다양한 블록체인 플랫폼에 적합한 미래 네트워크 요구사항 분석

김수연*, 이창수**, 강현국**
*계명대학교 산학협력단
**고려대학교 전자정보공학과
e-mail : sykim388@gmail.com

The Requirement Analysis for Future Network suitable for various Blockchain Platforms.

Suyeon Kim*, Chang Su Lee**, Hyun K. Kahng**
*Dept. of Industry Cooperation, Keimyung University
**Dept. of E&I Engineering, Korea University

요 약

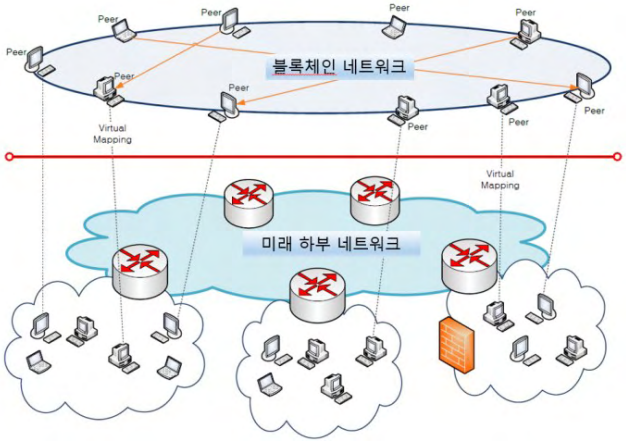
본 논문에서는 최근 혁신적인 거래시스템으로 각광받고있고 앞으로 다양한 응용 플랫폼이 개발될 것으로 예상되는 블록체인 시스템의 안정적인 프로토콜 기능과 효율적 트래픽 운영을 제공하기 위한 하부 네트워크 구조로써 미래 네트워크의 필요 기능과 서비스에 대한 연구를 진행하였다. 이러한 하부 네트워크 구조는 현재 많이 사용되고 있는 인터넷 또는 OSI Reference 모델의 수정된 프로토콜 형태가 아니라 새로 표준화가 진행되고 있는 ISO/IEC JTC1 SC6 의 미래 네트워크 구조에 필요한 서비스 기능을 위한 요구사항을 제시하고자 한다. 가까운 미래 블록체인이 대중화될 때 블록체인의 안정적인 동작과 효율적인 시스템 구성을 지원하기 위하여 하부 네트워크로 사용될 미래 네트워크의 요구사항들을 분석하고 분석된 내용을 바탕으로 앞으로 표준화가 진행될 미래 네트워크의 핵심 서비스 기능으로 제안하고자 한다.

1. 서론

비트코인(Bitcoin)이라는 전자 암호 화폐를 구현하기 위해 처음 제시된 블록체인 기술은 P2P 기반의 네트워크에서 신뢰할 수 있는 중앙 서버의 제어없이 거래가 가능한 시스템으로 4 차 산업혁명의 기반 기술로 관심을 모으고 있다. 최근에는 PC 와 스마트폰을 이용한 O2O(Online to Offline) 거래가 증가하면서 핀테크에 이어 해킹과 위·변조가 불가능한 블록체인 기술을 산업전반에 적용하려는 새로운 비즈니스 모델이 증가하고 이를 위한 다양한 응용프로그램들이 개발되고 있다. 더불어 글로벌 금융기관들은 파트너십 체결을 통해 블록체인 시스템 구축과 표준 개발을 추진하고 있으며 이를 통한 블록체인의 활성화가 전 세계적으로 이루어질 것이라고 예상된다.

그러나 최초로 제시된 블록체인 기술은 비트코인 같은 암호 화폐의 구현 기술로 탄생했기 때문에 데이터 구조나 프로토콜 방법이 범용적이지 못하여 최근에는 다른 영역에서도 적용이 가능하도록 다양한 종류의 블록체인 플랫폼이 만들어지고 있다. 블록체인 시스템은 증권회사, 은행, 거래솔루션기업, O2O 를 포함한 다양한 전자상거래 기업으로 확대되고 있으며, 스타트업을 비롯한 가상화폐 개발자, 핀테크 업체, 정보보호업체, 저작권/소유/등기 기관들이 참여하여 개발을 주도하고 생태계를 구축할 것으로 예상한다.

그러나 현재는 단순히 인터넷 상에서 기존의 망을 이용하여 블록체인 시스템의 운영을 예상하고 있지만 기존 거래 방식과 다른 방식의 다양한 블록체인 플랫폼과 응용 프로그램이 빠른 시간에 도래할 것으로 예상함에 따라 다양한 형태의 블록체인 플랫폼에 적합하고 이를 원활하게 운영할 하부 네트워크에 대한 필요성이 (그림 1)처럼 예상된다.



(그림 1) 블록체인 네트워크의 하부 네트워크 구조

본 논문은 산업통상자원부의 '국가표준기술력향상사업'의 지원에 의해 작성되었습니다.

현재의 네트워크 시스템에서 다양한 블록체인 응용이 도래하여 발생할 수 있는 문제점에 대하여 분석하고 ISO/IEC JTC1 SC6 에서 표준화가 추진중인 미래네트워크의 요구사항에 이러한 문제점과 해결 방법에 대한 내용을 적용한다면 블록체인과 함께 최적의 미래 네트워크가 새로운 플랫폼으로 사용자에게 최적의 거래 시스템을 제공할 수 있을 것이라 생각한다.

이를 위하여 본 논문의 2 장에서는 블록체인 시스템의 간략한 소개 및 현재의 인터넷 망에서 발생할 수 있는 문제점에 대하여 소개하고 3 장에서는 이러한 문제점을 해결하기 위한 미래네트워크의 요구사항을 제시하고 진행 중인 미래 네트워크 표준화에 이러한 요구사항을 적용하기 위한 필요성을 제시한다. 마지막으로 4 장에서 미래 네트워크에 적용할 요구사항에 대한 결론을 제시하고 앞으로의 연구계획을 제시하고자 한다.

2. 블록체인 시스템 소개 및 하부 네트워크에 대한 문제점 분석[1][2][3]

블록체인 시스템을 기반으로 한 비트코인은 중앙집중 형 서버를 중심으로 트랜잭션을 처리하는 기존 방식과는 다르게 일반 노드들이 연결된 P2P 네트워크 상에서 참여자들이 보유한 자원(프로세싱 파워, 디스크 용량, 네트워크 대역폭 등)을 이용하여 트랜잭션이 가능한 시스템으로 혁신적인 기술로 등장하였다. 이러한 블록체인 기반의 비트코인 클라이언트는 누구나 프로그램을 다운로드 받아서 비트코인을 송금하거나 채굴하는 것이 가능하며 특정한 곳에서 사용도 가능하다. 이러한 비트코인은 [표 1]과 같은 흐름도를 가지고 있다.

라이프 사이클	내용
① 계정(계좌) 생성	전자지갑(Wallet) 생성(개인키, 공개키 자동 생성)
② 거래 생성	비트코인 전송
③ 거래 검증	P2P 네트워크에서 거래 전송
④ 블록 구성 및 생성	노드에서 트랜잭션을 블록 생성
⑤ 채굴 및 보상	블록의 정당성 확보를 위한 채굴
⑥ 블록 검증	P2P 네트워크 전파 및 각 노드의 블록 검증
⑦ 블록체인 생성	블록체인 생성(the longest chain)
⑧ 난이도 조정	14일마다 블록 생성 주기 변경

[표 1] 비트코인 거래의 전체 흐름도[4]

[표 1]에서 ①의 계정 생성은 은행 계좌와 동일하게 개인의 계좌를 생성하는 것과 동일하다. 이때 개인키와 공개키가 생성된다. ②의 거래 생성은 공개키를 주소(또는 계좌번호)로 하여 비트코인을 전송하거나 받을 수 있다. ③의 거래 검증은 ②에서 생성된 거래를 주변 노드에게 전달하여 검증을 받게 된다. 이 검증을 통하여 거래가 적정하다 판단되면 다시 전파하고, 거래가 적정하지 않다고 판단되면 그 거래를 삭제하게 된다.

④의 블록 구성 및 생성은 각 노드에서 적정하다고 판단된 거래를 블록 제작을 위한 메모리 풀에 저장한다. ⑤의 채굴 및 보상은 ④에서 메모리 풀에 저장된 거래로 생성된 블록을 합의 알고리즘을 통하여 새로운 블록으로 생성하는 과정이다. ⑥의 블록 검증은 생성된 블록을 주변 노드에게 전달하면 주변 노드로부터 블록의 적정성을 확인하고 전체 노드의 절반 이상이 생성된 블록의 적정성에 동의하면 새로운 블록으로 승인된다.

⑦의 블록체인 생성은 ⑥에서 생성된 블록을 전달받은 노드는 그 블록의 검증을 완료하고 기존의 블록체인에 연결하게 된다. 분산된 데이터 구조이기 때문에 채굴된 블록이 동시에 다른 노드에서 탄생될 수 있어서 네트워크 지연으로 발생하는 블록체인 분기(Forking) 현상이 발생할 수 있다. 실제로 비트코인 에서는 가장 긴 블록체인만 살아 남고 나머지 체인은 짧은 고아 블록으로 사라지게 된다. ⑧의 난이도 조정은 블록의 생성 주기를 10 분 간격으로 조정될 수 있도록 채굴이 어렵게 스스로 발생 확률을 조정한다.

앞의 블록체인 생성 흐름에서 보듯이 블록체인은 분산된 데이터 구조이기 때문에 채굴된 블록이 동시에 서로 다른 노드에서 동시에 탄생될 수 있으며 이러한 블록들이 플랫폼에 참여된 노드들에게 동시 다발적으로 전달되게 되어 분기 현상이 많이 발생할 수 있다. 이러한 분기 현상이 많이 발생할수록 체인에 연결되지 못하는 고아 블록이 많이 발생하여 네트워크의 정체 현상만 발생시키고 대역폭의 낭비를 일으키게 된다. 블록체인에서는 가장 긴 블록 체인만이 살아남는 구조인데 이러한 고아블록은 네트워크의 처리 속도가 느리면 느릴수록 많이 발생하게 된다.

따라서 5G 망이나 미래 네트워크의 근간이 될 빠른 처리 속도를 고려한다면 네트워크 구성 방법에 따라 고아 블록의 생성을 최소화할 수 있을 수도 있다. 그리고 네트워크 사용량에 따라 요금을 부과하여야 하는 경우에도 블록체인의 알고리즘을 좀더 단순화하거나 하부 네트워크에서 플랫폼 별로 대역폭을 잘 관리한다면 네트워크 사용 요금과 컴퓨팅 파워를 절약할 수 있을 것이다. [5]

이처럼 중앙 서버의 제어없이 개별 노드의 안정된 보안 기능으로 블록 체인이 다양한 분야에서 사용될 것으로 예상되지만 블록체인 시스템의 도입으로 인하여 하부 네트워크에 발생할 수 있는 문제점도 묵과할 수 없다. 본 논문에서는 다음과 같은 3 가지의 문제점을 제시하였다.

1) 하부네트워크 측면에서 과도한 트래픽의 발생 가능성: 다양한 블록체인 응용프로그램들이 야기하는 트랜잭션의 전송 및 적정성 확인 과정에서 발생하는 트래픽, 그리고 네트워크내 모든 참여자에게 블록 전송 및 합의 과정을 거치는 블록 적정성 확인 과정의 빈번한 데이터 교환에 따른 다량의 트래픽 발생
2) 분산 제어의 부재: 블록체인의 가입 및 트랜잭션은 누구나 할 수 있어서 일부 노드가 다량의 데이터를 국지적으로 발생시킬 수 있다. 이러한 문제점으로 인하여 망의 부하를 고려한 블록체인 시스템의 트래픽 제어를 할 수 없음.
3) 망 자원의 공정성 부여: 블록체인 시스템에서 컴퓨팅 자원을 많이 가진 사람이 블록 생성을 독점

하게 되어 컴퓨팅 자원의 불균형에 따른 네트워크 대역폭 사용의 불공정성이 발생함.

3. 블록체인 시스템 지원을 위한 미래 네트워크의 요구사항 분석

2 장에서 언급한 블록체인 시스템이 하부 네트워크에 일으킬 수 있는 문제점 외에 다수의 문제가 더 발생할 소지도 있지만 본 논문에서는 위의 3 가지 문제에 따른 미래 네트워크의 요구 사항에 대하여 검토하고자 한다.

이미 ISO/IEC JTC1 SC6 에서는 블록체인을 비롯한 다양한 상위의 응용 프로그램을 지원하기 위한 하부 네트워크 구조에 대한 연구를 진행하고 있으며 예상되는 요구사항을 바탕으로 표준화가 진행 중이다. 미래네트워크의 요구사항에 대한 세부적인 내용은 TR 29181 문서에서 정의가 되어 있으며 이를 바탕으로 ISO/IEC 21558 미래 네트워크 구조에 대한 표준화와 ISO/IEC 21559 미래 네트워크에 대한 프로토콜과 메커니즘을 표준화하고 있다.[6][7]

ISO/IEC 21558 미래 네트워크 구조 문서는 [표 2] 와 같은 영역으로 세분화되어 구성되어 있다.

문서번호	제목
ISO/IEC 21558-1	Part 1: Overview and high level architecture
ISO/IEC 21558-1	Part 2: Naming and Addressing
ISO/IEC 21558-1	Part 3: Switching and Routing
ISO/IEC 21558-1	Part 4: Mobility
ISO/IEC 21558-1	Part 5: Security
ISO/IEC 21558-1	Part 6: Media Transport
ISO/IEC 21558-1	Part 7: Service Composition
ISO/IEC 21558-1	Part 8: Quality of Service
ISO/IEC 21558-1	Part 9: Networking of Everything

[표 2] 미래 네트워크 표준화 영역

블록체인 시스템의 원활한 운영을 위하여 하위 계층에 속하는 미래 네트워크의 요구사항을 분석하면 다음과 같다.

1) 트래픽 제어의 필요성: 각 노드에서 발생하는 블록의 정보를 측정하여 트래픽을 제어하고 망에 과도한 트래픽이 발생하지 않도록 조정할 필요가 있는데 이러한 트래픽 조정을 위하여 Part 3 의 라우팅 구성시에 블록체인의 체인 유효성 검증을 위한 트리 구성을 고려하여 미래 네트워크의 라우팅 프로토콜을 고려할 필요가 있다.
2) 효율적인 블록체인 시스템을 구성할 수 있도록 서비스되는 블록체인 응용 별로 효율적인 네트워크를 구성하고 하부 망에서는 이를 지원한다. 이를 위하여 고아블록의 생성을 최소화하도록 네트워크의 구성이 이루어지게 하고 고아블록이 많아 만들어지면 네트워크를 재구성할 수 있도록 한다.
3) 정당한 방법으로 하부 망은 컴퓨팅과 망 자원의 사용량을 파악하고 많은 자원을 사용하는 노드를 제어하고 자원을 공평 배분하여 망 트래픽의 공정성을 유지하게 한다. 특정 플랫폼의 특정 노드에서 트래픽을 과도하게 사용한다면 Part 8 의 QoS 의 값을 조정하여 트래픽의 사용을 대가에 비례하여 사용할 수 있도록 조정한다.
4) 블록체인시스템의 안정적 운영을 위하여 하부망은 안정성과 견고함을 제공함 필요가 있다. 블록체인 응용이 다양해지고 발생하는 트랜잭션의 수가 기하급수적으로 증가할 것으로 예상됨에 따라 변화하는 블록체인의 트래픽 양에 따라 하부 망이 안정적으로 유지될 필요가 있는데, Part 2 의 Naming 기법과 Part 3 의 스위칭 기법에 많은 노드가 참여하고 트래픽 관리가 원활하도록 구성하여야 한다.

4. 결론

앞으로 블록체인 기술은 다른 영역에서도 적용이 가능하도록 다양한 종류의 블록체인 플랫폼 형태로 만들어질 것이다. 블록체인 시스템은 증권회사, 은행, 거래솔루션기업, O2O 를 포함한 전자상거래 기업으로 확대되고 있으며 다양한 개발 기관들이 참여하여 새로운 생태계를 구축할 것으로 예상한다. 따라서 본 논문에서는 다양한 응용 플랫폼이 개발될 것으로 예상되는 블록체인 시스템의 안정적인 프로토콜 기능과 효율적 트래픽 운영을 제공하기 위한 하부 네트워크 구조로써 미래 네트워크의 필요 기능과 서비스에 대한 연구를 소개하였다.

현재의 네트워크 시스템에서 다양한 블록체인 응용이 도래하여 발생할 수 있는 문제점에 대하여 분석하였고 ISO/IEC JTC1 SC6 에서 표준화가 추진중인 미래 네트워크에 이러한 문제점을 해결할 수 있는 요구사항들에 대하여 소개하였다. 본 논문에서 제시한 4 가지의 요구사항을 바탕으로 하부 미래 네트워크가 블록체인 플랫폼에 제공할 서비스를 정의하고 그러한 서비스를 제공하기 위하여 필요한 프로토콜 메커니즘을 표준화하는 것은 지금부터 준비해야 할 일이라고 생각한다. 적합한 하부 미래네트워크가 표준화된다면 블록체인과 최적의 미래 하부 네트워크가 새로운 플랫폼으로 사용자에게 최적의 거래 시스템을 제공할 수 있을 것이라 생각한다.

참고문헌

[1] 김원, “비트코인 블록체인 동작원리 및 진화”, 주간기술동향 1851 호, 2018. 6. 20, pp. 2-15.
[2] 임명환, “블록체인 기술의 활용 동향 분석”, 주간기술동향 1772 호, 2016. 11. 15, pp. 2-14.
[3] Satoshi Nakamoto, “Bitcoin: A Peer-to Peer Electric Cash System”, www.bitcoin.org, 2008. 10. 31.
[4] https://bitcoin.org/en/developer-reference#block-chain
[5] Shin-Gak Kang, Wook Hyun, Changkyu Lee, “Proposed updates to Study Rport of PWI-P2P, “Functional Architecture and Protocols for Managed P2P communications”, ISO/IEC JTC1/SC6/WG7 N154.

[6] ISO/IEC 21558 – Information Technology – Telecommunications and information exchange between systems – Future Network – Architecture
[7] ISO/IEC 21559 – Information Technology – Telecommunications and information exchange between systems – Future Network – Protocols and mechanisms