한국정보전자통신기술학회논문지(jkiiect)'18-12, Vol.11 No.6
논문 18-11-06-718 http://dx.doi.org/10.17661/jkiiect.2018.11.6.718

DApp 개발을 위한 블록체인 2.0 이더리움 플랫폼 분석 연구

김 순 곤*

A Study on the Blockchain 2.0 Ethereum Platform Analysis for DApp Development

Soon-Gohn Kim*

요 약 최신 컴퓨터 네트워크 기술과 IoT 기술을 융합하여 의료 사물 인터넷(Internet of Medical Things; IoMT) 환경에서 건강관리 및 모니터링과 같은 원격의료(telemedicine)는 양질의 의료정보 서비스 제공을 통해 삶의 질 향상, 의료비용과 의료기관 혼잡도 감소, 의사와 환자간 정보 공유 및 의사소통 향상 등의 긍정적 요소가 크게 부각되고 있다. 본 논문에서는 블록체인과 관련된 연구 및 블록체인을 적용한 플랫폼에 대해 알아보고 이를 비교 분석하여 제품 유통 탈중앙화 DApp 개발한 결과를 제시하였다. 이 과정에서 기존 제품 유통 순서도에 블록체인 기술을 응용하여 상품 사기 파악, 데이터 관리, 고객 관리, 상품 정보의 위조, 변조 방지, 거래 이력 추적 등을 할 수 있고 제품 거래를 원활히 할 수 있게 하는 유통 DApp 개발을 통해 이더리움 플랫폼의 동작 운영 과정을 검증하였다.

Abstract In a positive Internet of Medical Things (IoMT) environment, by combining the latest computer network technology with IoT technology, remote health care such as health care and monitoring is improved through the provision of quality medical information services. In this paper, we identified and compared the platforms applied with blockchain and presented the results of developing the product distribution de-centralized DApp. In the process, we developed a distribution platform that can use blockchain technology to identify product fraud, manage data, manage customers' information, prevent forgery, track transaction history, and facilitate product transactions.

Key Words : Blockchain, Ethereum, Smart contract, Blockchain-based IoT, DApp

1. 서론

블록체인 기술의 발달에 따라 은행, 기업, 기관, 정부 등의 중앙 집중적인 제 3자의 보증 없이도 당사자끼리 직접 신뢰할 수 있게 해주는 블록체인 위에 스마트 컨트랙트를 추가하여 실행할 수 있게 해주는 DApp이라는 개념이 출현하였다[1]. 최신 컴퓨터 네트워크 기술과 IoT 기술을 융합하여 의료 사물 인터넷(Internet of Medical Things; IoMT) 환경에서 건강관리 및 모니터링과 같은 원격의료(telemedicine)는 양질의 의료정보 서비스 제공을 통해 삶의 질 향상, 의료비용과 의료기관 혼잡도 감소, 의사와 환자간 정보 공유 및 의사소통 향상 등의 긍정적 요소가 크게 부각되고 있다[2]. 더불어, 원격의료시 제공되는 개인의 건강 정보 보호, 위변조 방지 등을 위한 고수준의 기술 도입 필요성이 매우 필요한 상황이며 이를 위해, 블록체인 기반 사물 인터넷(Blockchain-based IoT; BIoT) 기술이 적극적으로 연구 및 도입되고 있다[3].

이더리움(ethereum)은 2013년 Thiel Fellow인 Vitalik Buterin에 의해서 제안된 후 2015년 중순에 첫 공개된 후 많은 찬사를 받으며 단기간에 두 번째로 규모가 큰 가상화폐로 자리매김하

This Paper was supported by Joongbu University Research & Development Fund in 2018.
* Corresponding Author : School of Software Engineering, Joongbu University (sgkim@joongbu.ac.kr)
Received December 04, 2018 Revised December 12, 2018 Accepted December 17, 2018

였으며 비트코인이나 타 가상화폐와는 다르게 스마트 컨트랙트(smart contract)라는 개념을 접목했다는 부분이 이더리움의 성공에 큰 영향을 주었다[4]. 1994년 암호학자 Nick Szabo에 의해 처음으로 제안된 스마트 컨트랙트를 블록체인에 접목시킴으로써 이더리움은 기본적인 거래장부(ledger) 기록 외에 튜링 완전한 컴퓨팅 기능과 그 기능을 이용하여 프로그램을 실행할 수 있는 환경을 제공하였지만 소개된지 3년도 되지 않아 엄청난 성공을 했지만 DAO Attack, OPCODE Computational DDOS Attack 등의 공격을 당하기도 하였고 타 블록체인에 비해 복잡한 구조로 인해 아직까지도 많은 공격을 받고 있는 중이다[5].

본 논문에서는 블록체인과 관련된 연구 및 블록체인을 적용한 플랫폼에 대해 알아보고 이를 비교 분석하여 제품 유통 탈중앙화 DApp 개발한 결과를 제시하였다. 이 과정에서 기존 제품 유통 순서도에 블록체인 기술을 응용하여 상품 사기 파악, 데이터 관리, 고객 관리, 상품 정보의 위조, 변조 방지, 거래 이력 추적 등을 할 수 있고 제품 거래를 원활히 할 수 있게 하는 유통 DApp 개발을 통해 이더리움 플랫폼의 동작 운영 과정을 검증하였다.

2. 연구배경 및 관련연구

기존의 화폐는 중앙 집중 방식을 사용하여 화폐를 관리 및 보증을 수행했지만 중앙 집중 방식에 대한 신뢰성이 떨어지자 그림1과 같이 화폐 관리 방식을 화폐를 이용하는 모든 사람이 화폐의 관리와 보증에 참여하는 분산 방식을 사용하는 새로운 화폐인 비트코인이 제안되었다[6]. 비트코인이 만들어지면서 거래 장부(ledger)인 블록체인도 만들어졌고, 블록체인의 가장 중요한 특징은 분산 네트워크이며 관리하는 중앙에서 관리하는 노드가 없이 일반 단말(terminal) 노드로만 구성되어 있으며, 블록들이 체인처럼 서로 연관성을 가져 데이터의 보안성을 유지할 수 있다. 또한 각 노드는 P2P 방식으로 다른 노드들과 연결하여 그물 모양의 네트워크를 구성하며 모든 노드는 거래를 요청할 수 있다. 네트워크의 노드들의 거래 장부 단위에는 블록이라는 데이터 구조를 서로 주고받으며 거래를 요청하고 화폐의 정당성 확인 및 네트워크 관리 역할을 수행한다. 블록은 해당 블록의 정보를 담는 헤더와 거래라는 데이터가 담긴 페이로드로 구성되어 있다.

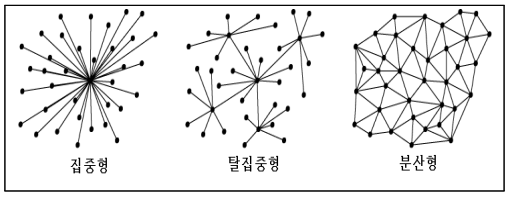

그림 1. 이더리움 네트워크 분산 구조
Fig. 1. Ethereum Network Distributed Structure

블록체인은 네트워크에 참여한 모든 노드가 네트워크를 이용 및 관리를 하며, 첫 블록부터 현재까지 생산된 블록이 체인처럼 연관성을 가지기 때문에 보안성이 높으며 흐름도 파악할 수 있어 안전한 거래가 가능하다. 또한 비트코인 주소는 바로 돈과 직결되기 때문에 64진수에서 혼돈할 만한 문자와 비교하여 0(영), O(대문자 o), I(대문자 i) 및 l(소문자L)이나 필요없는 연산자 +,/를 제거한 58진수가 된다.

Mithril 플랫폼[7]은 모바일 게임 광고 시장의 수많은 중개인을 제거하고 게임 플레이 데이터를 기반으로 게임 개발사와 게이머를 직접 연결해 광고 효율을 획기적으로 개선하는 것을 목표로 하는 플랫폼이다. 게이머의 동의를 얻어 게임 플레이 데이터를 수집하는 모바일 앱으로 데이터를 제공하는 조건으로 암호 화폐 MTR를 받는다. 게임 데이터가 쌓일수록 게이머는 더 많은 MTR를 확보할 수 있으며 게임사로부터 VIP 초대장을 받을 수 있다. 보유한 MTR은 현금화하거나 게임 아이템의 구매 및 게임 크라우드펀딩 투자에 사용할 수 있다.

Steemit 플랫폼[8]은 스팀 서클체인 데이터베이스를 기반으로 한 블로그 및 소셜 네트워크 웹

사이트다. 스팀 블록체인이 스팀과 스팀 달러라는 것을 만들어내고 스팀 달러는 매직 빈 토큰으로 포스팅을 하고 뭔가를 발견하면 재미있는 컨텐츠를 생산해내면 되는 플랫폼이다. 스팀 코인이라는 블록체인에 기반한 토큰, 즉 스팀이라는 이름의 가상화폐를 벌 수 있는 구조로 글에 대한 보상으로 제공한다.

OmniJoin[9]은 환자와 의료 서비스 제공업체가 편안하고 안전한 온라인 환경에서 연결할 수 있도록 도와주는 원격의료 시스템으로서 안전한 클라우드 기반 화상회의, 건강관리 공급자가 HIPAA 준수를 유지하면서 편안하고 쉽게 액세스 할 수 있는 서비스로 응용범위를 확장하면서 개인적이고 수준 높은 보살핌 서비스를 지원하고 있다. OmniJoin을 통해 원격의료 서비스 신청자는 의료상담을 용이하게 하는 문서 및 이미지를 전송하고 공유 할 수 있으며 OmniJoin은 온라인 대기실을 제공하여 대기중인 신청자와 의료 및 건강관리 전문가를 만날 수 있는 가상 대기실을 생성한 후 OmniJoin은 MPEG4를 사용하여 비디오 인코딩 및 디코딩을 수행하고 고객이 H.264를 선택할 수 있도록 하였으며, iOS 및 Android용 모바일 기반 어플리케이션 제공되는 특징을 가지고 있다.

Al-Taee et al.[10]은 당뇨 관리를 위해 의료센서와 휴머노이드 로봇을 통합하여 e-헬스 플랫폼 개발로서 IoT와 Web-of-Things 개념을 도입하여 혈당 모니터, 혈압 모니터 및 체중계와 같은 의료센서는 블루투스를 통해 로봇에 연결되며 휴머노이드 로봇과 의료용 센서의 통합으로 특히, 어린이 당뇨병 치료에 다차원적 치료가 가능한 특징을 가지고 있다.

Jang-Jaccard[11]는 원격진료를 위해 WebRTC[12]라는 웹 실시간 통신을 이용하는 프레임워크를 제안하였으며, WebRTC는 개발자가 화상회의 시스템을 웹 브라우저에 직접 구축할 수 있다. 두 시스템 모두 WebRTC 호환 브라우저가 브라우저간에 직접 비디오, 오디오 및 데이터를 교환하는 장점을 가지고 있으며, WebRTC는 P2P 연결 및 NAT(Network Address Translation) 탐색 기술을 지원한다. 또한 강력한 보안 아키텍처가 포함되어 있어 개인 건강정보를 보호하고 관리하기 위한 의료 서비스에 적합하며 의사와 환자는 다양한 유형의 네트워크에서 안전하게 연결할 수 있고 WebRTC 엔드 포인트는 환자의 생체신호를 모니터하는 센서의 게이트웨이 역할을 수행하는 중요한 기술적 특징이 있다.

3. 유통 DApp 설계 및 구현

3.1 전체 시스템 구성

전체적인 DApp의 시스템은 Back-End 시스템 사양으로 Solidity, Truffle FrameWork, API, 라이브러리 등은 계약을 작성하는 곳에서 필요하며 제품 구매, 등록, SOT 환전, 암호 화폐 상품운영 등 Back-end에서 모든 것을 구현한 후에 JavaScript를 이용하여 UI와 연동하여 E-bay같은 시스템을 완성하였다.

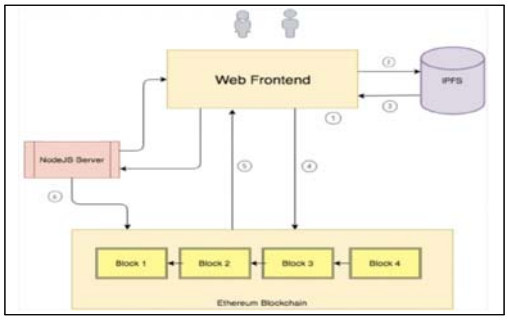

그림 2. DApp 전체 시스템 구조
Fig. 2. DApp Overall System Structure

실제로 그림2와 같은 DApp 웹구조에서 Front-end에는 HTML폼이 있어서 사용자가 이름, 가격, 이미지, 설명 등의 상품 정보를 직접 입력하고 저장할 수 있고 상품 정보와 이미지를 IPFS에 올리고 그 링크를 연결한다. 또한 컨트랙트를 호출하여 IPFS의 상품 링크를 블록체인에 저장한다. 상품을 블록체인에 올리는데 성공하면 컨트랙트가 이벤트를 하나 생성하고 이 이벤트는

모든 제품 정보를 저장하게 된다.

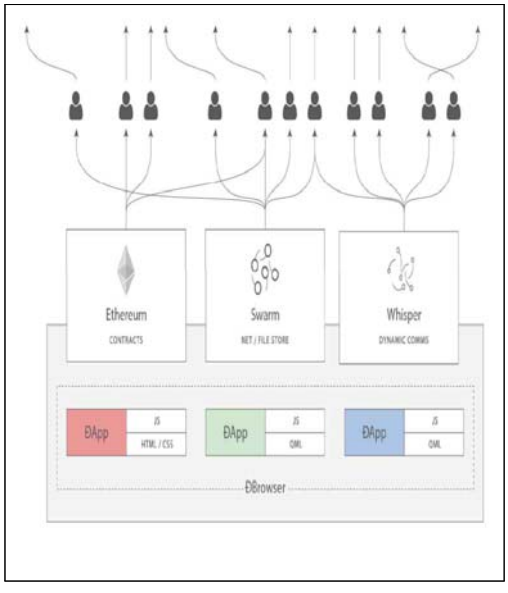

그림 3. 이더리움내의 분산어플리케이션 구조
Fig. 3. DAPP Structure on the Ethereum Platform

node.js 서버에서 이러한 이벤트를 모니터링 하고 컨트랙트가 이벤트를 생성하면 이벤트의 내용을 읽어서 Mongo DB 데이터베이스에 상품 정보를 입력한다. 일반적인 제품의 유통 구성도는 그림 3과 같이 되어 있으며 본 o논문에서도 이를 기반으로 주문, 결제, 제품 생산들 모두에 블록을 이용하여 사용하는 방식으로 바꿔서 기존 유통업 어플과의 차이점을 두었다.

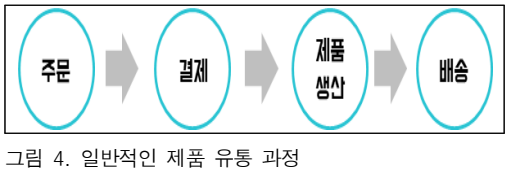

그림 4. 일반적인 제품 유통 과정
Fig. 4. General Goods Distribution Procedure

4.2 시스템 구현 결과

그림 5. 전제 시스템 메인 페이지
Fig. 5. Overall System Main Page

그림 5의 메인 페이지에서는 제품의 구입 가능한 제품여부를 확인할 수 있으며, 제품을 등록할 때의 판매자의 디테일한 정보들도 블록 안에 저장되어 있어서 안전성과 신뢰성도 높다.

그림 6의 제품 등록 페이지는 제품을 등록할 수 있는 페이지이며 제품을 등록할 때는 블록으로 저장하여 등록하기 때문에 보안성이 높다.

그림 6. 제품 등록 및 업로드 페이지
Fig. 6. Goods Registration and Upload Page

그림 7의 제품 디테일 페이지는 제품의 정보를 볼 수 있는 페이지로 판매자가 올려돈 정보를 구매자가 볼 수 있다.

그림 7. 제품 정보 페이지(구매전)
Fig. 7. Goods Information Page(Before Buying)

그림 8의 제품 디테일 페이지는 제품을 구매한 후에 E-Bay 시스템과 유사한 에스크로 서비스(이더를 판매자에게 바로 보내는 것이 아닌 일종의 구매자 보호 정책(2-of-3 멀티시그 에스크로 컨트랙트)을 이용하여 보내게 된다.

그림 8. 제품 정보 페이지(구매후)
Fig. 8. Goods Information Page(After Buying)

2-of-3 멀티시그 에스크로 컨트렉트란 세 명 중 두 명이 동의해야 이더를 판매자에게 전송하거나 구매자에게 환불하는 행위가 승인된다는 내용이다. 여기서 세명은 구매자, 판매자, 중계자를 뜻하고 중재자는 관리자를 두어 구매자가 물품에 이상이 있다고 전달되면 중계자가 이더를 받지 못하게 제한하여 제한할 수 있다. 마찬가지로 구매자가 환불을 요청할 때 판매자 물품에는 이상이 없고 악용하려는 구매자가 있을 때 중재자가 동의를 안하면 이더 전송이 발생되지 않기 때문에 안전거래를 유도 할 수 있다. 즉, 에스크로 서비스는 중재자가 구매자와 파매자에게 안전한 거래를 할 수 있게 중재해주는 서비스이다.

4. 결론

본 논문에서는 블록체인과 관련된 연구 및 블록체인을 적용한 플랫폼의 특징을 고찰한 후 제품 유통 탈중앙화 DApp 개발 결과를 제시하였다. 기존 제품 유통에 더불어 블록체인 기술을 응용하여 상품 사기 파악, 데이터 관리, 고객 관리, 상품 정보의 위조, 변조 방지, 거래 이력 추적 등을 할 수 있고 제품 거래를 원활히 할 수 있게 하는 유통 DApp 개발 결과는 이더리움 플랫폼의 동작 운영 과정을 통해 검증결과를 제시하였다.

블록체인은 현재까지도 연구되고 있고, 다양한 분야에서 응용사례가 나오고 있다. 관련 법규의 부재 및 처리속도, 저장용량 등의 해결해야 할 기술적인 문제도 있지만 DApp의 가치는 비용과 운용효율 면에서 크기 때문에 블록체인의 기술적 발전이 DApp를 다양한 분야에서 활용할 수 있을 것으로 기대된다.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, March 2008.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ``Internet of Things (IoT): A vision, architectural elements, and future directions,'' 'Future Generat. Comput. Syst., vol. 29, no. 7, pp. 16451660, 2013.

[3] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. weusecoins.com. 2014.

[4] Kwang-Man KO, et al., "Decentralized Consensus on Internet of Things: Review, Taxonomy, Open Research Issues," IEEE Access, Volume 6, pp.1513-1524, Feb, 2018.

[5] Tiaco M. Fernandez, et al., “A Review on the Use of Blockchain for the Internet of Things,” IEEE Access, Vol. 6, pp.32979-33001, 2018.

[6] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, ``A survey on Internet of Things from industrial market perspective,'' IEEE Access, vol. 2, pp. 16601679, Jan. 2014.
[7] Mithril, https://mithrilcoin.io/
[8] Steemit, https://steemit.com/
[9] Zastrin, https://kr.zastrin.com/
[10] Al-Taee M. A., Al-nuaimy W., Muhsin, Z.J, Al-Ataby A., "Robot Assitant in Management of Diabetes in Children Based on the Internet of Things," in IEEE Internet of Things Journal, April 2017, pp. 437-445.
[11] Jang-Jaccard J., Nepal S., Celler B., Yan B., "Webrtc-based video conferencing service for telehealth," Computing, vol. 98, no. 1, pp. 169-193, 2016.
[11] WebRTC. (n.d.). Retrieved February 23, 2018, from https://webrtc.org/architecture/.
[12] Soonduck Yoo, Kiheung Kim, 'A Study on Improvement for Service Proliferation Based on Blockchain', The Journal of The Institute of Internet, Broadcasting and Communication VOL. 18 No. 1, 2018

저자약력

김 순 곤(Soon-Gohn Kim) **[종신회원]**

- 전북대학교 일반대학원 전자계산기공학과 졸업(공학박사)
- 동아생명보험(주) 전자계산실 (DBA)
- 한국원자력연구소 핵전산연구부 (선임연구원)
- 중부대학교 소프트웨어공학부 (교수)

〈관심분야〉 데이터베이스시스템, 정보보호암호화응용프로토콜, 정보시스템감리, 데이터마이닝, 유비쿼터스컴퓨팅, 서버장애예측, 소프트웨어시스템분석설계