ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 19-02-25

j.inst.Korean.electr.electron.eng.Vol.23,No.2,508~516,June 2019
http://dx.doi.org/10.7471/ikeee.2019.23.2.508

블록체인 DPoS 합의 알고리즘을 활용한 IoT 장치 관리 시스템 개발

Development of IoT Device Management System Using Blockchain DPoS Consensus Algorithm

김 미 희*★, 김 영 민*

Mihui Kim*★, Youngmin Kim*

Abstract

Smart home with various IoT devices provides convenient and efficient services. However, security is important because sensitive information such as private video and audio can be collected and processed, as well as shared over the Internet. To manage such smart home IoT devices, we use blockchain technology that provides data integrity and secure management. In this paper, we utilize a PoS(Proof of Stake) method that verifies the block through the accumulated stake in the network rather than the computation power, out of the PoW(Proof of Work) block chain, in which the computation for the existing verification must be continuously performed. Among them, we propose a blockchain based system with DPoS(Delegated Proof of Stake) method to actively solve the scalability part, for security that is suitable for smart home IoT environment. We implement the proposed system with DPoS based EOSIO to show realization, and we show performance improvement in terms of transaction processing speed.

요 약

다양한 IoT 기기로 구성된 스마트 홈에서는 편리하고 효율적인 서비스를 제공한다. 그러나 사적인 영상과 음성과 같은 민감한 정보까지 수집 및 처리될 뿐 아니라 인터넷을 통해 공유될 수 있어서 보안이 중요하다. 이러한 스마트 홈 IoT 장치 관리를 위하여 데이터 무결성 및 안전성을 제공하기 위해 블록체인 기술을 활용하고자 한다. 본 논문에서는 기존 검증을 위한 연산을 지속적으로 수행해야 하는 PoW(작업 증명) 블록체인에서 아닌 네트워크에 축적된 지분을 통해 블록을 검증하는 PoS(지분 증명), 그 중에서 확장성 부분을 해결하고자 하는 DPoS(위임 지분 증명) 방식으로 스마트 홈 IoT 환경에 적절한 보안용 블록체인 체계를 제안한다. DPoS 체계인 EOSIO 기반으로 제안시스템을 구현하여 실현가능성을 보이고, 성능평가를 통해 트랜잭션 처리 속도 측면의 성능 향상을 보이고자 한다.

Key words : IoT device management, Blockchain, Integrity, DPoS consensus, System development

* Dept. of Computer Science & Eng., Computer System Institute, Hankyong National University
★ Corresponding author
E-mail : mhkim@hknu.ac.kr, Tel : +82-31-670-5167
※ This work was supported by a research grant from Hankyong National University in the year of 2019.
Manuscript received Jun. 7, 2019; revised Jun. 19, 2019; accepted Jun. 19, 2019.

Ⅰ. 서론

IoT(Internet of Things)기반 스마트 홈에는 가정 내부 감시를 위한 카메라, 원격 제어가 가능한 도어락 등 다수의 IoT 장치들이 통신으로 연결되어 자동화 서비스와 편의성을 제공한다. 이러한 스마트 홈 IoT에는 내부의 센서들이 감지한 온도나 조명 장치의 동작 여부 등의 정보부터 홈CCTV의 영상이나 음성과 같은 민감한 개인정보까지 다양한 정보를 수집, 처리, 저장할 뿐 만 아니라 인터넷을

통해 공유될 수 있다. 따라서 홈 IoT 장치와 저장된 해당 정보에 허가받지 않은 외부 사용자가 접근할 수 없어야 한다. 이를 위해 인증 또는 접근 제어를 위한 여러 가지 보안 기법이 적용되고 있다[1]. 각 장치들은 각자의 보안 기법으로 접근 제어를 수행하는데 이는 IoT 장치의 인증 정보 관리와 장치 간 연동 및 자동화가 어려워질 수 있다.

블록체인은 제 3의 신뢰 기관(Trusted Third Party) 없이 분산 원장과 네트워크의 참여자(노드) 간 합의로 트랜잭션을 검증하고 블록을 생성하여 데이터의 무결성을 제공한다[2]. 블록체인 기술은 높은 보안성을 제공하고 모든 기록이 공개적으로 접근 가능하다. 해당 기술은 암호 화폐인 비트코인에 적용되어 주목받기 시작하였으나, 금융 이외의 분야(예, 유통, 물류, 관리 등)에서도 블록체인을 활용한 시도가 확대되고 있다. IoT 장치관리를 위해서도 블록체인을 활용한 연구가 진행되었다. [3]의 논문에서는 각기 다른 IoT 장치의 사용자 인증 방법 다양화로 인한 연동 문제를 해결하기 위해 블록체인을 활용하여 여러 IoT 네트워크에서의 사용자 인증을 통일하는 기법을 제안했다. 또한 관리의 경량화를 위해 두 계층의 블록체인으로 나누어 구성한 후 실제 데이터는 비공개 체인에 저장하고 검증할 해시값은 공개 체인에서 비교 검증하는 체계를 가지고 있다. 그러나 이는 원본 데이터가 손실, 변조가 생기면 복원할 수 없는 문제가 있다. [4]에서는 홈 IoT 관리를 위해서 PoW(Proof of Work, 작업 증명) 합의 알고리즘 기반 스마트 컨트랙트가 동작하는 네트워크를 제안하였다. 하나의 메인 네트워크와 각 가정마다 만든 비공개 네트워크를 기반으로 홈 IoT의 권한 관리와 위협 탐지를 구현하였다. PoW 합의 알고리즘에서는 블록에 담긴 트랜잭션의 무결성 검증을 위해 지속적인 컴퓨팅 파워를 제공해야 하며 동시에 트랜잭션 처리속도에 영향을 주게 되는 문제가 있다.

본 논문에서는 스마트 홈 IoT 장치 관리를 위해 기존 인증 메커니즘의 다양화로 인한 연동 문제를 해결하기 위해 블록체인 기술을 적용한다. 블록체인 기술을 활용한 IoT 장치 관리에 대한 기존 연구에서 블록 검증 절차로 인해 많은 연산력이 요구되는 문제와 데이터 무결성 확인 문제를 개선한 단일 블록체인 네트워크를 제안한다. 제안하는 구조는 연산력이 아닌 네트워크에 축적된 지분을 통해 블록을 검증하는 PoS(Proof of Stake, 지분 증명) 방식, 그 중에서 확장성 부분을 적극적으로 해결하고자 하는 DPoS(Delegated PoS, 위임 지분 증명) 방식으로 IoT 환경에 적절한 보안용 블록체인 체계이다.

2장에서는 IoT 기반 스마트 홈 구조와 블록체인에 대해 설명하고, 3장에서는 제안 시스템의 구조 및 처리 흐름을 설명한다. 4장에서는 EOSIO 플랫폼[5]을 활용하여 제안 시스템을 구축하고, 5장에서 실험을 통해 제안 시스템의 성능을 분석한다. 6장에서 결론을 맺는다.

II. 기반 연구

1. IoT 기반 스마트 홈

IoT 기반 스마트 홈은 조명 및 난방 장치 등을 원격으로 제어 및 모니터링하고, 정의된 패턴을 통해 해당 장치들의 작동을 자동화하는 체계이다[6]. 스마트 홈은 크게 내부 환경과 외부 환경으로 나눈다. 내부 환경에서는 댁내에서 백색가전 및 센서들로 구성된 IoT 장치 네트워크들과 사용자로부터 명령을 받거나 상태정보를 모니터링 할 수 있도록 사용자인터페이스가 제공되고, 이들은 홈 게이트웨이를 통해 연결되어 있다. 외부 환경에서는 내부 환경의 스마트 홈을 인터넷을 통해 서비스제공자와 컨텐츠 제공자를 연결해 주어 스마트 홈에서 발생한 데이터의 분석이나 응용서비스를 제공한다. 즉 홈 게이트웨이는 스마트홈 내의 장치들을 하나의 네트워크로 연결하고 외부 환경과의 연결을 통해 서비스 제공자, 사용자, 스마트 홈을 연결한다.

기존 홈 네트워크에서는 IoT 장비들이 클라이언트로서 저장장치를 포함한 서버(혹은 홈 게이트웨이)의 제어를 받으며, 서버는 저장장치의 데이터베이스에 접근 제어, 요청 자료 목록, 기록 등을 저장 관리한다[7]. 그러나 이러한 구조는 중앙관리의 약점인 해커가 서버의 권한을 탈취할 경우 자료와 기록 등의 내용이 조작될 수 있을 뿐만 아니라 홈 네트워크의 제어권을 탈취 당할 수 있어 더욱 큰 위험에 노출될 수 있다.

이러한 취약점을 보완하고자 안전하게 데이터를 관리하고, 처리의 연산력을 외부 소스를 활용하기 위해 클라우드 네트워크를 이용한 스마트 홈 구조가 제안되었다[8]. 그러나 이러한 구조에서도 클라

우드 서버가 노출되는 경우 데이터의 안전성을 보장할 수 없다. 본 논문에서는 블록체인 기술을 통해 IoT 기기 관리의 안전성을 제공하고 블록체인의 블록을 생성하는데 많은 연산력이 요구되지 않는 합의 알고리즘을 사용하고자 한다.

2. 블록체인과 합의 알고리즘

블록체인 기술은 2008년 사토시 나카모토가 제안한 비트코인이라는 가상화폐로부터 시작된다. 이는 가상화폐의 발행 및 자금 중개 기능을 제공하고 제3의 신뢰 기관 없이 사용자 간 거래의 신뢰성을 제공하는 메커니즘이다. 이 때 블록 생성에 사용한 합의 알고리즘은 PoW이다[9]. PoW를 통해 블록에 거래내역을 정리해 주고, 그 보상으로 코인과 거래 수수료를 지급받는 것이 채굴(Mining) 프로세스이다. 비트코인에서 채굴은 네트워크에 참여한 각 노드가 경쟁적으로 SHA-256 해시 연산을 하여 난이도를 만족하는 nonce값을 찾는 과정이다. 이 nonce값을 먼저 찾은 노드가 자신의 서명과 nonce를 담은 블록을 생성하고 보상을 받게 된다. nonce를 찾는 과정은 규칙이 없으므로 무작위 대입으로 진행한다.

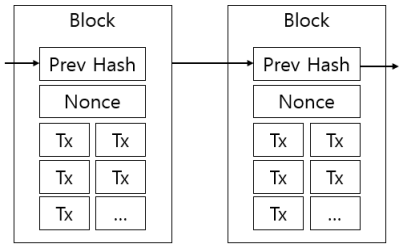

Fig. 1. Block structure of Bitcoin.
그림 1. 비트코인의 블록 구조

그림 1은 이러한 비트코인의 블록 구조를 도식화하고 있다. 블록은 트랜잭션(Tx)들을 담고 있고 이전 블록의 해시값을 가지고 체인으로 연결되며 해당 블록이 정당함을 증명하는 nonce를 담는다. 증명된 블록은 자료의 무결성을 제공하기 위해 분산하여 소유한다. PoW의 단점으로는 네트워크에 참여한 노드가 지속적으로 nonce를 찾기 위해 연산을 해야 하므로 연산력의 낭비가 발생하며 한 노드가 네트워크에서 51% 이상의 연산 비율을 확보하면 데이터를 조작할 수 있어 소규모 네트워크에 적합하지 않다. 비트코인의 전자화폐 거래 서비스는 금융 거래를 유일한 목적으로 두고 있지만 이더리움 등 다른 블록체인 네트워크는 스마트 컨트랙트(Smart Contract) 실행을 위해 트랜잭션에 데이터를 포함할 수 있다[10]. 스마트 컨트랙트란 어느 조건이 만족되면 수행해야할 코드를 거래에 추가한 것이다. 스마트 컨트랙트가 동작하는 블록체인 네트워크에서는 트랜잭션 처리 속도가 높을수록 사용자가 느끼는 실행 속도가 빨라질 것이다.

PoS 합의 알고리즘은 PoW 기반 네트워크에서 합의를 위해 소비되는 연산력을 트랜잭션 처리에 사용하도록 한 합의 알고리즘이다. 네트워크상의 지분으로 블록을 증명하는 PoS가 등장하였다. PoS는 채굴 작업으로 인해 발생하는 해시 파워 낭비와 연산력 저하 문제를 해결하기 위해 블록 생성을 네트워크상의 지분을 기준으로 결정한다. 그러나 참여자 간 지분에 따라 블록을 검증함으로써 악성 사용자의 방해로 분기가 해결되지 않거나 트랜잭션이 조작될 수 있다[11]. DPoS는 모든 노드가 블록을 검증해서 발생하는 확장성 문제와 악의적 사용자의 블록 생성 참여로 인한 문제를 해결하기 위해 블록 생성을 검증하는 절차를 일부 노드에게 위임한다. EOSIO를 통해 개발되어 운영되는 EOS의 경우 투표를 통해 블록을 생산하는 노드, BP(Block Producer)를 결정한다[12]. 가장 많은 투표 지분을 확보한 노드가 BP로 결정되며 그 결과로 분산성은 다소 낮아지지만 가용성과 확장성을 확보하였다. 표 1에서는 이러한 합의 알고리즘을 비교하였다.

Table 1. Comparison of consensus algorithms.
표 1. 합의 알고리즘의 비교

Factors	PoW	PoS	DPoS
Consensus Pivot	Hash rate	Stake	Stake + Vote
Scalability	Low	Low	High
Tx Speed	Low	High	High

PoW 기반 네트워크에서 블록 생성 절차로 인해 트랜잭션 속도가 느려지는 것은 PoW 기반 블록체인의 공개 네트워크의 트랜잭션 속도를 보면 알 수 있다[13]. PoS 기반 합의 알고리즘은 트랜잭션 속도가 빠르지만 많은 지분을 가진 노드의 악성 행위를 막기 어렵다. PoS의 블록 생성 방식을 모든 노드가 아닌 대표를 선출하고 대표 노드 간 합의를 통해 블록을 생성하는 DPoS 기반으로 IoT 보안을

관리한다면 악성 행위를 하는 노드를 저지함과 동시에 처리 속도에 영향이 적고 트랜잭션의 기록이 영구적으로 남는 점을 활용할 수 있을 것이다.

비잔틴 문제 허용(BFT, Byzantine Fault Tolerance)이란 합의 알고리즘이 동작할 때 올바른 노드가 2/3 이상 합의에 성공하면 악의적 혹은 사고로 인해 합의에 실패한 노드를 무시하고 블록을 생성하더라도 블록에는 문제가 없음을 뜻한다[14]. 이를 응용하면 일부 노드가 지속적으로 악의적 행동을 함이 파악되더라도 블록의 무결성에 영향 없이 해당 악성 노드로부터 블록을 생성할 권리를 박탈해서 네트워크의 영향력을 줄일 수 있다.

스마트 홈 IoT 네트워크에서는 많은 센서와 장치로부터 요청과 데이터가 발생한다. 이는 네트워크에서 다량의 트랜잭션을 처리할 필요가 있어야 함을 보인다. 네트워크에서 생성된 데이터와 그 데이터 또는 장치에 대한 접근권한 등의 설정 정보 변조를 막기 위해서 본 논문에서는 블록체인 기술을 활용하고자 한다. 이를 통해 데이터의 무결성과 가용성을 모두 확보한 체계를 구축한다.

III. 제안 시스템

본 장에서는 DPoS 합의 알고리즘을 이용하여 다양한 IoT 기기들을 안전하고 낮은 오버헤드의 블록체인 기반 관리 시스템을 제안한다.

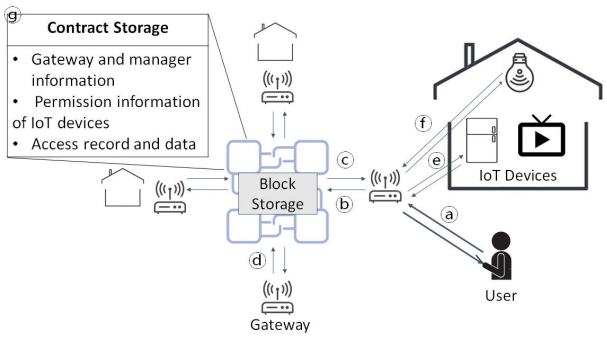

Fig. 2. Proposed system structure.
그림 2. 제안 시스템 구조도

그림 2는 본 논문에서 제안하는 시스템의 구조를 도식화한 것이고, ⓐ~ⓖ는 엔터티 간 정보 또는 처리 프로세스를 나타내고 있다.

ⓐ 사용자 등록, 제어 등의 트랜잭션 전달
ⓑ 트랜잭션에서 요청한 블록 데이터 검색
ⓒ 요청에 따라 검색된 블록 데이터 전달
ⓓ 처리한 데이터를 블록에 저장
ⓔ 게이트웨이가 트랜잭션에서 요청한 장치에게 요청 전달
ⓕ 블록에 접근하기 위한 요청
ⓖ 블록체인 저장소에 저장되는 정보

본 논문에서 제안하는 시스템은 블록체인 네트워크와 스마트 컨트랙트, 게이트웨이, 사용자, IoT 장치로 구성된다. 게이트웨이는 사용자와 IoT 장치로부터 전송받은 데이터를 블록체인 네트워크로 전송한다. 게이트웨이는 블록 데이터를 저장할 저장소를 포함한다. 블록체인 네트워크상의 게이트웨이 계정에 스마트 컨트랙트를 배치하면 ABI(Application Binary Interface)를 호출하여 스마트 컨트랙트에 포함된 기능을 실행할 수 있다. 게이트웨이는 ABI를 실행하기 위한 API(Application Programming Interface) 엔드포인트를 제공하여 IoT 장치나 사용자에게 블록에 접근할 수 있도록 한다. IoT 장치는 게이트웨이를 통해 블록체인 네트워크에 자신이 처리할 데이터 요청이 존재하는지 감시한다. 데이터 요청이 정당한 사용자에 의해 발생한 경우, 요청받은 데이터를 게이트웨이를 통해 블록체인 네트워크에 전송한다. 사용자는 사용자 어플리케이션을 사용해 미리 지정된 게이트웨이를 통해 블록체인 네트워크에 접근한다.

그림 3은 본 논문에서 제안하는 시스템에서 스마트 컨트랙트의 구조를 도식화한 것이다. 스마트 컨트랙트는 사용자 관리 모듈, 장치 관리 모듈, 데이터 처리 모듈로 구성된다. 사용자 관리 모듈(User Management Module)은 네트워크 소유자 정보와 접근이 허용된 사용자 정보를 포함한다. 네트워크 소유자(Network Owner)는 게이트웨이를 블록체인 네트워크에 등록하여 컨트랙트를 배치한 사용자이다. 접근이 허용된 사용자 목록(Permitted User List)은 네트워크 소유자가 데이터에 접근할 수 있도록 허가한 사용자를 목록이다. 장치 관리 모듈(Device Management Module)은 장치 목록을 포함하며, 장치의 등록과 삭제를 수행한다. 장치 목록(Device List)은 해당 네트워크에 속한 장치의 목록이다. 데이터 처리 모듈(Data Processing Module)은 요청된 트랜잭션 필드와 데이터 요청 기능을 가지고 있다. 요청받은 트랜잭션 리스트(Requested

Tx)는 내부 장치에게 요청한 트랜잭션을 기록하고 이후에 블록에 있는 트랜잭션을 수집하여 기록 테이블을 구성하는데 사용한다.

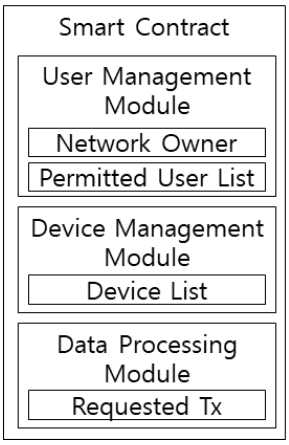

Fig. 3. Contract structure.
그림 3. 컨트랙트 구조

사용자 관리 모듈에 포함된 메소드는 사용자 등록과 삭제 메소드이다.

- **사용자 등록:** 네트워크 소유자가 수행할 수 있고, 데이터를 요청할 수 있는 사용자를 등록하는 메소드
- **사용자 삭제:** 네트워크 소유자가 수행할 수 있고, 데이터 요청 권한을 가진 기 등록 사용자의 삭제

장치 관리 모듈에 포함된 메소드는 장치 등록, 장치 삭제 메소드이다.

- **장치 등록:** 네트워크에 참여하여 권한 관리를 받을 수 있도록 IoT 장치를 등록하는 메소드
- **장치 삭제:** 권한 관리를 받지 않도록 기 등록된 IoT 장치를 삭제하는 메소드

데이터 처리 모듈의 메소드는 다음과 같다.

- **데이터 요청 및 처리:** 사용자가 네트워크에 어떤 IoT 장치의 데이터를 요청하면, 우선 어떤 사용자가 어떤 장치의 데이터를 요청했는지 기록한다. 이후에 해당 사용자가 접근이 허용된 사용자인지 여부를 접근이 허가된 사용자 목록에서 확인한다. 허가된 사용자일 경우 요청이 정당함을 표시한다. 접근이 허가된 사용자 목록에서 사용자를 확인하지 못하거나 IoT 장치가 존재하지 않는다면 정당하지 못한 요청임을 표시한다. 블록체인을 활용한 시스템의 특성 상 기록을 남기려고 하고자 하는 트랜잭션은 하나의 튜플로 기록한다. 모든 작업이 트랜잭션으로 블록에 기록되므로 해당 기록을 추적하여 테이블을 재구성할 수 있다. 그러므로 제안하는 체계에서는 블록체인의 특징인 삭제 불가 특성을 활용해서 누군가가 침투하더라도 DBMS(Database Management System)와 다르게 침투한 흔적을 지울 수 없다.

Ⅳ. 제안 시스템 구현

제안하는 시스템 프레임워크는 DPoS 기반의 블록체인 플랫폼을 기반으로 한다. 그 중 대중적인 DPoS 체계인 EOS를 개발하는데 사용한 EOSIO를 통해 구현한다.

EOSIO는 네 가지 컴포넌트로 이루어져 있다.

- **nodeos:** EOSIO의 블록 생성과 API의 엔드포인트 부분인 핵심 데몬이다.
- **cleos :** 지갑을 관리하거나 블록체인과 상호작용하는 명령어 인터페이스이다.
- **keosd :** EOSIO의 지갑 속 키를 안전하게 보관하는 부분이다.
- **EOSIO.cdt :** EOSIO의 컴파일러인 eosio-cpp를 가지고 있다. C++로 작성된 코드를 웹어셈블리(wasm) 파일로 컴파일 하고 ABI 파일을 생성한다.

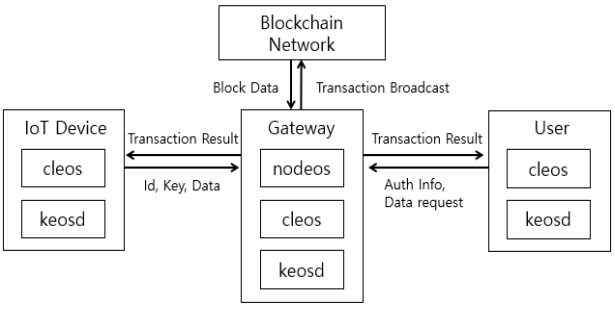

Fig. 4. Development diagram based on EOSIO.
그림 4. EOSIO로 구현 구성도

그림 4는 이러한 EOSIO 컴포넌트로 구성한 IoT 장치 관리를 위한 시스템 구성도이다.

- **계정(지갑) :** cleos가 keosd를 통해 계정과 키를 생성한다. 계정에는 이름을 지정할 수 있다. 계정을 생성하면서 잠금 해제에 필요한 키가

하나 발생한다. 권한 관련한 키로 소유권 RSA 키 한 쌍, 활동 RSA키 한 쌍이 필요하다. 이후 추가적으로 keosd를 통해 비공개 키를 추가할 수 있다.

- **키 :** 소유권 키는 계정의 소유권에 관한 키, 활동키는 계정의 활동에 관한 키, 그리고 공개와 비공개 키 한 쌍이 있다.
- **스마트 컨트랙트:** EOSIO.cdt는 C++ 기반으로 작성된 코드를 ABI와 wasm(웹 어셈블리) 파일을 만들고 블록체인에 배포해서 컨트랙트 wasm 파일은 계정에 발행하여 동작한다.
- **ABI :** JSON과 Binary 간 변환 방법에 대한 JSON 명세이고 이를 통해 컨트랙트의 데이터 교환 규칙을 기술하고 있다.

사용자는 네트워크에서 게이트웨이를 소유하고 그 게이트웨이의 설정 권한을 가진다. 사용자는 이용의 편의를 위해 실제 장치의 블록체인 상 지갑 주소나 ID가 아닌 별칭을 통해 원래 주소나 ID로 매핑할 수 있는 테이블을 가진다.

게이트웨이는 블록 데이터를 직접 내려 받아 저장하고 트랜잭션을 요청하는 블록체인의 엔드포인트이다. 같은 네트워크상의 센서 장치들에게 블록 정보를 제공하거나 서명된 트랜잭션을 블록에 전송한다. 게이트웨이는 RestAPI를 통해 블록정보를 제공하거나 트랜잭션의 입력을 받는다.

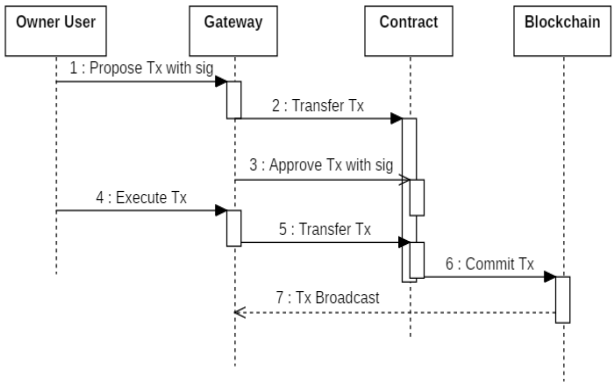

Fig. 5. Mutisig sequence diagram.
그림 5. 다중서명 시퀀스 다이어그램

그림 5는 다중서명을 위한 시퀀스 다이어그램이다. 게이트웨이와 사용자의 서명을 동시에 요구하는 다중서명(Multisig) 트랜잭션을 네트워크에 올려서 게이트웨이가 사용자 소유임을 증명하는 블록을 네트워크에 올린다. 이를 통해 사용자는 게이트웨이로 구성된 네트워크의 권한 정보를 수정할 수 있는 권한을 가진다. IoT 장치는 블록체인에서 사용할 수 있는 계정을 가진다. 장치는 대용량 저장장치를 가지기 어려우므로 블록체인에 직접 참여한 게이트웨이를 통해 블록에 접근하거나 트랜잭션을 작성한다.

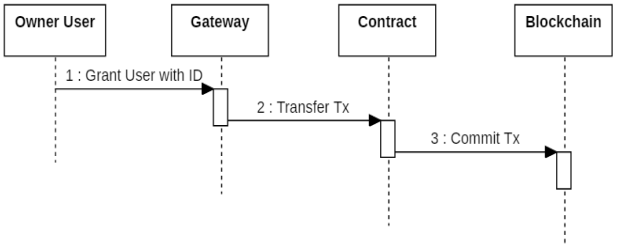

Fig. 6. Sequence diagram of permission setting.
그림 6. 권한 설정의 시퀀스 다이어그램

그림 6은 권한 설정을 위한 시퀀스 다이어그램이다. 게이트웨이를 소유하고 있는 사용자는 네트워크에 등록된 IoT 장치에 접근할 수 있는 사용자를 지정할 수 있다. IoT 장치에게 자료를 요청할 때 설정된 권한을 통해서 요청의 정당성을 판단한다.

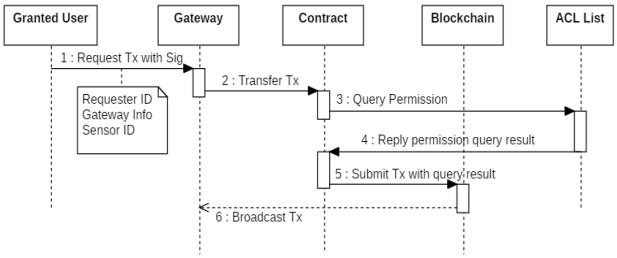

Fig. 7. Sequence diagram of data request.
그림 7. 자료 요청의 시퀀스 다이어그램

그림 7은 자료 요청의 시퀀스 다이어그램이다. 자료를 요청하기 위해서는 요청자 ID, 게이트웨이 정보(지갑 주소), 센서 ID 총 세 가지 정보가 필요하다. 요청자는 자신의 비공개 키로 트랜잭션을 서명하여 자신이 요청함을 증명해야 하며 이후 권한 테이블과 비교를 통해 요청의 정당성 여부를 트랜잭션에 기록한다.

이러한 프레임워크를 구현함으로써 트랜잭션을 분산 네트워크인 블록체인에 저장하여, 투명하고 영구적이며 추적 가능한 관리 프레임워크를 만들 수 있다.

Ⅴ. 성능 평가

본 논문의 성능 평가를 위해 [15]에서 구축한 센서 네트워크에서의 프로세싱 이벤트를 활용하였다. 해당 네트워크는 온도, 습도, 조도 등의 환경 변수를 수집하기 위해 만들어졌다. 센서 장치들의 트랜잭션 발생 주기 등을 토대로 네트워크에서 처리해야 할 트랜잭션 수를 이용하고자 한다. 자료 요청 트랜잭션을 반복적으로 네트워크에 전송하여 승인된 트랜잭션의 수를 확인하고, 트랜잭션 수 당 블록 사이즈를 측정하였다. 또한 PoW와 비교하여 트랜잭션 처리속도를 측정하였다. 실험에서 사용된 기본 게이트웨이 사양은 표 2와 같다. 트랜잭션 수는 [15]에서 제시한 센서들의 전송 주기가 겹칠 경우 보낼 수 있는 트랜잭션의 최대 개수에 근사하여 350개로 진행한다.

Table 2. Gateway specification.
표 2. 게이트웨이 사양

Part	Specification
CPU	i7-7700HQ
RAM	DDR4 2400MHz 1/4GB
Storage	500GB SATA3 SSD

{"id":"fed344dbc79668c1708955b09ac6e41f4eb1b3574f8ad474470cb7ffd2cbfaa3","trx":{"receipt":{"status":"executed","cpu_usage_us":404,"net_usage_words":15,"trx":[1,{"signatures":["SIG_K1_Ke7d48UFBRrcNS6CuT6Bh899K6XSzWxyYheS3tB9eu3eKXv18hD7KKrpg5avZ2h5Z1M3bWWj8kuCX8pSGr2Qriu5NoCW3g"],"compression":"none","packed_context_free_data":"","packed_trx":"47a5c45cdba9f38b3288000000000100000004c2323ad000000269b94b1bd010000000000000e3d00000000a8ed323218000000004c2323ad0000000000000e3d00000000b868a6c200"}]},"trx":{"expiration":"2019-04-27T18:53:59","ref_block_num":43483,"ref_block_prefix":2285014003,"max_net_usage_words":0,"max_cpu_usage_ms":0,"delay_sec":0,"context_free_actions":[],"actions":[{"account":"polman","name":"rqstdata","authorization":[{"actor":"bob","permission":"active"}],"data":{"addnet":"polman","rqster":"bob","targetdevice":"senali"},"hex_data":"000000004c2323ad0000000000000e3d00000000b868a6c2"}],"transaction_extensions":[],"signatures":["SIG_K1_Ke7d48UFBRrcNS6CuT6Bh899K6XSzWxyYheS3tB9eu3eKXv18hD7KKrpg5avZ2h5Z1M3bWWj8kuCX8pSGr2Qriu5NoCW3g"],"context_free_data":[]}},"block_time":"2019-04-27T18:53:00.500","block_num":43486,"last_irreversible_block":43594,"traces":[{"receipt":{"receiver":"polman","act_digest":"82c2235fd20fd01e83f94e450e8ac3e85707d846ef8aa68686cf0661d9fa56e7","global_sequence":61416,"recv_sequence":17890,"auth_sequence":[["bob",4]],"code_sequence":1,"abi_sequence":1},"act":{"account":"polman","name":"rqstdata","authorization":[{"actor":"bob","permission":"active"}],"data":{"addnet":"polman","rqster":"bob","targetdevice":"senali"},"hex_data":"000000004c2323ad0000000000000e3d00000000b868a6c2"},"context_free":false,"elapsed":2396,"console":"","trx_id":"fed344dbc79668c1708955b09ac6e41f4eb1b3574f8ad474470cb7ffd2cbfaa3","block_num":43486,"block_time":"2019-04-27T18:53:00.500","producer_block_id":null,"account_ram_deltas":[],"except":null,"inline_traces":[]}]}

Fig. 8. Transactions in block.
그림 8. 블록 내 트랜잭션

그림 8은 블록에 담긴 트랜잭션을 조회한 내용이다. 이 트랜잭션은 곧 여러 BP에 의해 검증되어 돌이킬 수 없는(irreversible) 트랜잭션이 되고 네트워크 자체를 공격하지 않는 한 삭제할 수 없는 기록이 된다. 이를 통해 체계에 접근하고자 하는 기록을 반영구적으로 기록하여 악의적인 사용자가 접근하더라도 그 사실을 알아챌 수 있다.

블록체인을 통해 무결성을 유지하려는 시도는 PoW 합의 알고리즘으로 시작되었다. 이 무결성은 유지한 채로 트랜잭션 속도를 통해 확장성까지 확보하는 것이 본 논문에서 사용한 DPoS 기반의 블록체인 시스템이다. 또한 스마트 컨트랙트를 통해 작성된 체계의 특징상 기록된 접근 기록의 무결성도 유지되므로 안전한 관리 체계를 제공한다.

일반적으로 IoT 장치와 게이트웨이는 PoW 기반 체계에서 채굴을 진행할 만큼 충분한 연산력을 갖추지 못한다. 이는 PoW 기반 네트워크에서 연산력의 51%를 지켜내기 어려움을 뜻하며 트랜잭션의 무결성이 더 쉽게 깨어질 수 있음을 나타낸다. 그러나 기존 사용자의 허가나 연동을 통해 연산력을 제공받아야 하는 DPoS의 경우 단순 연산력으로는 네트워크의 무결성을 침해할 수 없다. 블록에 기록된 정보의 증명은 네트워크의 지분에 따라 수행되기 때문이다.

Table 3. Block size per block size.
표 3. 트랜잭션 수 당 블록 사이즈

Tx Contained	Block Size (Byte)
0	670
1	1,623
15	14,996
30	29,345

표 3은 트랜잭션 반복 테스트를 진행하면서 필요한 수만큼 트랜잭션이 담긴 블록의 용량을 계산하였다. 초당 트랜잭션 실험에 따르면 블록 당 담길 수 있는 트랜잭션 수는 약 25~33개 이다. 한 블록은 0.5초에 하나씩 생성되므로 1초에 60개의 트랜잭션이 발생한다는 계산에 따라 하루에 발생하는 블록 수는 5,184,000개이다. [15]의 센서 네트워크에서는 29일간 약 2,540,000개의 전송이 발생했다. 1초에 약 1개의 트랜잭션이 발생하였다면 1초에 트랜잭션 0개와 1개인 블록이 하나씩 생성되므로 초당 용량 증가는 약 2,293Byte이다. 그러므로 블록체인의 용량은 하루에 198.12MB 만큼 증가한다. 가동 후 1년이 지난 네트워크 용량은 약 72.31GB이다.

그림 9는 게이트웨이 CPU 성능에 따라 350개의 트랜잭션을 합의 알고리즘만의 차이를 두고 처리하는데 소요된 시간이다. 4Core CPU를 사용한 게이트웨이에서는 PoW보다 DPoS 합의 알고리즘의

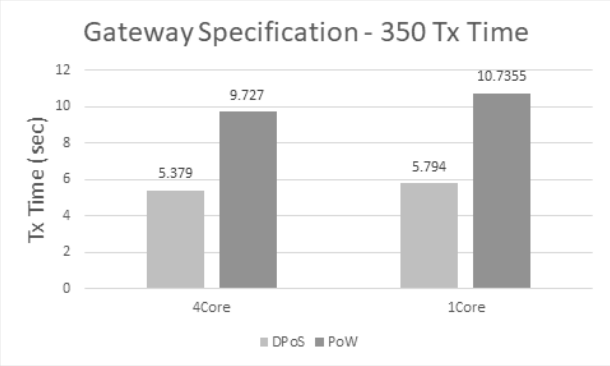

Fig. 9. Transaction time of consensus algorithms.
그림 9. 합의 알고리즘들의 트랜잭션 처리 속도

트랜잭션 속도 차이가 약 3초 빠름을 알 수 있다. 1Core CPU를 사용한 시스템에서는 DPoS의 경우 거의 소요 시간 증가가 미비하여 CPU 코어 수의 영향이 적음을 알 수 있으며 이는 비교적 적은 연산력을 가지고 원활한 트랜잭션 처리가 가능함을 보인다.

```
"rows": [{
    "device": "senali",
    "rqster": "alice",
    "isright": 1,
    "tmstmp": 1555350249
  },{
    "device": "senali",
    "rqster": "bob",
    "isright": 0,
    "tmstmp": 1556390261
  }]
```

Fig. 10. Experiment of authority record.
그림 10. 권한 기록 실험

그림 10은 허가된 사용자와 허가받지 않은 사용자가 메소드를 호출했을 때의 결과이다. 같은 메소드를 사용해서 네트워크의 같은 센서에 요청을 했을 때 인증된 사용자가 서명한 트랜잭션만 승인되므로 악의적인 사용자는 개인키를 해킹하거나 암호화된 트랜잭션을 해독하지 않으면 센서가 제공한 내용을 획득할 수 없을 것이다.

Ⅵ. 결론

본 논문에서는 다양한 사양의 스마트 홈 IoT 장치의 안전한 관리를 위하여 블록체인 기술을 활용한 관리 시스템을 제안하였다. 기존 검증을 위한 연산을 지속적으로 수행해야 하는 PoW 블록체인에서 벗어나 연산력이 아닌 네트워크에 축적된 지분을 통해 블록을 검증하는 PoS 방식, 그중에서 확장성 부분을 적극적으로 해결하고자 하는 DPoS 방식으로 IoT 환경에 적절한 보안용 블록체인 체계를 제안하였다. 이러한 블록체인 기반 관리 시스템은 다른 IoT 응용에서도 적용가능 할 것이다. 향후, 일반적인 홈 게이트웨이가 대용량 저장 장치를 가지고 있지 않으므로 용량 문제에서 자유로운 시스템 체계를 연구할 것이다.

References

[1] B. L. Risteska Stojkoska and K. V. Trivodaliev, “A review of Internet of Things for smart home: Challenges and solutions,” *Journal of Cleaner Production,* vol.140, pp.1454-1464, 2017.
DOI: 10.1016/j.jclepro.2016.10.006

[2] Y. Seo, J. Song, Y. Kong, “Blockchain Technology: Prospect and Implications in Perspective of Industry and Society,” *SPRI Issue Report*, No.2017-004, 2017.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in *Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp.618-623, 2017.
DOI: 10.1109/PERCOMW.2017.7917634

[4] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” arXiv:1802.04410 [cs], 2018. DOI: 10.1109/JIOT.2018.2847705

[5] EOSIO, https://github.com/eosio

[6] V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Loge, “The Smart Home Concept: our immediate future,” in *Proc. of 1ST IEEE International Conference on E-Learning in Industrial Electronics*, Hammamet, pp.23-28, 2006. DOI: 10.1109/ICELIE.2006.347206

[7] K. Kim, et. al., “IoT based smart home service framework technology,” *Broadcasting and Media Magazine*, Vol.20, No.3, pp.290-302, 2018. DOI: 10.1109/MobServ.2015.66

[8] M. Kim, “A Scheme of IoT Device Management using Virtual Machine at Edge Cloud,” Master Thesis, Kyungnam Univ., 2019.
[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008, https://bitcoin.org/bitcoin.pdf
[10] “Introduction to Smart Contracts-Solidity 0.5.8 documentation.” https://solidity.readthedocs.io/en/v0.5.8/introduction-to-smart-contracts.html
[11] V. Buterin, “On Stake,” Jul. 2014. https://blog.ethereum.org/2014/07/05/stake/
[12] B. Xu, D. Luthra, Z. Cole, and N. Blakely, “EOS: An Architectural, Performance, and Economic Analysis,” https://whiteblock.io/library/eos-test-report.pdf
[13] “Blockchain speeds & the scalability debate | Blocksplain.” https://blocksplain.com/2018/02/28/transaction-speeds/
[14] X. Hao, L. Yu, L. Zhiqiang, L. Zhen, and G. Dawu, “Dynamic Practical Byzantine Fault Tolerance,” in *Proc. of IEEE Conference on Communications and Network Security (CNS)*, Beijing, pp.1-8, 2018. DOI: 10.1109/CNS.2018.8433150
[15] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, and X. Li, “Does Wireless Sensor Network Scale? A Measurement Study on GreenOrbs,” *IEEE Trans. Parallel Distrib. Syst.,* vol.24, no.10, pp.1983-1993, 2013. DOI: 10.1109/TPDS.2012.216

BIOGRAPHY

Mihui Kim (Member)

1997 : B.S. in Dept. of Computer Science and Engineering, Ewha Womans University, Korea
1999 : M.S. in Dept. of Computer Science and Engineering, Ewha Womans University, Korea
1999~2003 : Researcher, ETRI (Electronics and Telecommunication Research Institute), Korea
2007 : Ph.D in Dept. of Computer Science and Engineering, Ewha Womans University, Korea
2007~2009 : Full Time Lecturer, Dept. of Computer Science and Engineering, Ewha Womans University, Korea.
2009~2010 : Postdoctoral Researcher, Computer Science, North Carolina State University, USA
2011~Current : Associate Professor, Dept. of Computer Science & Engineering, Hankyong National University, Korea
Research interests : Security and efficient protocol design in IoT and crowdsensing system, Blockchain technologies

Youngmin Kim (Member)

2013~Current: MS student, Dept. of Computer Science & Engineering, Hankyong National University, Korea
Research interests: Security in IoT and crowdsensing system, Blockchain technologies