

사물인터넷과 블록체인 융합에 관한 연구

이용주* · 우성희**

*충북대학교, **한국교통대학교

Research for the convergence of IoT and Blockchain

YongJoo Lee* · Sung-Hee Woo**

*ChungBuk National University, **Korea National University of Transportation

E-mail : *silvianna7@naver.com, **shwoo@ut.ac.kr

요 약

최근 사물인터넷 기술에 관한 연구가 활발히 이루어지고 있는 가운데, 기존 중앙 집중형 운영에서의 문제점으로 지적되는 사물인터넷 서버 측 부하와 보안의 취약성을 극복하고자 블록체인의 도입에 관한 연구가 요구되고 있다. 본 논문에서는 사물인터넷의 진화에 따른 네트워크의 구조 변화와 이로 인한 문제점을 분석하고, 이를 해결하기 위한 방안으로 블록체인과의 융합을 제안하기 위해 융합을 위한 네트워크 도메인을 제시한다. 또한 사물인터넷과 블록체인의 융합으로 얻어지는 장점과 다양한 응용분야에 대해서도 기술한다.

ABSTRACT

Recently, the research for IoT technologies has been established actively, however the structure of centralized network has been pointed out as the vulnerable points. To solve these problems such as system load and security vulnerability, the research to introduce block chain technology is needed. In this paper, we propose the network domain for convergence of block chain and IoT platform, and describe the advantages from the convergence and various and applicable fields.

키워드

IoT, BlockChain, Security

I. 서 론

4차 산업의 핵심 기술로 여겨지는 사물인터넷, 클라우드, 빅데이터에 관한 연구가 활발하게 진행되어 지고 있는 가운데, 과거의 전통적인 중앙 집중형 특징으로부터 발생하는 문제를 해결하기 위한 연구의 필요성이 제기 되고 있다. 수 백 만개에 이를 것이라고 예측되는 디바이스의 연결을 감당할 수 있는 중앙 집중형 구조의 서버부하와 보안의 취약점이 가장 시급한 문제로 대두 되면서, 이러한 문제를 해결해 줄 수 있는 분산 장부 기술 기반의 블록체인의 도입을 위한 연구가 활발히 진행 되고 있다. 본 논문에서는 사물인터넷의 향후 발전 방향에 대해 분석하고 이로 인해 발생하는 문제점을 극복하기 위한 방안으로 블록체인의 융합을 위한 도메인 모델을 제안한다. 또한 이러한 융합으로 얻을 수 있는 장점과 응용 분야에 대해서도 기술한다.

II. 본 론

1. 사물인터넷

사물인터넷은 소형 하드웨어와 무선 네트워크 기술의 발전으로 미래를 바꿀 기술로 각광 받고 있으나 제한된 플랫폼으로 인해 확장성이 부족하고 보안에 취약한 점이 그동안 단점으로 지적되었다. 그러나 여전히 4차 산업혁명의 근간에는 사물인터넷이 있다고 해도 과언이 아닐 만큼 사물인터넷은 각종 정보통신 기술 융합의 중심에 위치하고 있다. 현재 사물인터넷 기술은 발전하는 과도기에 있으나 기술의 성숙기에 들어서는 2020년 경에는 디바이스간의 연결이 P2P 구조가 되면서 구성원 모두가 동등한 지위가 되어 계층 구조가 완화되게 된다. 이에 시스템 구축 및 유지비용이 절감하게 되고 게이트웨이와 같은 별도의 추가 장비 없이도 새로운 사물인터넷 디바이스가 시스템에 참여할 수 있게 된다. 그림1은 이러한 사물인터넷 구조의 진화를 보여주고 있다.

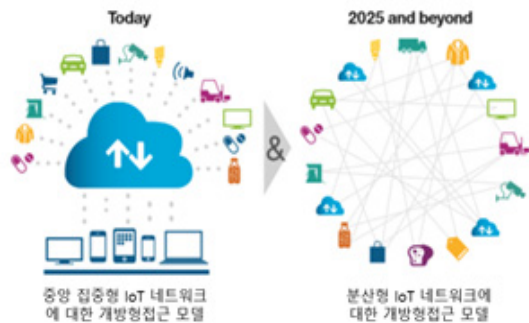


그림 1. 미래의 분산형 사물인터넷 모델

개별 사물인터넷 디바이스들은 보안에 취약하며 그간 디바이스를 공격하여 시스템까지 공격하는 사례가 있어왔다. 또한 사물인터넷 플랫폼에 연결되는 수많은 디바이스들을 어떻게 효율적으로 관리할지가 중요한 이슈였다. 그러나 사물인터넷과 블록체인이 융합된 네트워크에서는 다양한 장비의 이용내역이나 거래내역을 기록하는 방법이 간단하게 해결되며, 분산된 데이터를 가지는 환경에서는 사물인터넷 디바이스 하나만 공격하는 것은 의미가 없으므로 보안성에 대해서도 큰 장점이 있다. 즉 시스템 일부에 문제 생기더라도 전체 시스템은 대체로 안전하며 영향이 적어 사물인터넷과 블록체인을 융합하려는 시도가 다양해지고 있다.

2. 블록체인

블록체인은 피어-피어 환경에서 안전한 데이터 저장을 제공하는 기술이다. 블록체인 기술을 이용한 대표적인 응용이 암호화폐인 비트코인이며 기존 서버-클라이언트 구조의 중앙 집중형 통화발행 및 관리방식이 아닌 인터넷 환경에서 은행과 같은 제 3자의 개입이 없고, 사용자간 신뢰 관계가 없이 안전하게 암호화폐 거래가 가능하도록 개발되었다. 즉 관리하는 중앙 기관 없이 피어-피어 네트워크 환경에서 사용자 간 직접적인 암호화폐를 통한 안전한 거래를 제공한다. 이러한 기능을 가능하게 하는 블록체인의 특징은 크게 두 가지로 살펴 볼 수 있다. 첫째는 시간별로 블록이 정리되어진다. 한 블록에는 앞의 블록과 뒤의 블록을 연결하는 연결정보가 포함되어 있으며, 앞 블록의 내용을 변경하면 뒤에 이어지는 모든 블록을 다시 생성해야 한다. 따라서 과거 블록의 내용을 조작하는 것은 어렵다. 반대로 과거 시점의 거래 기록이 존재한다면 그것은 그 시점에 거래가 이루어졌다는 것을 객관적으로 알 수 있고 이러한 특징은 변조의 공격을 막아 무결성을 제공한다. 두 번째 중요한 특징은 분산 원장이다. 블록체인 네트워크에 참가한 모든 사람이 모든 거래 기록을 기록한 원장을 소유하기 때문에 거래의 투명성이 높다는 것이 특징 중 하나이며 거래를 관리하는 중앙 시스템이 없어 탈중앙화가 가능하다. 그림2는 이러한 블록체인의 동작원리를 보여준다.

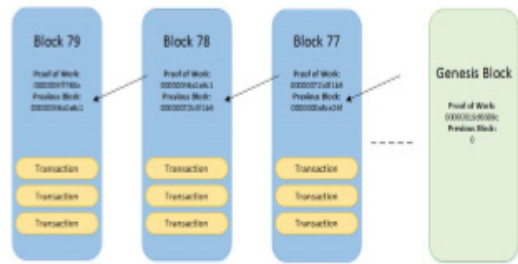


그림 2. 블록체인의 동작원리

비트코인 블록체인에 참여하는 사용자들은 거래를 작성하고 자신의 개인키로 거래에 서명한다. 작성된 거래들은 다른 사용자들에게 브로드캐스팅하여 전달하고, 합의과정에서 특정 합의 알고리즘을 통해 거래들을 하나의 블록으로 생성한다. 생성된 블록은 기본 블록체인에 연결되게 되고, 블록의 정보는 다른 사용자들에게 브로드캐스팅한다. 사용자들은 블록체인에 연결된 블록의 정보들을 바탕으로 중앙 시스템 없이 사용자들 간에 데이터의 신뢰성을 확인할 수 있다. 블록체인의 종류는 크게 세가지로 나눌 수 있다. 첫째는 공용형으로 노드형과 블록체인에 제한이 없으나 이를 위해 블록 생성시에 높은 나이도를 요구하는 단점이 있다. 개인형은 단일 조직에서 이용하기 좋으며 이때는 노드형과 블록체인에 제한을 두고 블록생성과 마이닝에 대한 보수도 정책에 따라 조절할 수 있다. 마지막으로 컨소시움형은 여러 개의 블록체인이 협업하는 형태로 엔터프라이즈 이용은 컨소시움형이 될 것으로 보인다. 현재 가장 보편적인 블록체인기술로 알려진 이더리움은 비트코인과 비슷한 전자화폐 기능을 가지고 있지만 프로그램 확장 기능이 구현돼 있기 때문에 보다 넓은 분야에서 활용할 수 있다. 하지만 기능적으로 참가자를 제한하는 구조는 없기 때문에 컨소시움형으로 적용하기에는 제한이 있다. 반면에 Hyperledger Fabric은 컨소시움형에 특화된 몇안되는 블록체인 기반기술로 공용형의 문제인 PoW의 파이널리티 불확실성을 해결하고 PBFT 등 합의 알고리즘으로 교환가능하며 속도에는 이점이 있다. 또한 공용형에는 없는 권한형 네트워크 때문에 보다 중심적인 용도로 사용할 수 있다.

3. 사물인터넷과 블록체인의 융합도메인

사물인터넷 플랫폼의 네트워크는 크게 디바이스들이 M2M 통신으로 연결되는 M2M 디바이스 도메인과 사물인터넷 플랫폼, 클라우드 등의 서버 등이 위치한 네트워크 도메인, 그리고 서비스 어플리케이션이 위치한 어플리케이션 도메인으로 이루어진다. 블록체인과 사물인터넷의 융합으로 블록체인은 사물인터넷 플랫폼과 같은 레벨의 기능을 수행하는 네트워크 도메인에 위치할 수 있다. 그림3은 이러한 융합 환경에서 도메인 구조를 보여준다.

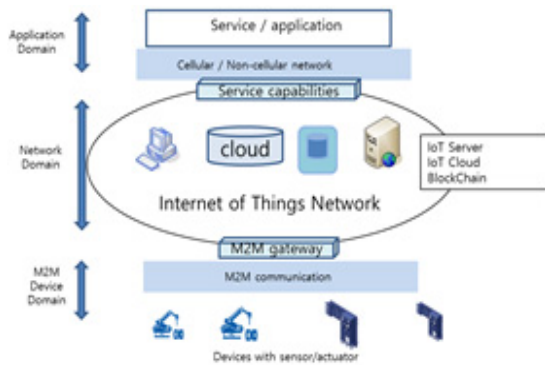


그림 3. 사물인터넷과 블록체인의 융합도메인

사물인터넷과 블록체인이 융합된 구조에서 각 노드는 동등한 권한을 가지고 리소스를 교환하며 거래를 할 수 있고, 기밀성과 무결성이 보장된다.

따라서 블록체인 서버는 수평적 레벨에서는 클라우드와 사물인터넷 서버와 통신하며 필요한 내용을 공유하고 수직적 레벨에서는 디바이스 도메인과 어플리케이션 도메인의 엔티티들과 통신을 하게 된다. 이로 인해 기존의 사물인터넷 응용에서 제약이 많았던 다양한 분야로의 진출이 활발해 질 것으로 예상되는데 그중에서도 보안성이 강화된 분산 환경에서의 응용이 주를 이룰 것으로 예상된다.

4. 융합도메인으로 인한 서비스 변화

사물인터넷과 블록체인의 융합으로 제공되는 보안기능과 분산 환경으로 인해 다양한 분야로의 응용이 가능하게 한다. 기존에 사물인터넷 환경에서는 사물에 연결된 디바이스의 각 센서가 수집한

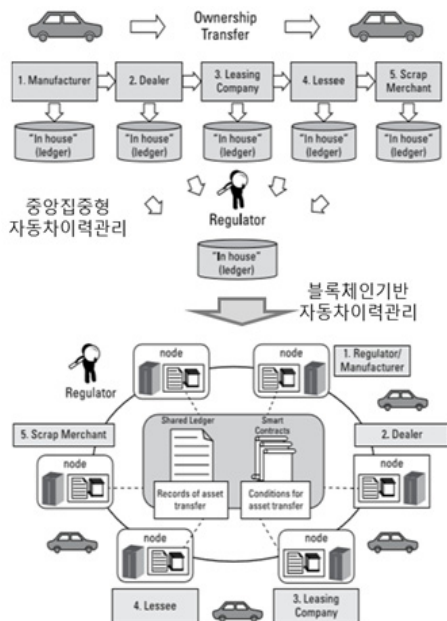


그림 4. 사물인터넷과 블록체인의 융합으로 인한 응용서비스 변화

빅데이터를 활용하는 수준에 그쳤다. 예를 들어 차량의 센서가 수집한 데이터를 렌터카 업체에서 활용할 수 있고, 보험 회사나 결제 기능이 필요한 서비스와의 연계도 가능하다. 중고차 이력 관리 서비스의 경우에는 중고차에 대한 이력을 번조 없이 관리하여 신뢰성 있는 이력을 제공할 수 있다. 그림 4는 이러한 융합 환경에서의 서비스 제공의 변화를 보여준다.

사물인터넷과 블록체인의 융합으로 현재 4차 산업의 핵심 기술인 인공지능 빅데이터와 연계하여 무인자동차, 3D프린터, 가상현실, 지능형 드론, 지능형 로봇 등의 신성장 산업에 효율성을 제공하고 신뢰성을 강화할 수 있다.

III. 결 론

본 논문에서는 현재 활발하게 연구되고 있는 사물인터넷 플랫폼의 미래 구조에 대해 살펴보고 이로 인해 발생가능한 문제점들을 분석하여 이를 보완하기 위한 방안으로 블록체인과의 융합 모델에 대해서 다루었다. 사물인터넷 플랫폼과 블록체인의 융합으로 보안 기능뿐만 아니라 시스템의 신뢰도 등을 향상시킬 수 있어 다양한 응용에 활용 되고 4차 산업 혁명의 인프라로 자리 잡을 것으로 예상된다.

참고문헌

- [1] 박병주 외 2인, "블록체인 기반 IoT 디바이스 인증스킴", Journal of the Korea Institute of Information Security & Cryptology, Vol.27, No2, Apr, 2017.
- [2] 이성범 외 3인, "블록체인 시스템의 보안성 분석:암호화폐에서의 사례연구", Journal of the Korea Institute of Information Security & Cryptology, VOL.28, No1, Feb.2018.
- [3] 최종석 외 3인, "블록체인 기반 탈중앙화 사물인터넷 플랫폼 연구", 정보보호학회지, 제27권 제6호, 2017.
- [4] M.Gupta, "Blockchain" IBM Online(<http://www.IBM.COM>)