IoT 시스템을 위한 블록체인 구현 기술에 관한 연구

김재우, 김동성*
ICT융합특성화연구센터, *금오공과대학교
jaewookim@kumoh.ac.kr, *dskim@kumoh.ac.kr

A Study on the Blockchain Implementation Technique for IoT Systems

Jae-Woo Kim, Dong-Seong Kim*
ICT Convergence Center, *Kumoh National Institute of Technology

요 약

4차산업혁명 시대의 온라인 신뢰 기술인 블록체인은 분산원장처리 기술로 트랜젝션 내역을 블록 단위로 네트워크상에서 분산으로 저장하고 검증하는 보안에 뛰어난 기술이다. 블록체인기술은 거래 플랫폼 뿐만아니라 산업 보안과 사물인터넷 플랫폼에 까지 다양하게 적용하기 위한 연구가 진행되고 있다. 본 고에서는 이러한 블록체인 기술을 구현하는데 있어서 기존의 방법과 지원 플랫폼에 대해서 분석하고, IoT 시스템을 위한 블록체인 구현방법에 대한 가이드를 제시한다.

Ⅰ. 서 론

블록체인에 의한 분산 원장 처리 기술은 4차 산업혁명 분야의 인프라 기술로 인공지능, 사물인터넷(Internet of Things:IoT)과 함께 활용 전망이 매우 높은 기술이다. 블록체인 기술은 peer to peer 네트워크 통신을 기반으로 하고 있으며, 블록구조에 포함된 데이터 트랜젝션 정보는 네트워크를 통해 분산된다. 블록체인은 블록과 블록간, 그리고 블록 내부의 트랜젝션 데이터 또는 프라이빗 데이터 사이에 서로 암호화 해시로 연결되어 체인 형태의 구조를 가진다. 이러한 체인형태의 데이터는 구조상 영원히 지우거나 수정할 수 없는 특성을 가진다. 블록체인은 크게 퍼블릭 블록체인과 프라이빗 블록체인으로 분류된다[1].

최근 IoT 시스템과 블록체인의 융합이 새로운 화두로 제시되고 있다[2]. 인터넷 연결과 정보 교환에 초점을 두고 상대적으로 보안에 대한 고려가 부족한 IoT 기술은 보안 문제를 해결하기 위해 블록체인 기술을 적용하는 연구가 진행되고 있다[3]. IoT 시스템에 볼록체인 기술을 적용하여 해결하고자 하는 보안 이슈로는 다수의 IoT 노드들중 임의의 노드가 해킹을 당하거나 물리적 손상을 입었을 때 그 상태를 빠르게 복원할 수 있도록 하는 것과 공격에 의한 데이터의 위/변조가 일어나더라도 블록체인 기술을 통해 빠르게 복구할 수 있는 무결성의 측면이 있다.

한편 IoT 시스템은 엣지 컴퓨팅을 기반으로 한다. 엣지 컴퓨팅은 중앙화된 컴퓨팅 로드를 분산시키기 위한 기술로 중앙화된 컴퓨팅이 아닌 탈중앙화 컴퓨팅으로 블록체인 기술의 목적과 일치한다고 볼 수 있다. 또한 IoT 기기들의 발전으로 사람의 개입이 없이 장치들끼리 정보를 주고받는 M2M(machine to machine) 통신기술이 IoT 기기 사이에서도 적용되고 있다. 이는 블록체인의 스마트 계약 어플리케이션을 이용하여 M2M 통신을 구현함으로써 M2M 통신을 효과적으로 수행할 수 있다.

이러한 블록체인 기술을 IoT 시스템에 적용하기 위해서는 실제 블록체인을 구성할 네트워크와 블록체인 엔진 구현이 필요하다. 블록체인 기술을 적용하여 암호화폐 거래, 기업 서비스, 정보 보안 분야에 적용하기 위한 시도가 늘어나면서 블록체인을 구현하기 위한 구현 인프라도 증가하고 있다. 본 논문은 블록체인 구현 방법에 대한 절차를 서술하고 현재 오픈소스 기반 블록체인 플랫폼에 대해 구현관점에서 분석한다. 마지막으로 IoT 시스템을 고려한 블록체인 구현조건을 도출하여 구현 가이드를 제시한다.

그림 1 블록체인 구현 절차

Ⅱ. 블록체인 구현방법

블록체인의 구현 방법은 두 가지로 정의할 수 있다. 블록체인 기술 자체를 위한 구현과 블록체인을 이용한 서비스 애플리케이션 구현으로 나누어진다. 첫째로 블록체인 플랫폼을 이용하지 않고 자체 블록체인 구현을 위해서는 블록체인의 가장 기본이 되는 비트코인 블록체인을 기준으로 구현을 시도하는 것이 일반적이다[4]. 그림 1은 일반적인 블록체인을 구현하기 위한 절차를 도시화한 것이다. 우선 개발자는 블록체인 구현을 위해 어떤 프로그래밍 언어를 사용할지를 정해야 그에 따라 블록체인을 구현시 필요한 함수 라이브러리를 제공 여부를 판단할 수 있다. 다음 단계는 블록체인의 블록구조, 해시 함수, 암호 알고리즘 구현과 같은 기본적인 블록체인 구조와 이를 생성하기 위한 함수들을 구현한다. 해시함수는 직접 코딩할 수도 있고 Hashlib 라이브러리에서 지원하는 SHA256 함수를 사용할 수 있다. 다음 단계는 합의 알고리즘을 구현한다. 합의 알고리즘은 블록체인 기술의 핵심 요소이다. 합의 알고리즘을 통해 블록체인 네트워크가 운용된다. 합의 알고리즘이 결정되면 블록체인을 통한 트랜젝션 즉 거래를 어떻게 동작할지를 구현한다. 이때 거래를 발생시키기 위한 개인키, 공개키 그리고 이를 저장하기위한 지갑을 구현할 수도 있다. 마지막 단계는 구현된 블록체인을 운용시킬 네트워크와 통신 인터페이스를 정합하는 단계와 블록체인을 가시화하고 쉬운 접근성을 위한 사용자 인터페이스를 구현함으로써 블록체인을 구현을 완료한다.

표 1 블록체인 플랫폼

플랫폼	특징
이더리움	다양한 언어 지원, 다양한 Dapp 개발 진행 EVM 기반 스마트 계약 실행 Pow 알고리즘 사용
하이퍼레저	리눅스 재단에서 설립 IBM에서 추진 기업용 비즈니스 거래 적용 플랫폼 PoET 외 다양한 합의 알고리즘 적용 가능 허가형 블록체인
네오	온체인에서 설립, 분산앱 확장성 지원 DBFT 알고리즘 사용
스텔라	교차 자산의 가치를 전송하기 위해 개발 금융 거래 플랫폼, SCP 알고리즘 사용
오픈체인	디지털 자산 안전 관리 플랫폼 분할된 합의 알고리즘 사용 채굴없이 경제적으로 운영
이오스	블록원에서 개발 비트코인과 이더리움의 확장성 이슈를 해결 위임 PoS 알고리즘 사용
리플	디지털 거래소, 기업, 은행, 결제 서비스를 연결하기 위해 개발, 확률적 투표 알고리즘 사용 퍼미션드 블록체인 제공

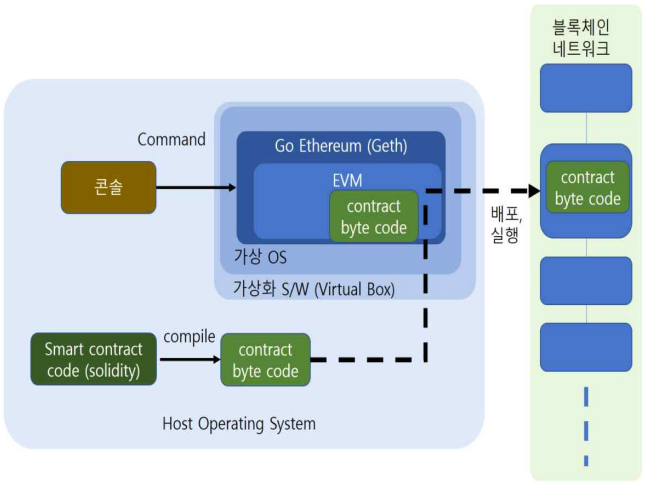

그림 2 이더리움 블록체인 구현 및 구동 블록도

두 번째 블록체인 구현 방법은 기존의 블록체인 오픈소스 플랫폼을 이용하는 방법이다. 표1에서 이더리움 플랫폼을 포함한 오픈소스를 지원하는 블록체인 플랫폼과 특징을 정리하였다. 표1에 정리된 플랫폼 외에도 큐오럼, 멀티체인, 엘리먼츠 등이 있다. 기존의 블록체인 플랫폼을 이용하여 원하는 블록체인 어플리케이션을 만드는 것을 탈중앙화 어플리케이션 개발 즉 DApp(Decentralized Application) 개발이라 한다. 대표적으로 이더리움 블록체인 플랫폼은 스마트 계약 서비스를 위해 다양한 프로그래밍 언어를 지원하고 있다. 그림 2는 이더리움 플랫폼의 구조를 도시화 한 것이다. 이더리움 플랫폼은 Ethereum Virtual Machine (EVM)을 통해 이더리움 블록체인 네트워크 내에 실행 가능한 프로그램을 개발할 수 있도록 한다. 이를 지원하는 API가 Geth 이다. 스마트 계약을 위해 Solidity 라는 언어를 사용하여 DApp를 개발하고 해당 코드를 컴파일하여 EVM에서 배포하고 실행하도록 한다. 배포 및 실행은 콘솔이나 브라우저로 EVM에 명령할 수 있다. EVM을 사용하기 위해서는 리눅스와 같은 가상OS를 설치하고 가상 OS위에 Geth를 설치하여 EVM을 구동한다.

1. IoT 시스템의 블록체인 네트워크 구현 고려사항

IoT 시스템에 블록체인을 적용하기 위해서는 IoT 기기의 특성과 IoT 네트워크 구조를 고려하여야 한다. IoT 기기는 상대적으로 저사양의 저전력의 컴퓨팅파워를 가진다. 따라서 낮은 컴퓨팅파워로 합의 알고리즘을 수행할 수 있는 프라이빗 블록체인 유형이 적합하다. 그리고 IoT 네트워크의 IoT 노드들은 비정형화된 다품종 특성을 가지는 이종 프로세스를 사용하는 특징이 있다. 따라서 기존의 이식성이 좋고 다양한 언어를 지원하는 블록체인 플랫폼을 이용한 구현 방법이 적절하다. 마지막으로 IoT 기기는 센서로부터 실시간으로 데이터를 처리해야 하는 데이터의 실시간성을 보장해야 한다. 이를 위해서는 블록체인의 트랜잭션 처리 속도가 상대적으로 빠른 프라이빗 유형의 블록체인이 적절하다.

Ⅲ. 결론

본 논문에서는 IoT 기기로 구성된 IoT 시스템에 보안과 서비스 응용강화를 위한 블록체인 기술을 적용하기 위해서 블록체인 구현 방법에 대하여 기술하였다. 먼저 기존의 블록체인을 구현사례를 분석하여 블록체인 구현에 대한 절차를 도시하였다. 추가로 블록체인 플랫폼을 이용하여 블록체인 네트워크를 구현 방법에 대하여 논의하고 대표적인 플랫폼을 예를 들어 그 방법을 정리하였다. 마지막으로 IoT 시스템에서 블록체인 구현하기 위하여 고려해야할 사항을 정리하고 각 사항에 대한 블록체인 구현방법을 제시하였다. 분석결과 IoT 시스템을 위한 블록체인 구현은 개발시간을 단축하기 위해서는 기존의 블록체인 플랫폼을 이용하는 것이 이득이 있으며 IoT 기기의 저사양 특성을 고려하여 적은 컴퓨팅파워가 소모되는 합의 알고리즘을 사용할 것과 빠른 트랜잭션 처리를 위하여 프라이빗 블록체인 또는 허가형 블록체인을 구현할 것을 제시하였다. 향후 연구로는 실제 IoT시스템 사례를 들어 구체적인 블록체인 구현모델을 도출하고 실제 구현을 통해 블록체인 네트워크를 시험할 계획이다.

ACKNOWLEDGMENT

이 논문은 2019년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업과 기초연구사업으로 수행된 연구임 (2018R1A6A1A03024003, 2019R1I1A1A01063895).

참 고 문 헌

[1] Z. Zheng, S. Xie, H. Dai and H. Wang, "An overview of blockchain technology: Architecture consensus and future trends", Proc. IEEE Int. Congr. Big Data Big Data Congr., pp. 557-564, Jun. 2017.

[2] Qin Wang, Xinqi Zhu, Yiyang Ni, Li Gu, Honbo Zhu, "Blockchain for the IoT and industrial IoT:A review" Internet of Things, Vol. 10, pp 100081, June, 2020

[3] D Minoli, B Occhiogrosso "Blockchain mechanisms for IoT security" Internet of Things, Vol. 1-2, pp 1-13, September, 2018

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008