효율적인 BIoT 개발을 위한 블록체인 ETH 2.0 플랫폼 분석

이용주[1,*] · 우성희[2]

[1]충북대학교 · [2]한국교통대학교

Blockchain ETH 2.0 Platform Analysis for Efficient BIoT Development

YongJoo Lee[1,*] · Sung-Hee Woo

[1]ChungBuk National University · [2]Korea National University of Transportation

E-mail : yjlee3363@naver.com / shwoo@ut.ac.kr

요 약

4차 산업에 대한 꾸준한 투자와 개발로 IoT 기술이 보다 발전하게 되었고, 이에 따라 필요한 보안 플랫폼을 제공할 수 있는 플랫폼 기반의 블록체인 기술이 필요하게 되었다. 블록체인 기반의 IoT 어플리케이션인 BIoT는 향후 보다 다양한 분야에 적용되기 위하여 보다 정교한 보안성과 확장성 및 효율성을 제공하는 플랫폼 기술이 요구된다. 본 논문에서는 최근 발표되어 이슈가 되고 있는 스마트 컨트랙트 ETH 2.0을 분석하여 기존의 BIoT 개발에 요구되는 사항들을 비교하고 향후 다가오는 BIoT의 미래를 전망하여 본다.

ABSTRACT

The steady investment and development in the fourth industry led to the development of IoT technology, which led to the dissemination of platform-based blockchain technology that could provide the necessary security platform. BIoT, a blockchain-based IoT application, requires blockchain platform technology that provides more sophisticated security, scalability, and efficiency in order to be applied to more diverse fields in the future. In this paper, we analyze the recently announced smart contract ETH 2.0 to compare the requirements for existing BIoT development and to predict the future of BIoT in the future.

키워드

Blockchain, IoT, BIoT, ETH, 비콘체인, 사물인터넷

Ⅰ. 서 론

사물인터넷(Internet of Things) 기술은 우리 사회 곳곳에서 많은 변화를 일으키며 다양한 분야로 발전되고 있다. IoT 단말기는 센서의 부착으로 인터넷에 연결되어 실시간으로 정보를 처리하는 역할을 한다. 홈 네트워크와 연동되면 집안에서 가전 등을 이용하여 집안일을 제어할 수 있는 등 다양한 분야에 적용되고 있다. 그러나 이렇게 다양한 분야에 적용되는 IoT 단말은 실제로 민감하고 중요한 정보들을 다루게 되어 보안 취약성이 늘어나게 되고, 그 수가 폭발적으로 증가함에 따라 효율적인 처리 방식에 대한 문제도 급부상하게 되었다.

이 논문에서는 향후 미래의 IoT 네트워크에서 최적의 대안으로 떠오르고 있는 블록체인 플랫폼에 대해서 살펴보고 효율적인 BIoT 처리를 위한 Ethereum (ETH) 2.0에 대해서 심층 분석해 보고자 한다.

Ⅱ. 관련연구

사물인터넷은 각종 기기나 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 말한

* speaker

다. 인터넷으로 연결되어 있어서 서로 데이터를 주고받을 수 있고, 수집된 데이터를 사용자에게 제공할 수도 있다. IoT 산업은 빠르게 성장하고 있고 2022년에는 1조 달러를 돌파할 것으로 예상된다. 블록체인 기반의 IoT에 대한 연구도 활발히 진행되고 있는데, 블록체인 네트워크에 참여하는 모든 노드는 네트워크를 이용 및 관리를 하여 체인처럼 연관성을 갖게 되어 보안성이 높고 안전한 거래가 가능하다. 그러나 블록체인과 IoT를 결합하기 위해서는 기존의 중앙 집중형 구조로 설계되어 있는 IoT 기기와 분산된 네트워크 구조를 추구하는 블록체인간의 이질적인 문제를 해결해야 한다. 또한 폭발적인 사용량의 증가가 예상되는 IoT 기기에 비해 거래 속도가 제한적이고 느린 블록체인은 성능적인 측면에서 떨어지기 때문에 기존의 작업증명과 같은 합의 알고리즘을 채택하는 이더리움 플랫폼에서는 한계가 있다. 이러한 문제를 극복하고자 다양한 형태의 네트워크가 제안되고 있다.

2.1 IoT 체인

IoT Chain은 블록체인 기반의 IoT를 지원하기 위하여 PBFT(Practical Byzantine Fault Tolerance), SPV(Simplified Payment Verification) 등의 해결책을 제안하였다. SPV는 블록체인 처리 효과를 높이기 위해 트랜잭션들은 제외하고 블록의 헤더만을 저장하여 블록 사이즈를 줄이는 방법을 채택하였다. 또한 IoT 기기의 사용자 데이터에 대한 보안성을 강화하여 사용자 데이터를 사고 팔 수 있도록 네트워크를 설계하였다.

2.2 IoTEX

중앙 집중화된 방식으로 동작하는 IoT 디바이스들에 확장성, 운영비절감, 개인정보 등의 보안성 등을 제공하기 위해 제안된 블록체인 플랫폼이다. 다수의 독립적인 서브 블록체인이 배치되며 중앙의 루트 블록체인이 다수의 서브 블록체인을 관리하는 구조로서 루트 블록체인이 서브체인 간 연결을 담당하는 역할을 한다. 빠르고 효율적인 합의 체계를 확보하기 위해 다양한 하이브리드 형식의 협의 알고리즘을 제안하였다.

III. BIoT 개발을 위한 ETH 2.0

3.1 효율적인 BIoT를 위한 ETH

이더리움은 합의 알고리즘으로 작업증명(Proof of Work: PoW)를 채택하였다. 막대한 컴퓨팅 능력을 투자하여 복잡한 계산에 대한 문제(Nonce)를 해결한 채굴자에게 보상하여 주는 알고리즘이다. 이를 위해 Edash라는 이더리움 합의엔진을 개발하여 컴퓨터 메모리상의 일정양의 데이터를 읽은 후 nonce와 함께 해시 계산을 하는 메모리 IO 중심의 작업 증명 방식을 적용하였다. 이더리움의 인기가 수년간 지속되면서 토큰을 관리하는 이더스캔의 거래량이 폭발적으로 증가하게 되었다. 그러나 늘어나는 거래량에 비해 처리율은 제한적인 상황에서 빠르게 처리할 수 없는 문제에 부딪혔고 거래가 밀리고 지연되는 백로그(backlog) 현상이 발생하였다. PoW 방식의 근본적인 문제인 검증에 사용되는 많은 전력과 늘어나는 용량으로 데이터 분할저장에 대한 필요성, 보안문제 등을 해결할 필요성이 대두되었다. 이에 따라 이더리움의 문제점을 보완하여 업그레이드 된 이더리움 2.0(ETH 2.0)이 2020년에 출시되었다. ETH 2.0의 완벽한 전환은 4단계(세리니티) 후에 완성될 예정이며 이는 완전한 PoS(Proof of Stake: PoS)로의 전환을 의미한다.

3.2 ETH 2.0: 스마트 컨트랙트의 진화

- 비콘체인(Beacon chain)

채굴을 통해 블록체인 네트워크에 보안을 제공하는 방식에서는 언제든 공격을 받을 위험에 노출돼 있다. 이더리움은 비콘체인을 통해 단계별 진화를 위한 지속적인 확장의 토대를 마련하였다. ETH 2.0에서의 가장 큰 변화는 작업증명(PoW)에서 지분증명(PoS) 으로의 전환을 시도한 점이다. ETH 2.0으로의 업그레이드는 비콘체인의 도입인 0단계부터 시작되게 된다. 현재 전환을 위한 과정에 있고 비콘체인은 PoW와 PoS를 연결하는 알고리즘의 역할을 한다. 비콘체인의 프로세싱은 기존 POW 체인 프로세싱과 근본적으로 유사하지만 POS 메커니즘을 처리하기 위해 PoS의 유효성 검증인 집단(Active validator set)을 저장하고 관리한다. 취득 거래 검증인과 토큰을 관리하고 제안된 블록의 투표를 진행하여 검증인에게 전달하며 보상과 처벌을 진행하는 PoS 메커니즘의 종합적인 관리역할을 하게 된다.

- 확장성문제 샤딩

PoW의 문제점을 해결하기 위한 대안으로 PoS로의 전환을 준비함과 함께 기존 버전에서의 확장성을 해결하기 위한 문제 또한 중요한 이슈가 되었다. 이를 해결하기 위한 방안으로 제시된 것이 샤딩(Sharding)이다. 기존의 버전에서 블록 검증에 전체 노드가 참여하는 방식에서 발생하는 성능문제와 확장성 문제를 보완하기 위한 방법으로 노드를 샤드(Shard)라는 작은 그룹으로 나누어 그룹별로 거래를 처리하도록 하는 방식이다. 샤딩으로 인한 부정거래를 방지하기 위하여 비콘체인이 샤딩을 위한 프로세스를 관리하여 담합과 공격 등을

방지하고, 소규모 샤드가 거래를 동시다발적으로 처리할 수 있도록 해주게 된다.

3.3 IoT와 블록체인의 결합: BIoT

미래에 4차 산업개발이 보다 안정적으로 우리 생활에 파고 들었을 때 가장 눈에 띄는 변화는 폭발적인 수의 IoT 단말이다. 미국 시장조사업체 "주니퍼리서치"에 따르면 2020년에 IoT 단말기가 500억 개를 넘어설 것으로 예상하고 있다. 무수히 늘어나는 단말들을 어떻게 효율적으로 처리할 수 있는지에 대한 네트워크 구조가 결국은 미래 사물인터넷에 대한 해답이 될 것이다.

먼저 인터넷에 연결된 모든 단말이 모두 컴퓨팅 가능한 상태로 운영할 수도 있고, 이를 보다 효율적으로 처리해서 게이트웨이 형식의 거점 기기를 이용하는 방식도 가능하다. 다양한 방법의 네트워크 구성을 위해 에지 컴퓨팅, 분산 에지, 포크 컴퓨팅 등 다양한 방법들이 제안되고 있지만 500억 단말의 수를 효율적으로 처리하기 위해서는 자동이 필수적으로 요구된다. 이러한 기술을 제공하는 것이 분산원장기술인 블록체인이다. IoT 단말마다 스마트 컨트랙트 절차를 자동화 하여 사물 간 소통을 하게 함으로써 보다 효율적인 문제 처리가 가능하게 된다. IoT가 블록체인 기반으로 대중화되기 위해서는 이러한 단말의 처리를 위한 확장성, 보안성, 성능이 필수적으로 요구된다. ETH 2.0 기반에서는 이를 모두 반영한 새로운 플랫폼을 제시하게 되었다.

Ⅳ. 결론

미래의 산업구조 핵심은 엄청난 수의 사물간의 효율적인 소통이다. 이것은 결국 사물인터넷 시대에 데이터처리의 단말 처리 능력을 극대화 시킬 수 있느냐의 문제이고 이를 위한 해답은 확장성과 보안성이 보장된 블록체인 기술과의 결합에 있다.

확장성과 보안성이 보장된 ETH 2.0의 등장은 현재진행형이고 늘어나는 IoT 단말수도 예측에 불과하므로 향후 보다 치밀하게 다양한 상황에 대비하여야 한다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2019-0-00708, 뉴로모픽 아키텍처 기반 자율형 IoT 응용통합개발환경).

This work was supported by Institute for information & communications Technology Promotion(IITP) grant funded by the Korea government (MSIT) (No. 2019-0-00708, Integrated Development Environment for Autonomic IoT Applications based on Neuromorphic Architecture).

References

[1] Banafa, Ahmed, "IoT and blockchain convergence: benefits and challenges," IEEE Internet of Things (2017).

[2] Liang, Xueping, et al. "Towards data assurance and resilience in IoT using blockchain," MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017.

[3] Novo, Oscar, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet of Things Journal* 6.3(2018):4694-4701.