Managing IoT Devices using Blockchain Platform

Seyoung Huh*, Sangrae Cho*, Soohyung Kim*

*ETRI, Daejeon, South Korea

one@etri.re.kr, sangrae@etri.re.kr, lifewsky@etri.re.kr

Abstract — **Since the start of Bitcoin in 2008[1], blockchain technology emerged as the next revolutionary technology. Though blockchain started off as a core technology of Bitcoin, its use cases are expanding to many other areas including finances, Internet of Things (IoT), security and such[2]. Currently, many private and public sectors are diving into the technology[3]. Aside from that, as software and hardware improve, we would see the beginning of IoT. And those IoT devices need to communicate and synchronize with each other. But in situations where more than thousands or tens of thousands of IoT devices connected, we expect that using current model of server-client may have some limitations and issues while in synchronization. So, we propose using blockchain to build IoT system. Using blockchain, we can control and configure IoT devices. We manage keys using RSA public key cryptosystems where public keys are stored in Ethereum and private keys are saved on individual devices. Specifically, we choose Ethereum as our blockchain platform because using its smart contract, we can write our own Turing-complete code to run on top of Ethereum. Thus, we can easily manage configuration of IoT devices and build key management system. Even though we can simply use account as a key management system, which most of blockchain platform supports, we decide to use Ethereum because we can manage the system in a more fine-grained way. For the proof of a concept, we use a few IoT devices instead of a full system of IoT system, which consists of thousands of IoT devices. But in our later study, we would like to build a fully scaled IoT system using blockchain.**

Keywords— Blockchain, IoT, Ethereum, Key Management, Information & Network Security, Authentication, Smart Contract

Seyoung Huh is a researcher of Authentication Research Team in ETRI, South Korea. His research interests include blockchain, authentication, cryptography, and any security-related fields.

Sangrae Cho is a senior researcher of Authentication Research Team in ETRI, South Korea. He graduated from Imperial College London in 1996 obtained BEng Computing degree and studied MSc in Information Security in Royal Holloway, University of London in 1997. He started his career as a researcher in LG Corporate Technology Institute in 1997 and has worked in ETRI for over 15 years as a security researcher. During that time, he has actively involved in constructing national PKI infrastructure project until 2001. From 2004, he has done several projects relating to Digital Identity Management including SAML v2.0 and Authentication technology based on FIDO (Fast Identity Online) specifications.