim2@sju.ac.kr, nmsung@keti.re.kr, {nkenyele,jssong}@sejong.ac.kr

***Abstract*—The Internet of things is predicted to connect millions of devices. Therefore, standardized M2M technologies will play a crucial role in the next *massive connectivity*. A number of organizations also called Standards Development Organizations (SDO) are working towards a horizontal solution that would fit several vertical platforms; among them oneM2M. Blockchain technology is a new paradigm which has been applied in diverse applications such as crypto currency and smart contract. In this demo, we develop an API that enables blochchain in oneM2M platform. We use a blockchain system named Logchain that is suitable for IoT due to its consensus algorithm. The API enables the IoT users to either store their data in a conventional database or blockchain database.**

***Keywords*—oneM2M, IoT, BlockChain, Service Layer, Standards**

I. Introduction

Assume that we have a farmer noted as User A that decides to store the data of his production in an IoT platform. However there some data that are very sensitive such as the temperature of some goods which has just been delivered to the transportation agency. The extreme variation of the good's temperature could affect its state (quality of the good). A typical example could be the cheese, whose temperature's variation can affect its state. Therefore, the farmer decides to store the temperature data in a blockchain based database. This will ensure the integrity of the data and any modification will be traced and tracked [1] [2]. In process of the moving the good (cheese) from the farmer to the distributor (shop owner) through the the transporter, any attempt to change the data will fail and a warning message will be sent to all the peers. In this demonstration we mainly use two technologies namely Logchain and oneM2M. Logchain is a blockchain system developed by a team in Sogang University (South Korea). Logchain is suitable for IoT scenario because it uses blind voting as a consensus algorithm. We also consider oneM2M platform as an IoT platform. oneM2M is one of the leading SDOs for standardization. Fig. 1 describes the flow diagram between oneM2M and Logchain.

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.2017-0-00325, Block chain based IoT Reliability and Management System Development)

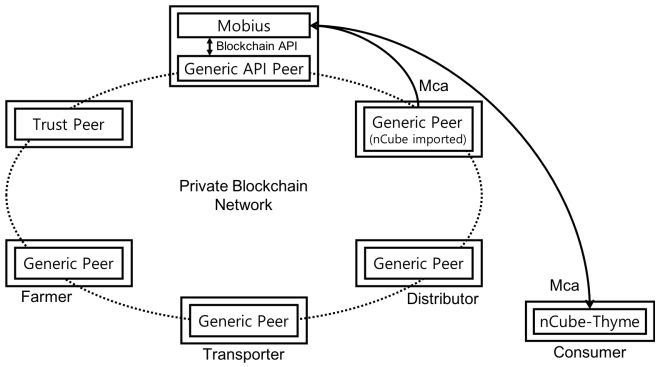

Fig. 1. oneM2M Logchain Flow Diagram.

II. Design and Implementation

This scenario consists of seven entities (peers) participating in the system. The details of the entities and their functions as shown in 1 are described as follows:

1) Each generic peer of the logchain connects to the trust peer of the logchain. Before this step, the trust peer should modify and manage the configuration file containing peer connection information. That is why logchain is considered as a *private blockchain*. Enabling blockchain to IoT platform ensures that only the authorized entity (peer) can retrieve the data in blockchain based database.
2) The application of the oneM2M ADN-AE registers to the IoT platform. After registration, the ADN-AE creates a `container(cnt)` resource that can be parent resource of `contentInstance(cin)` and `subscription(sub)` resources of oneM2M.
3) The application sends a request for creating a subscription resource to the IoT paltform. In the process of creating the API function, application set *BC* attribute to store the resource in the blockchain database. The `subscription` resource allows the resource creator to receive notification about created, updated and deleted resource placed in the same parent resource. Any modification from a malicious user can cause data leak, therefore the subscription resource's integrity is important to oneM2M/IoT service.

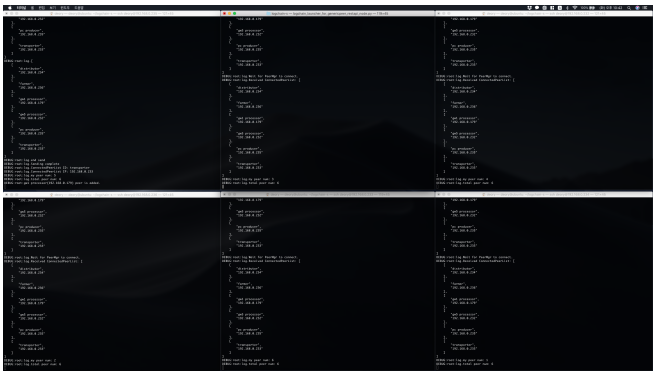

Fig. 2. All peers connection

Fig. 2 shows the screen shots of all the peers connected as private blockchain.

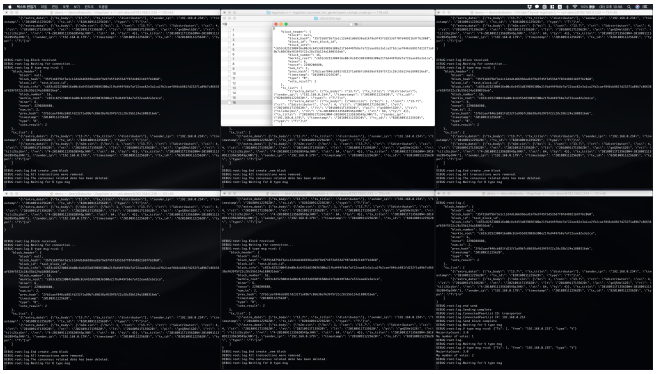

Fig. 3. Uploading sensor's data to the network.

After a successful connection of all the peers, a generic peer can upload the data in the private blockchain network. In our scenaio, the farmer upload the sensor data to the network. Then the generic peer (nCune imported) create a oneM2M resource and upload the data to the private blockchain as described in Fig. 3. On that stage, all the peers in the private network are aware of the new uploaded data. The oneM2M resource will send a request to Mobius platform to create oneM2M resource [add more details] as shown in Fig. 4

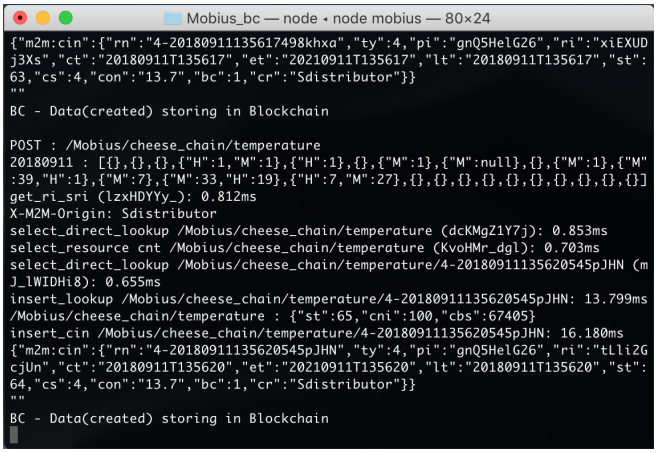

Fig. 4. Conversion to oneM2M resource

Assume that one the enttiy on the private blockchain network such as the transporter wishes to change the temperature data of the good provided by the farmer. For instance, the transporter might incur some refrigeration issues which could deteriorate the state of the good. In a normal database (which is not blockchain based), the transporter can modify the data and disclaim any responsibility. Fig. 5 shows that such attempt can not succeed. Fig. 5 is made by three figures, one on the left side and two on thr right side. The left side describe a new entry of data has been uploaded. The first temperature data was 21.7 Celsius degree and now a new entry of 13.7 Celcius degree is upload. As we mentioned earlier, the proposed API relies on a blockchain technology that uses blind voting as consensus algorithm. In this case the new uploaded data would can be saved and validated by all the peers. The second figure on the right side (in black) shows a warning message that notify that an attempt to modify the data has been done. The upper figure on the right side shows that the end user of the good (assume the consumer) will still get the unmodified data as uploaded on the private blockchain network.

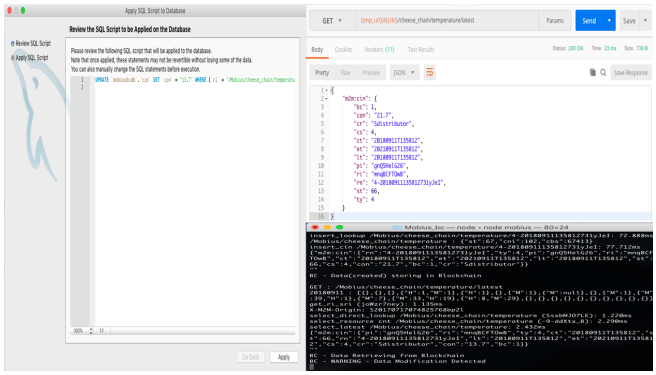

Fig. 5. Blockchain Validation

III. Industry Application and Conclusions

The proposed API can be applied in the following industries

- Supply-Chain Communications and Proof-of-Provenance: The integration of blockchain technology can proactively avail a digitally permanent and auditable records that ensures the stakeholders on the state of the product at each stage.
- Growing Online/Distance Education: The presented concept can be used to verify the students transcripts and educational records for online courses.

We showed in this demo paper the different steps involved in order to enable blockchain in oneM2M platform. We developed an API that allows a user to either store his data in a conventional database or blockchain database. We provide figures that show the API configuration, the upload of data in the private blockchain and unsuccessful attempt (attack) to modify data stored in the private blockchain. In the future work, the concept is intended to be tested within area industry environment.

REFERENCES

[1] X. Wu, B. Duan, Y. Yan, and Y. Zhong, "M2m blockchain: The case of demand side management of smart grid," in *Parallel and Distributed Systems (ICPADS), 2017 IEEE 23rd International Conference on*. IEEE, 2017, pp. 810–813.

[2] S. Yin, J. Bao, Y. Zhang, and X. Huang, "M2m security technology of cps based on blockchains," *Symmetry*, vol. 9, no. 9, p. 193, 2017.

TABLE I
CHARACTERISTIC OF USED DEVICES

Table Head	**Characteristic of used devices**		
	Running OS	***Operating system***	***Note***
PC A			
PC B			
PC C			
PC D	More details		

[a]Details are in the Appendix.

The details of the devices used in the experiment are found in Tab. I.