Review of Ethereum: Smart Home Case Study

Yu Nandar Aung
Faculty of ICT, Mahidol University
Bangkok,Thailand
yunandar.aun@student.mahidol.ac.th

Thitinan Tantidham
Faculty of ICT, Mahidol University
Bangkok, Thailand
thitinan.tan@mahidol.ac.th

***Abstract*—Nowadays, Internet of Things (IoT) plays a vital role in various domains, which are home, agricultural, healthcare, tourism, transportation and education. The more of its development, the more we need to consider about its security and privacy issues. In this paper, we consider smart home system (SHS) as a case study. SHS is an integration of home appliances together with sensors to get automatic operations of heating, lighting, air conditioning, home security, health care systems, etc. Moreover, SHS allows homeowner to monitor and perform appliances functions remotely at any instant time via the Internet. Due to the widespread availability and proliferation of the SHS, attackers can impersonate as a homeowner to steal important data (e.g., vital signs) for doing extortion and life threatening. Therefore, in this paper, we present an approach of private Blockchain implementation for SHS to cope of its privacy and security issues. We review Ethereum Blockchain packages for SHS according to its smart contract features for handling access control policy, data storage and data flow management.**

Keywords—blockchain; ethereum; internet of things; security; smart home

I. INTRODUCTION

According to the consecutive development of digital technology, Internet of Things (IoT) support numerous applications and services in various domains. Smart home system (SHS), one of IoT applications, consists of heterogeneous home appliances and sensors to get scheduling and automatic operations like lighting, ventilation, air-conditioning, health care, surveillance and security system. Moreover, homeowner can remotely monitor and perform appliance functions at any instant time via the Internet. Therefore, SHS makes the living standard of our lives to be more comfortable, convenient and safe.

Nowadays, there are various SHS applications in market such as Samsung Smart Things, Google Brillo/Weave, Apple HomeKit, Allseen Alljoyn and Amazon Alexa [6]. However, SHS have security risks. For example, an internet-connected door lock with a PIN, which can be programmed from home owner's smartphone, is convenient for user. But, a stranger can unlock the door by doing malicious activities. Attackers trick a victim into clicking on a link, with a phishing email purporting to come from Smart Things support. The crafted URL link would take the victim to the actual Smart Things websites. When the victim clicks the link, they may force the victim to add or change new four digits PIN for system backup or update.

Moreover, the attacker would have to convince their victim to download a malware disguised application to simply monitor the battery charge of various devices. After installing this malware application, the attacker can remotely control the victim's SHS (turn of the smoke detector or steal PIN code of door lock). Distributed Denial of Service (DDoS) attack is another kind of cyber-attacks that the hacker temporarily enslaves internet-enabled devices into an arrangement. For example, Mirai is the most predominant DDoS-IoT-botnet malware as it infected 4,000 active IoT devices like CCTV cameras, DVRs, home routers [10, 15].

Following the never-ending string of disclosures about major data breaches, home users are wary of placing much personal data in public and private clouds with good reason. Therefore, in this paper, we propose a decentralized approach of data management (Blockchain technology) to cope SHS security and privacy issues [14]. Blockchain is a list of records or blocks, which are linked and secured. The first Blockchain is introduced with Bitcoin by using the technological underpinnings of cryptocurrencies proposed by Satoshi Nakamoto [11] for a payment system to transfer digital currency without any central authority. Blockchain has been used to provide security and privacy in peer-to-peer networks and can be applied in different applications such as academic, healthcare, and Internet of Things (IoT).

The rest of our paper is organized as follows. Section II explains some related IoT system that uses Blockchain technology. Section III presents our proposed system architecture. Section IV mentions details about Blockchain technology and challenges that we need to solve for Ethereum implementation in SHS. Finally, conclusions and future work are given in Section V.

II. BLOCKCHAIN CONCEPT

Formally, people used a ledger to maintain their data systematically. Especially they used these for maintaining financial transaction records by their respective balance account types. These ledgers were maintained centrally by authorized parties which are bank or government as a trusted party. According to the successive wave of digital technology, these physical ledgers are changing to digital ledgers but still maintained centrally by authorized parties. Therefore, these centralized systems are becoming an attractive point of adversaries' parties as they are single point of failure. Conventional security protecting ways may leak according to

978-1-5386-1431-0/17/$31.00 ©2017 IEEE

professional hackers. Therefore, a new technology, Blockchain, is emerging to prevent this security leak.

Blockchain used the idea of ledger to maintain every financial transaction within a member of their network. To prevent single point of failure, Blockchain distributes identical ledgers to every member of its network. By this way, every member can see what is now happening and if some suspicious things happen at a ledger in one node, other nodes will know immediately.

A. Decentralization

Decentralization is one of the Blockchain features. Otherwise, it distributes all of its Blockchain data to every node of their network. This is the reason why it does not require a central authority. Because of its decentralized features, it can prevent from single point of failure. Moreover, it is immutable to attack because the attacker has to attack every single node inside of Blockchain network [8].

B. Block

As mentioned above, Blockchain is a structure of data systematically based on timestamp. Each block contains the block's header and body. The first block of the Blockchain is called genesis which has no parent block. In particular, the block header includes block version, Merkle tree root hash, timestamp, nBits, Nonce and Parent block hash. The body of block is composed of transaction counters and transactions. The maximum number of transactions in one block depend on the block size and the size of each transaction. Moreover, Blockchain uses an asymmetric cryptography mechanism to validate the authentication of data transactions [5]. Digital signature based on asymmetric cryptography is used in untrustworthy environment [8].

C. Consensus Algorithm

The challenge of Blockchain is how to ensure that the data distributed to every node of the Blockchain network is identical [3]. Therefore, Blockchain needs consensus algorithms to agree on one consistent state of Blockchain transaction, as the Blockchain has many copies residing on each node of network. There are several common consensus approaches in Blockchain. These are Proof-of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated Proof-of-Stake (DPoS), Ripple and Tendermint.

PoW is a consensus strategy used in the Bitcion network [10]. The consensus means that nodes of Blockchain network have to calculate hash value of the previous block. When one node can solve, it has been selected to append a new Block with a bundle of transactions. Nodes that calculate the hash values are called miners and the PoW procedure is called mining in Bitcoin [17]. In PoW, the miners need high processing power to calculate these hash values and it consumes computing resources. Therefore, in order to save the resource space, other consensus algorithms are considered. However, PoW is vulnerable to attack as any intruders can be miners.

PoS is a resource saving approach to PoW. Mining process in PoS is to prove the ownership of the cryptocurrency balance. However, the selection of miners based on the amount of balance is not fair and it persuades attackers to create a fake balance. Peercoin's PoS system can be selected as a miner based on its own coin age which can be derived from older and larger sets of coins. Therefore, the mining resource is nearly zero.

Another consensus algorithm is PBFT, a replication algorithm to tolerate byzantine faults [1]. It has been utilized as a consensus algorithm for Hyperledger Fabric Blockchain application [4].

The next one is DPoS. The difference of DPoS from of PoS is that only the predefined nodes can validate the block. Therefore, the mining process of DPoS is faster if compared to PoW.

Ripple is another consensus algorithm. In this algorithm, nodes are divided into two types: server for participating consensus process and client for only transferring transactions. Each server has a Unique Node List (UNL). To append new block into the Blockchain, the server has to query the nodes in UNL and if it receives an agreement to 80%, then the transaction will be packed into the Blockchain.

D. Digital Signature

Every user, members of Blockchain network, owns a pair of private key and public key. The private key is used to sign digital transaction and therefore should be kept in confidentiality. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, Alice wants to send another user Bob a message.

- In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data.
- In the verification phase, Bob validates the value with Alice's public key.

In that way, Bob can easily check if the data has been tampered or not. The typical digital signature algorithm used in Blockchains is the elliptic curve digital signature algorithm (ECDSA) [2].

E. Public Blockchain

Public Blockchain means that anyone can join to the network. Moreover, everyone can participate in the mining process. Therefore, the approach of using consensus is important in order to eliminate malicious participants.

F. Consortium Blockchain

Consortium Blockchain means that only a predefined member of network can do mining process [13].

G. Private Blockchain

Private Blockchain means that only a specific owner can handle Blockchain network. Therefore, private Blockchain

does not need to use mining process. To prevent unauthorized users for appending the new block, smart contract features are applied by defining access policies.

III. Ethereum Blockchain

A. Ethereum

Basically, Ethereum is a "World Computer" as a platform gives users to run distributed applications in a decentralized manner. This means that applications running on Ethereum are available everywhere and every time [8, 9].

B. Ethereum Blockchain Accounts

Ethereum Blockchain has two types of accounts: externally owned account and contract account to specify an authorized person of SHS. During the installation, externally owned account has been automatically created as a default. Contract account can be set up with the policies for handling transactions.

C. Smart Contract on Ethereum

A smart contract is a legal agreement between parties for doing operations. It can be developed by using Turing complete language such as Solidity [9].

IV. Proposed System Architecture

According to Seyoung, et al. [12], IoT devices were manipulated by Ethereum Blockchain platform with smart contracts for tracking meter and setting policies to control on and off air conditioner and light bulbs in order to save energy. Moreover, Dorri, et al. [7] proposed a combination of private and public Blockchain. Their approach composed of three tiers: smart home systems (SHS), overlay network and cloud storage. Private Blockchain was employed to handle data flow in SHS, whereas public Blockchain was to manage data flow over cloud storage. As shown Figure 1, the architecture of our proposed system consisting of smart home miner (SH miner), private Blockchain and local storage connects to SH sensor and actuator devices. SH miner handles a private Blockchain. The function of the private Blockchain is to store policies for data flow or transaction management.

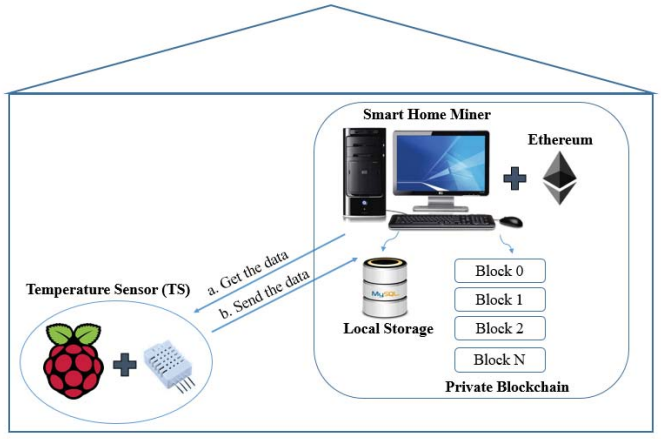

Fig. 1. Proposed System Architecture

A. SH Miner

SH miner, a computer, is to maintain private Blockchain. The private Blockchain contains policies set up by home owner. Furthermore, the private Blockchain saves all transactions flowing through SHS. Several accounts have been created to access this private Blockchain as each home may have more than one owner with different levels of authorization.

B. Transactions Handling

Private Blockchain is used to handle data flow based on the smart contract or authorized policies which are set up by home owner. As shown in Figure 2, *store transaction* will happen when sensors want to save their data inside of local storage. *Access transaction* will occur when actuators want to get some sensing data to do some actions. *Monitor transaction* will happen when home owner wants to know the current situation of their home.

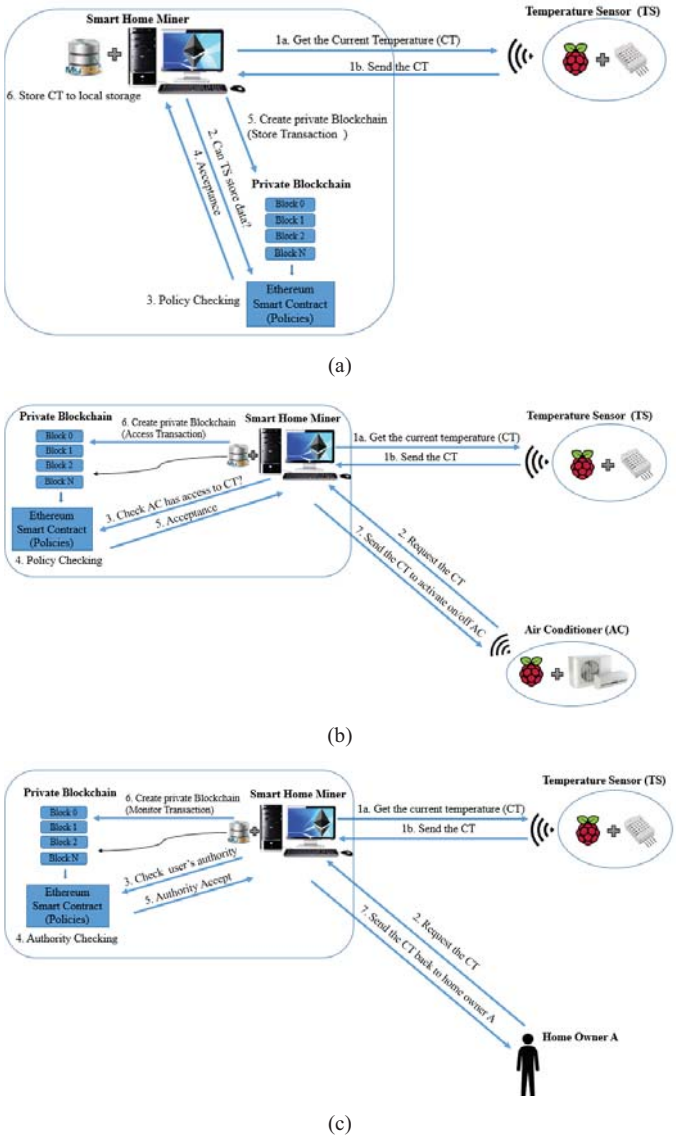

Fig. 2. SH Miner with Ethereum Private Blockchain Example (a) Store Transaction, (b) Access Transaction, (c) Monitor Transaction

C. Smart Contract (Policy)

The private Blockchain is organized into three kinds of transactions: store, access and monitor. Before handling these transactions, the private Blockchain needs to check the policy that is set up by the home owner. The followings are example policies of our proposed system.

- Only the sensors inside of this SHS can store their data inside of their corresponding smart home miner.
- Only the actuators inside of the SHS can request sensor data from their SH miner.
- Only the home owner can monitor the data inside of local storage of SH miner.
- Only the home owner can change and modify smart contract of private Blockchain.

D. Hardware Requirement

At our proposed system, smart contract is used to maintain data transactions and mining is not required. Therefore, this proposed system does not need to use high processing power computer.

E. Challenges of Ethereum Implementation on SHS

The transaction time of Ethereum Blockchain is around 20 seconds [16] and it is not fast enough for some conditions that require immediately responses. Therefore, it may be difficult for time-sensitive conditions.

V. Conclusions and Future Work

In this paper, we proposed the idea of how to apply Ethereum private Blockchain for SHS. By using the Ethereum private Blockchain, home owner can check every transaction history that has already done inside of their SHS. Moreover, we can set up the policies for handling transactions to define only the authorized person for accessing and monitoring data. Our future work, we will setup and evaluate this proposed idea on a real test bed environment.

Acknowledgment

This research paper was partially supported by the Faculty of Information and Communication Technology, Mahidol University.

References

[1] C. Miguel and L. Barbara, “Practical byzantine fault tolerance,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, pp. 173–186, 1999.

[2] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ecdsa),” International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[3] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170, 2005.

[4] “Hyperledger project,” 2015. [Online]. Available: https://www.hyperledger.org/

[5] NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

[6] E. Fernandes, “Security Risks in the Age of Smart Homes”, 2016 [Online] Available: http://scitechconnect.elsevier.com/security-risks-age-smart-homes/

[7] A. Dorri, S. S. Kanhere and R. Jurdak, "Towards an Optimized BlockChain for IoT," *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Pittsburgh, PA, pp. 173-178, 2017.

[8] C. Dannen, “Introducing Ethereum and Solidtty: Foundations of Cryptocurrency and Blockchain Programming for Beginner”, Brooklyn, New York, USA, ISBN-13 (electronic), 2017.

[9] D. Patel, J. Bothra and V. Patel, "Blockchain exhumed," *2017 ISEA Asia Security and Privacy (ISEASP)*, Surat, 2017, pp. 1-12, 2017.

[10] M. Lyu, D. Sherrat, A. Sivanathan, H. H. Gharakheili, A. Radford, V. Sivaraman. “Quantifying the reflective DDoS attack capability of household IoT devices”, Proceeding of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Netwroks, 2017.

[11] S. Nakamoto, Bitcoin: Peer-to-Peer Electronic Cash System, 2008.

[12] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, pp. 464-467, 2017.

[13] T. Swanson. “Consensus-as-a-serive: a brief report on the emergence of permissioned, distributed ledger system”, 2015.

[14] U. Saxena, J. S. Sodhi and Y. Singh, "Analysis of security attacks in a smart home networks," *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, Noida, pp. 431-436, 2017.

[15] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1-1, 2017.

[16] Y. Heinze, “How long do Ethereum transaction take?” 2017. [Online] Available: https://support.metalpay.com/hc/en-us/articles/115000373814-How-long-do-Ethereum-transactions-take-

[17] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, pp. 557-564, 2017.