정 보 보 호 학 회 지
제28권 제5호, 2018. 10

사물인터넷 서비스 연동을 위한 블록체인 아키텍처

최 종 석*, 허 신 욱**, 김 호 원**

요 약

본 논문에서는 사물인터넷 서비스와 블록체인 플랫폼간의 연동을 위한 아키텍처를 제안한다. 블록체인은 다양한 산업분야에서데이터 신뢰성 및 안전성 측면에서의 효율성을 제공한다. 반면에 데이터 쓰기 및 읽기에 대한 낮은 성능 때문에 실제 서비스 적용하기 어렵다. 특히 사물인터넷 서비스와 같은 다량의 데이터가 발생하는 분야에서는 블록체인을 실질적으로 적용하기 어렵지만, 사물인터넷은 프라이버시 및 데이터 보안 측면에서 많은 보안 문제를 야기할 수 있는 분야로써, 블록체인을 통한 데이터 추적 및 신뢰성 보안을 필수적으로 요구된다. 본 논문에서는 이와 같이 실시간성과 신뢰성을 보장하기 위한 사물인터넷 연동형 블록체인 플랫폼 아키텍처를 소개한다. 실시간성을 유지하기 위해서 단일 피어 검증을 통한 실시간 데이터 관리를 활용하며, 신뢰성 유지를 위해서 합의를 통한 분산원장을 활용한다. 단일 피어 검증 데이터는 합의 과정을 거치기 이전에 데이터를 수신받은 단일피어가 분산원장과 별도의 상태 데이터베이스를 통해 실시간 데이터를 저장하여 실시간 서비스에 제공한다.

Ⅰ. 서 론

콘텐츠 서비스의 발전에 따라 온라인 데이터에 대한 보안 및 프라이버시 보호에 대한 요구가 증가하였다. 이에 따라 고신뢰 보안플랫폼에 대한 연구가 진행되었으며, 블록체인은 비트코인[1], 이더리움[2] 등과 같은 암호화폐를 통해서 기술적 측면에서의 신뢰성이 입증되었다.이러한 퍼블릭 블록체인은 20~30 TPS(Transaction per second)로 기존 서비스를 수용하기 어려운 정도의 수준이다. 이를 개선하기 위해서 프라이빗 블록체인에 대한 연구가 시작되었으며, 대표적인 프라이빗 블록체인에는 하이퍼레져 프로젝트의 패브릭(Fabric)이 있다. 많은 연구[3~7]에서 하이퍼레져에 대한 성능 벤치마킹을 수행한 결과, 하이퍼레져 패브릭은 퍼블릭 블록체인보다는 효율적이지만 여전히 1000 TPS 이하인 것으로 나타났다.

최근에 많은 개인용 디바이스가 보급되면서 이를 이용한 사물인터넷서비스가 개발되었다. 이러한 사물인터넷 서비스는 디바이스, 네트워크, 플랫폼, 응용계층의 4개의 계층으로 구성된다. 특히 사물인터넷 플랫폼 계층은 다른 계층과 연동하고, 서비스를 제공하는데 필요한실질적 기능을 제공하는 핵심계층이라 할 수 있다. 대표적인 사물인터넷 플랫폼으로는 oneM2M[8], LwM2M[9], IoTivity[10] 등이 있으며, 특히 oneM2M은 국내 정부사업을 비롯해 다양한 분야에서 활용되고 있다.

본 논문에서는 실시간은 요구하는 사물인터넷 플랫폼에서 블록체인 기반의 고신뢰 보안 서비스를 제공하기 위한 방법을 제안한다. 본 논문에서는 oneM2M과 하이퍼레저 패브릭간의 데이터 연계를 위한 체인코드 개발 방법을 제시한다. 본 논문에서 제안한 기법은 트랜잭션및 합의를 통해 생성되는 블록체인 데이터와 단일 피어에 의해 생성되는 프라이빗 데이터와 같이 두 종류의 데이터로 관리한다. 이러한 기법을 적용하기 위해서는 트랜잭션별/데이터별 신뢰성 요구사항에 대한 명세가 필요하다. 이를 토대로 단일피어데이터로 활용할 것인지에 대한 검토가 요구된다.

본 논문에서 제안한 기법을 활용하면 실시간 데이터를 요구하는 사물인터넷 기반의 서비스(에너지, 스마트홈 등)에 블록체인 기반 고신뢰성을 제공할 수 있다.

본 연구는 2018년도 중소벤처기업부의 기술개발사업 지원에 의한 연구임 [S2607026]
* ㈜스마트엠투엠 (jseokchoi@smartm2m.co.kr)
** 부산대학교 ({shinwookheo, howonkim}@pusan.ac.kr)

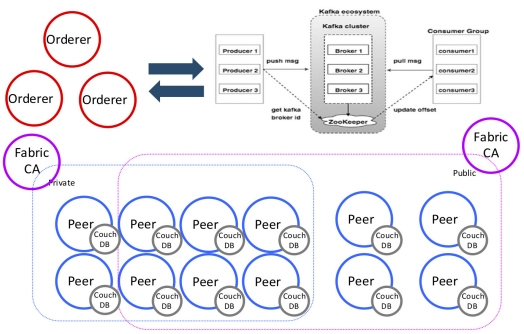
Ⅱ. Hyperledger Fabric 블록체인 구조

본 절에서는 리눅스 재단의 하이퍼레져 패브릭(Hyperledger Fabric)[11] 프로젝트를 살펴본다. 하이퍼레져 프로젝트는 2015년 17개 회원사로 시작되었으며, 현재 130개 회원사가 참여하고 있는 블록체인 프로젝트이다. 하이퍼레져 프로젝트 중 Fabric은 기업용 프레임워크 블록체인 프로젝트로 IBM에서 주도하고 있는 허가형(Permissioned) 구조의 블록체인 플랫폼으로, 분산 원장 기술과 스마트 컨트랙트(체인코드) 개념을 포함하고 있다.

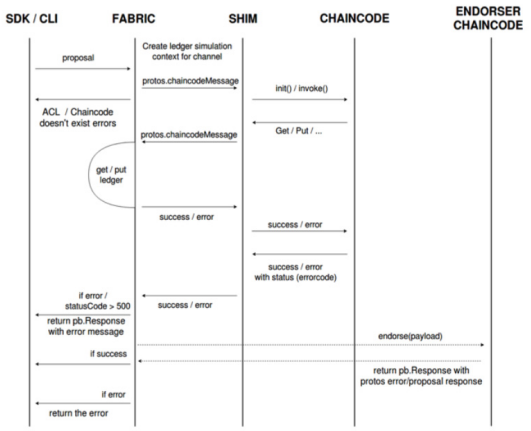
하이퍼레져 패브릭의 네트워크는 서비스 제공자(기업 또는 기관)의 승인을 받아야 참여 가능하며, 모든 노드들의 상호 검증을 높은 신뢰도를 가진다. 패브릭은 크게 검증노드, 비검증노드로 구분된다. 검증노드는 원장을 들고 있으며 트랜잭션에 대한 검증을 수행하며, 비검증노드는 트랜잭션 생성만 수행한다. 피어(Peer), Endorser, Orderer 등이 검증노드에 속하며, 클라이언트(SDK)는 비검증노드에 속할 수 있다.

Fabric v1.0 에서는 Endorser와 Consensus 노드가 분리되었으며, 각각의 체인코드는다른 Endorser를 가진다. Consensus 노드는 트랜잭션의순서를 보장해주는 역할을 수행한다.

패브릭에서의 스마트 컨트랙트 개념은 체인코드(Chain code)이다. 체인코드는 일반적으로 도커(Docker) 기반의 검증된 피어 형태로 네트워크에 참여하며, gRPC 통신 기반으로 체인코드 명령을 수행한다. 기본적으로 Init(초기화), Query(읽기),Invoke(쓰기) 3가지 필수 구현 함수가 있다. Init 또는 Invoke 함수는 트랜잭션이 발생하며, Query 함수의 경우 트랜잭션이



〔그림 1〕 하이퍼레저 네트워크 구성



〔그림 2〕 체인코드 수행과정

발생하지 않고 분산원장에 저장된 데이터를 조회한다. 클라이언트의 요청에따른 체인코드의 수행과정은 [그림 3]와 같다.

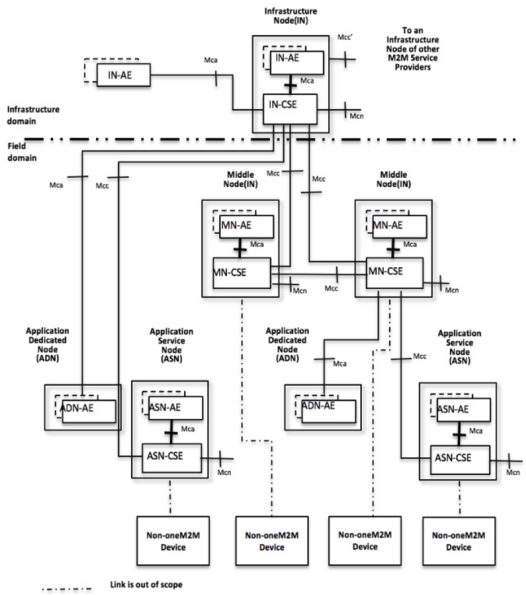
Ⅲ. oneM2M

본 절에서는 oneM2M의 전체 아키텍처를 살펴본다. oneM2M은 다양한 서비스의 요구사항을 만족시킬 수 있는 사물인터넷에서의 공통 플랫폼을 정의하고, 타 플랫폼과의 상호동작(Internetworking)을 표준화하였다. 다양한 응용 간의 호환을 위한 인터페이스를 정의하여 종래의 수직적인 형태의 사물인터넷 플랫폼에서 벗어나 수평적인 플랫폼을 구성하여 사물인터넷 플랫폼의 파편화 방지, 개발 및 운용비용을 감소할 수 있다. 스마트 홈, 스마트 카, 에너지, 헬스케어, 엔터프라이즈, 공공서비스와 같은 7개 산업 분야의 Use Case를 반영하여 요구사항을 도출하고, 핵심 기능(데이터수집 및 보고 기능, 기기의 원격 제어, 연결성 유지, 보안 및 프라이버시 기능 등)과 인터페이스를 정의하였다.

oneM2M의 개체는 User/End-User, application service provider, M2M service provider, network operator로 구성된다. User/End-User는 M2M 솔루션을 사용하는 개인 또는 기업을 의미하며, Application service providers는 M2M서비스를 제공하는 제공 주체를 의미한다. M2M service provider는application service provider에게 M2M 공통서비스를 제공하는 주체이며, network operator는 M2M service provider에게 네트워크를 제공하는 주체이다.

oneM2M은 여러 개의 노드(Node) 연결되어 하나의 인프라를 형성하며, 하나의 노드는 AE(Application Entity)와 CSE(Common Service Entity), NSE(Network Service Entity)로 구성된다. 기능적인 관점에서 AE는 M2M서비스를 제공하기 위한 애플리케이션 기능 로직을 담당하며, CSE는 AE를 위한 12개의 공통 서비스기능 제공한다. NSE는CSE에게 네트워크 장치 관리 및 서비스등을 제공하고, 각각의 개체(Entity)는 참조점(Reference Point)을 통해서 상호 동작한다. 이 때, 참조점은 CSE와 AE, CSE간의 연결을 의미하며, 실제 통신을 위한 바인딩 프로토콜(Binding Protocol)에 매핑되어 통신을 수행한다. [그림 4]은 oneM2M의 전체 구조를 보여준다. [그림 4]에서 Mca는 CSE-AE간의 통신, Mcc는 CSE-CSE간의 통신, Mcn은CSE와 NSE간의 통신, Mcc`는 다른 Infrastructure Domain CSE와의 통신을 나타낸다.

CSE는 Lookup/Discovery/Resolution을 포함한 다양한 같은 공통 서비스 기능(Common Service Function)을 제공하며, ROA(Resource-Oriented Architecture)에 기반하여 CRUDN(Create,Retrieve, Update, Delete, Notify) 연산을 12개의 공통서비스 기능에게 제공한다.



〔그림 3〕 oneM2M 전체구조도

Ⅳ. IoT 서비스 연동 블록체인 아키텍처

본 장에서는 고가용성, 고신뢰성을 제공하는 블록체인 기반 사물인터넷 서비스 구축 기법을 제시한다. 고가용성 제공을 위해 단일 피어상에서의 실시간 데이터 처리 기법과 사물인터넷 서비스 제공을 위한 oneM2M 플랫폼 연동 방안을 제시한다.

4.1. 블록체인상에서의실시간 데이터 처리 기법

프라이빗 블록체인은 퍼블릭 블록체인에 비해서 상대적으로 높은 TPS를 보이고 있다. 하지만 실시간 서비스를 위해서는 피어당 5000~20000 TPS의 성능이 보장이 되어야 한다. 본 논문에서는 단일피어 데이터 처리기법을 이용하여 실시간 데이터를 관리하는 기법을 제안한다.

4.1.1. 단일피어 데이터저장

하이퍼레저 패브릭과 동일하게 트랜잭션을 생성하되 실시간성과 고신뢰성에 대한 플래그를 제공하여 보장여부를 기술한다.

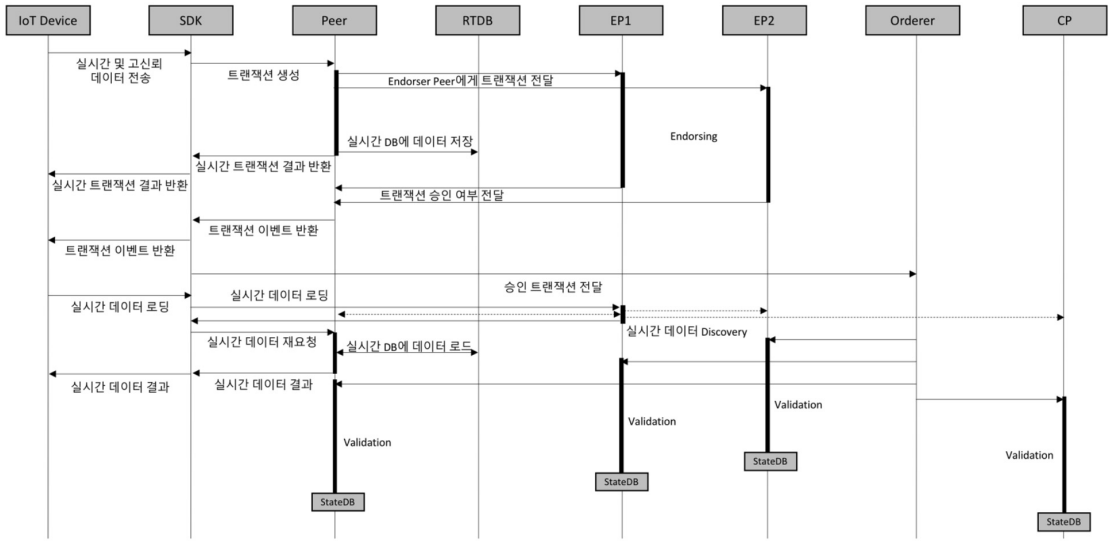
체인코드 호출시에 실시간성 플래그를 검사하여, 실시간성 플래그가 활성화 되어 있다면 단일피어 데이터 처리를 수행한다. 이때, 데이터를 저장하기 위해서 단일피어의 ID를 포함한 UUID를 이용하여 저장한다.

단일피어 데이터 처리는 별도의 실시간 데이터베이스를 이용하여 데이터를 관리하는 방법으로, 본 논문에서 제안하는 블록체인의 구조는 실시간 데이터베이스와 상태 데이터베이스 두가지를 동시에 운영한다.

4.1.2. 단일피어 데이터디스커버리

단일피어 데이터는 블록체인과 같이 분산원장을 통해서 관리되지 않기 때문에, 데이터를 보관하는 피어만 해당 데이터를 조회할 수 있다.

데이터를 가지고 있지 않은 피어에게 데이터를 요청하는 경우에는 데이터 디스커버리 프로토콜을 통해서 단일피어 데이터의 주체를 조회하고, SDK를 해당 피어로 리다이렉트를 수행한다.



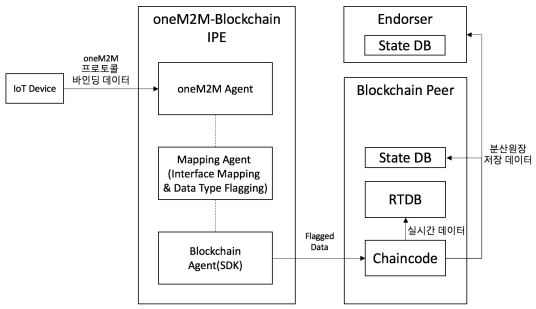
〔그림 4〕 실시간 데이터 처리 절차

4.2. oneM2M 플랫폼 데이터 연계 방안

본 절에서는 oneM2M 서비스 플랫폼과 블록체인간의 연동을 위한 IPE(Interworking Proxy Entity)의 구조를 제시한다

IPE는 oneM2M 표준 프로토콜로 바인딩된 데이터와 상호 연동을 위한 oneM2M Agent, oneM2M 프로토콜 인터페이스 매핑과 실시간 데이터와 상태 데이터베이스에 저장될 데이터를 표시(Flagging) 하는 Mapping Agent, 블록체인 연동을 위한 Blockchain Agent(SDK)로 구성된다.

IoT Device와 oneM2M Agent는 oneM2M 표준인 TS-0009 Protocol Binding 문서를 따르며 oneM2M 요청/응답메시지로 상호 연동이 가능하다. oneM2M Agent는 전달받은 요청을 Mapping Agent에 전달하거나, 요청에 대한 응답(체인코드 실행 결과)을 oneM2M 프로토콜에 맞춰 IoT Device로 전달하는 역할을 한다.



〔그림 5〕 oneM2M 플랫폼 데이터 연계 구조

Mapping Agent는 oneM2M 프로토콜을 체인코드에 적합한 형태로 데이터를 매핑하고, 전달받은 데이터에 실시간성과 고신뢰성 데이터 타입을 Flag를 통해 표시한다. 매핑과 Flag 표시가 완료된 데이터는 Blockchain Agent를 통해 체인코드로 전달된다.

Blockchain Agent를 통해 블록체인 피어로 전달되는 데이터는 실시간성 데이터와 상태 데이터베이스에 저장되는 고신뢰성 분산원장 데이터 타입으로 구분되며 데이터 타입에 따라 체인코드는 저장 위치를 선택하게 된다.

Ⅴ. 결 론

본 논문에서는 사물인터넷 서비스의 실시간성과 블록체인의 고신뢰성을 보장하기 위한 사물인터넷 서비스 연동형 블록체인 아키텍처를 설계하였다.

대부분의 블록체인은 상태 데이터베이스를 통해서 분산원장을 운용한다. 상태 데이터베이스에 저장되기 위해서는 합의와 트랜잭션 검증과정을 거치게 되는데, 이러한 과정은 블록체인의 성능을 저해한다. 실질적으로 사물인터넷 서비스를 포함한 대부분의 서비스가 높은 TPS를 요구하는 반면에 블록체인 플랫폼은 낮은 TPS를 보이며, 실질적인 서비스에 적용되기 어려웠다.

본 논문에서는 실시간성과 신뢰성을 동시에 보장하기 위해서 실시간 데이터베이스와 상태 데이터베이스를 함께 운용할 수 있는 아키텍처를 제안하였다. 실시간성을 보장해야하는 데이터를 플래그를 이용하여 활성화하고, 이를 기반으로 단일피어 검증을 통한 실시간 데이터베이스에 저장한다. 실시간 데이터베이스에 저장된 데이터는 분산원장기반으로 관리되는 것이 아니기 때문에, 단일 피어가 해당 데이터를 관리한다. 따라서 해당 피어만 해당 데이터를 조회할 수 있기 때문에, 다른 피어가 조회하기 위해서는 데이터 디스커버리 과정을 거쳐서, 데이터를 저장하고 있는 피어를 검색한 후에 SDK를 해당 피어로 리다이렉트 시켜주는 과정을 거친다.

본 논문에서 제안한 실시간성과 신뢰성을 보장할 수 있는 블록체인 모델을 통해서 기존의 높은 성능을 요구하는 서비스에도 블록체인을 적용할 수 있을 것으로 기대된다.

참 고 문 헌

[1] NakamotoSatoshi, “Bitcoin: APeer-to-Peer Electronic Cash System.”,2008.

[2] Buterin, V. "Ethereum: A next-generation cryptocurrency and decentralized application platform." Bitcoin Magazine (2014).

[3] Sousa, Joao, Alysson Bessani, and Marko Vukolic. "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform." 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2018.

[4] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." Proceedings of the Thirteenth EuroSys Conference. ACM, 2018

[5] Sukhwani, Harish, et al. "Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric)." Reliable Distributed Systems (SRDS), 2017 IEEE 36th Symposium on. IEEE, 2017.

[6] Vukolić, Marko. "Rethinking permissioned blockchains." Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017.

[7] Vukolić, Marko. Hyperledger fabric: towards scalable blockchain for business. Tech. rep. Trust in Digital Life 2016. IBM Research, 2016. URl: https://www. zurich. ibm. com/dccl/papers/cachin_dccl. pdf, 2016.

[8] Swetina, Jorg, et al. "Toward a standardized common M2M service layer platform: Introduction to oneM2M." IEEE Wireless Communications 21.3 (2014): 20-26.

[9] Tian, Linyi. "Lightweight m2m (oma lwm2m)." OMA device management working group (OMA DM WG), Open Mobile Alliance (OMA) (2012).

[10] Open Interconnect Consortium. "The Open Interconnect Consortium and IoTivity." (2015).

[11] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Vol. 310. 2016.

〈저 자 소 개〉

최 종 석 (Jongseok Choi)

2011년 2월 : 동명대학교 정보보호학과 (공학사)
2013년 2월 : 부산대학교 컴퓨터공학과 (공학석사)
2017년 2월 : 부산대학교 전기전자컴퓨터공학과 (공학박사)
2017년 2월~2017년 10월 : 스마일게이트 스토브 연구원
2017년 11월~현재 : 부산대학교 사물인터넷연구센터 연구교수
2018년 2월~현재 : ㈜스마트엠투엠 대표이사
관심분야 : 블록체인, IoT보안, 사이버보안, 암호 등

허 신 욱 (Shinwook Heo)

2013년 2월 : 부산대학교 정보컴퓨터공학부 졸업
2013년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석박사통합과정
관심분야 : 블록체인, IoT보안, 사이버보안 등

김 호 원 (Howon Kim)

종신회원

1993년 2월 : 경북대학교 전자공학과 (공학사)
1995년 2월 : 포항공과대학교 전자전기공학과 (공학석사)
1999년 2월 : 포항공과대학교 전자전기공학과 (공학박사)
2008년~현재 : 부산대학교 정보컴퓨터공학부 교수
2015년~현재 : 부산대학교 정보컴퓨터공학부 교수
관심분야 : IoT, 블록체인, 강화학습, 디지털트윈, 플랫폼 보안, 암호 프로세서 등