ETRI

2018
Electronics and
Telecommunications
Trends

블록체인 세대별 기술 동향

Past, Present and Future of Blockchain Technology

박정숙 (J.S. Park, jungsp@etri.re.kr) 고성능컴퓨팅연구그룹 책임연구원
박준영 (J.Y. Park, jyp@etri.re.kr) 고성능컴퓨팅연구그룹 연구원
최선미 (S.M. Choi, sonia@etri.re.kr) 기술경제연구그룹 선임연구원
오진태 (J.T. Oh, showme@etri.re.kr) 고성능컴퓨팅연구그룹 책임연구원
김기영 (K.Y. Kim, kykim@etri.re.kr) 고성능컴퓨팅연구그룹 책임연구원/PL

The explosive interest in block chain, which was triggered by Bitcoin in 2009, is leading to substantial investment and the development of block chain technology. There is no dispute among experts that block chain will be the next generation of innovation. However, despite the high expectations for block chains, the related technology still has certain limitations. In addition to improving issues such as a low transaction throughput, inefficient agreement algorithms, and an inflexible governance structure, it is necessary to solve various problems for commercialization and full-scale spreading owing to the trilemma problem among the scalability, security, and decentralization. Under this situation, identification of the technology characteristics according to the generation is helpful for the development of the core technology requirements and commercialization blueprint in establishing an R&D direction. Therefore, in this article, the development of blockchain technology is divided into generations and analyzed in terms of the operational structure, consensus algorithm, governance, scalability, and security.

* DOI: 10.22648/ETRI.2018.J.330614

*본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음[No. 2018-0-00201, 블록체인(PON 알고리즘) 기반 고신뢰 정보거래 플랫폼 기술 개발].

Ⅰ. 서론

블록체인은 2008년 비트코인의 핵심기술로 활용되며 그 간 개념적 시도에 그치던 전자화폐 관련 기술을 실용 가능한 수준으로 끌어올렸다[1]-[4]. 이후 금융거래 용도 중심으로 제한적 범위에서 응용되다, 2015년 스마트 계약 개념 도입 이후 그 적용 범위가 빠른 속도로 확대되기 시작했다. 최근에는 AI, IoT, 클라우드컴퓨팅, 빅데이터 등 다양한 분야와 융·결합하며 기술, 산업, 서비스 간 경계를 넘어 그 활용 가능성을 확장하는 추세다.

2018년 5월 기준 1,600여 종이던 가상통화 형태의 응용서비스는 10월 2,000여 종을 넘어섰으며[5] 블록체인 및 관련 스타트업에 대한 투자 역시 2017년 약 10억 달러 규모에서 2018년 첫 2개월간 전년 대비 40% 규모인 약 4억 달러가 투자된 것으로 알려지는 등[6] 블록체인이 4차 산업혁명을 견인할 핵심 기술의 하나라는 점에 전문가들 간 큰 이견이 없는 상황이다.

그러나 블록체인에 대한 높은 기대에도 불구하고 관련 기술은 여전한 한계를 갖는다. 낮은 트랜잭션 처리율, 비효율적인 합의 알고리즘, 유연하지 못한 거버넌스 구조 등 개선 이슈뿐 아니라, 확장성·보안성·분산화 간 발생하는 트릴레마(trilemma) 문제로 본격적인 상용화 및 확산을 위해서는 다양한 난제를 해결해야 한다.

따라서 이러한 한계를 극복하기 위한 개발 이슈들이 블록체인 R&D의 핵심 요구사항으로 채택되고 있으며, 수 종의 개발 사례들이 기존 기술 대비 개선점을 특징으로 내세우며 시장에 진출하고 있다. 다만, 많은 사례가 목표와 방향성만을 제시하고 있거나, 개발이 진행 중인 상태로 세부적인 특성들을 직관적으로 파악하기는 쉽지 않다.

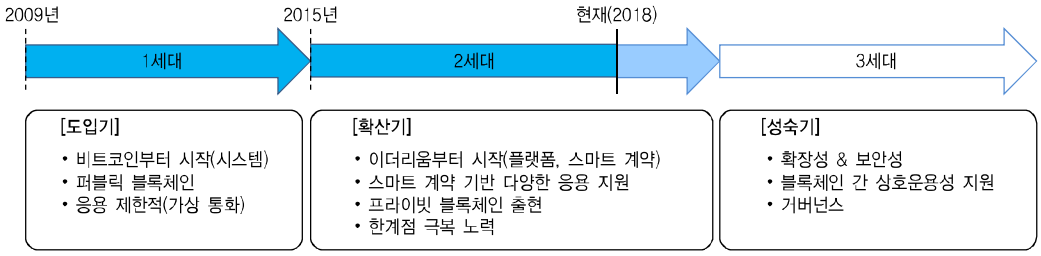
이에 본고에서는 블록체인 기술의 발전을 세대별로 구분하여 운영구조 및 합의 알고리즘, 거버넌스, 확장성 및 보안성 측면에서 사례별로 분석하여 살펴보고자 한다. 본 고에서는 확장성은 트랜잭션 처리 속도(TPS)로 보았고, 거버넌스는 당사자 간 자율적 의사 결정 과정 기능의 유무로 보았다. 기술을 세대에 따라 구분하여 그 특징을 확인하는 것은 R&D 방향 수립 시 기술 개발 핵심 요구사항 도출 및 상용화 청사진의 전망에 도움이 된다. 세대 구분을 위한 기준이 표준화된 상황은 아니나 기술 발전에 확연한 혁신이 있을 때 전 세대와 구분하는 통상적인 방법을 따랐다.

본고의 내용은 다음과 같다. 제 Ⅱ장에서는 블록체인 기술의 세대별 특징과 각 세대를 대표하는 블록체인 기술을 소개한다. 제 Ⅲ장에서는 블록체인 기술의 현황을 몇 개의 대표적 사례들을 통하여 살펴본다. 제 Ⅳ장에서는 향후 블록체인 기술의 발전 방향을 전망하고, 마지막으로 제 Ⅴ장에서 본고의 결론을 맺는다.

Ⅱ. 블록체인 기술의 세대별 특징

블록체인 기술을 세대별로 구분하여 주요 특성을 요약하면 (그림 1)과 같다[7].

현재의 블록체인 기술은 분산장부 공유기술을 처음 도입하고 적용한 비트코인이 발표된 2009년부터 2015



(그림 1) 블록체인 기술의 세대별 분류

년 이더리움이 발표되기 이전까지의 시기를 1세대로, 스마트 계약 기술을 활용한 이더리움을 시작으로 다양한 분야에 확산 가능성을 타진하는 응용 기술이 등장하는 현재까지의 시기를 2세대로 크게 구분 가능하다. 일부 다양한 기술적 시도를 통해 이더리움 대비 두드러진 개선점을 보이는 경우 2.5세대로 구분하기도 하나[8] 대부분 개발이 진행 중이며, 상용화 시장에 미치는 파급효과가 제한적인 것으로 판단하여 세분화하지 않았다.

1세대의 블록체인 기술은 분산장부 공유기술 기반의 암호화폐인 비트코인이 등장한 이후 주로 디지털 통화의 발행, 유통 및 거래 용도로 활용되어 개념적인 혁신성에도 불구 그 기술적 파급이 제한적이었으며 느린 거래 속도로 인해 기술의 응용 범위가 한정적인 영역에 그쳤다. 2세대 들어 이더리움이 미리 지정한 조건에 따라 계약이 자동으로 이루어지도록 구조화된 스마트 계약을 시스템에 채택하며 플랫폼 성격의 기술이 등장하였고 이를 기반으로 다양한 응용사례인 디앱(DApp)들이 확산되며 상용 시장에서의 파급력을 배가하였다.

그러나 (그림 1)에서 알 수 있는 바와 같이, 블록체인 기술은 그 발전 기간이 그리 길지 않았던 만큼 여전히 기술적 한계 및 취약점을 내포하고 있다. 향후 개발되어 3세대로 분류될 기술은 기존 1세대 및 2세대가 여전한 한계를 갖는 거래속도, 처리 용량, 상호운용성 등 다양한 성능지표를 개선하여 상용시장에서의 실용성을 담보하는 기술이 될 것으로 예상된다. 사례별 특징을 보다 상세하게 살펴보면 다음과 같다.

1. 제 1세대: 비트코인

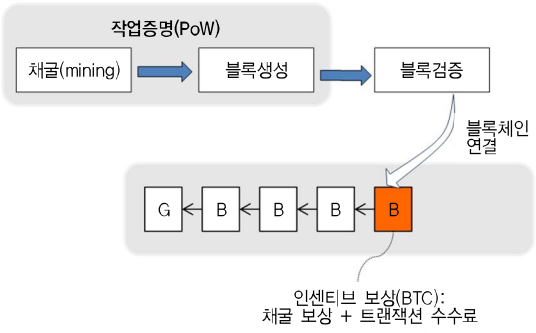
2008년 11월, 나카모토 사토시에 의해 암호학 기술 관련 메일링 리스트를 통해 공개된 비트코인은 P2P 기술과 공개키 암호, 해시함수 등의 암호 기술을 기반으로 구현된 분산 시스템으로 운영 주체가 존재하지 않는 특징을 가진다[4]. 기존의 은행과 같은 중개인 역할을 배제하고 사용자들 사이에 거래 내역을 완전히 분산 저장하도록 만든 새로운 개념의 금융 시스템으로 블록체인의 개념을 처음 상용화하였다. 이후, 라이트코인, 리플 등 유사 응용 사례들이 등장했으나 기능적 측면에서 유사하였으며, 구조적으로도 비트코인에 비해 획기적으로 개선된 특징은 없다[9], [10].

가. 운영 구조

비트코인은 중개인 역할 없이 사용자들 사이에 직접 안전하게 거래를 할 수 있도록 하는 분산 원장을 생성하기 위해 해시와 전자서명 같은 암호 알고리즘을 사용한 블록체인 구조와 작업증명에 의한 채굴(mining)을 사용한다[(그림 2) 참조]. 이러한 비트코인의 핵심적 특성은 네트워크 참가에 제한을 두지 않는 오픈 시스템으로 운영된다는 점으로, 채굴과 작업 증명 방식(PoW: Proof of Work)이라는 합의 메커니즘에 기반하여 비잔틴 문제[4]를 해결하고자 시도한 점이다.

또한 비트코인은 블록체인 생성에 참여하는 노드들에게 연산 능력에 따라 보상함으로써 시스템이 계속 운영될 수 있는 수단을 제공한다. 새 유효 블록을 생성한 노드들에 대해서는 그에 대한 보상으로 50BTC를 지급하고(21만 개의 블록이 추가될 때마다 절반씩 삭감) 블록에 포함되는 트랜잭션들에 대한 거래 수수료를 해당 블록 생성 노드에 지급하도록 되어 있다.

비트코인 응용은 튜링 완전성을 지원하지 않는 스크



(그림 2) 비트코인의 운영 구조

립트에 의해 동작하도록 되어 있어 컴퓨터적 문제 해결이 불가하다는 한계를 가진다.

나. 합의 알고리즘

작업증명 알고리즘(PoW)은 1991년 스팸 메일 방지용으로 제안된 비잔틴 합의 알고리즘이었지만[11], 비트코인에 채택되면서 유명해졌다[4]. 특히 이 방법은 PBFT (Practical Byzantine Fault Tolerant)[12], [13]와 같은 기존의 비잔틴 합의 알고리즘들이 시스템 내 f개의 악의적인 노드가 있다면 $3f+1$개 이상의 노드들이 있어야 안정적인 시스템 운영이 가능하다는 제한 조건이 있었던 것과는 달리, 이러한 제한을 두지 않고 경험적인 방법에 의해 운영되는 단순하고 획기적인 접근법이다.

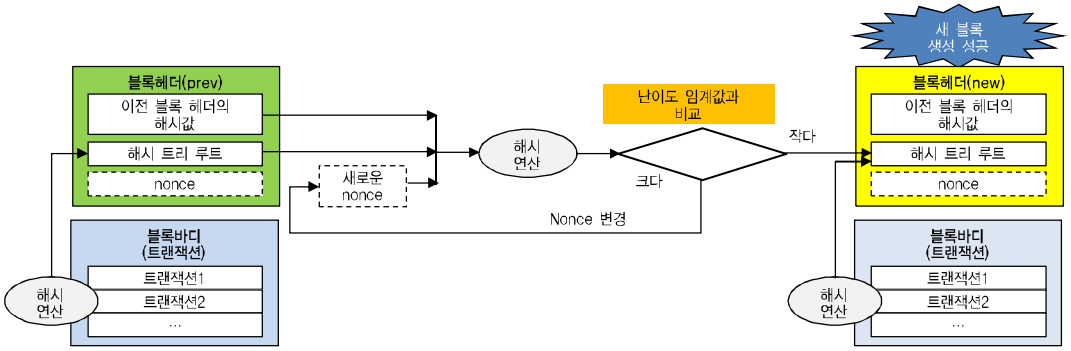
PoW는 (그림 3)에서 보는 바와 같이, 새 블록 생성을 위해서는 바로 앞에 생성된 블록의 헤더값과 직접 값을 대입할 수 있는 nonce 필드를 해시 연산하여 난이도(difficulty) 기준을 통과할 수 있는 값을 찾는 작업을 수행한다. 값을 찾으면 다른 노드들에 전파하여 블록체인에 자신의 블록을 연결하도록 하는데, 먼저 값을 찾은 다른 노드의 블록이 있으면 자신의 블록은 버려져야 한다. 해시값의 랜덤성으로 인해 nonce 필드는 0부터 시작해 조건에 맞을 때까지 같은 작업을 반복하게 되는데 이에 많은 에너지 소모가 필요하다.

PoW에서는 원하는 모든 노드가 블록 생성 과정에 참여함으로써 유효한 블록이 2개 이상 생성되는 fork가 발생할 수 있는데, 생성된 블록이 블록체인에 속할 수 있는 유효한 블록으로 합의되는 방법은 크게, 1) 가장 먼저 생성하여 배포하는 블록을 유효한 블록으로 인정해주는 것과 2) 가장 긴 체인을 유효한 것으로 인정하는 규칙에 기반한다.

또한, 블록 데이터 해시 연결을 위해 블록에는 블록 헤더의 필드들을 해시 함수로 계산한 블록 해시가 들어가고 이를 통해 해시 연결성을 검증해 블록체인 데이터가 중간에 위변조되지 않았음을 확인할 수 있다. 이러한 블록 헤더에는 바로 앞에 연결된 블록의 헤더 해시값도 포함함으로써 블록체인을 중간에 위·변조하는 것을 어렵게 만들 수 있다. 그러나 이러한 비트코인 PoW 방식은 다음과 같은 주요한 한계점을 가진다.

먼저, 블록 생성을 위해서는 해시값을 찾기 위한 해시 연산을 통해 작업증명을 통과해야만 하는데, 그 과정에서 엄청난 에너지가 소모된다.

블록 생성의 최종확정성 문제도 큰 이슈이다. 블록 생성이 전체 규모에서 유효하다는 것은 블록 생성시에는 결정하기 힘들어서, 각 노드들은 가장 먼저 도착한 블록을 유효블록으로 인정한다. 그러므로 네트워크의 상태나 악의적인 노드의 방해에 의해 체인이 2개 이상으로 분기하는 fork 현상의 발생을 감수하여야 하고, 뒤늦게 잘못된 체인에 붙은 블록과 트랜잭션들은 생성되고 한참 후에 유효하지 않은 것으로 결정됨으로써 버려져야 하는 경우도 생길 수 있다(생성되고 추후 6블록이 생성



(그림 3) 작업증명 방식

될 때까지 문제없으면 완전히 유효하다고 간주)[14].

또한, 악의적인 51% 공격에 대한 취약성도 존재한다. PoW는 가장 먼저 채굴하는 노드에 블록 생성 권한을 주는 방식으로, 악의적인 노드가 블록을 가장 먼저 생성할 경우에는 이중 지불이나 트랜잭션의 위·변조와 같은 문제점 등이 발생할 가능성이 있다.

다. 거버넌스

비트코인 시스템은 자체 의사결정 기능이 없어서 소유자들 간에 합의가 이뤄지지 않을 경우 가상 통화가 쪼개지는 '하드포크(Hard Fork)'가 일어나 생태계 파편화의 문제도 발생할 수 있다. 실제 비트코인은 2017년에 2번의 하드포크를 거쳐 비트코인 캐시와 비트코인 골드가 탄생되었다[15].

라. 확장성 및 보안성

비트코인에서는 분산 네트워크 환경에서 네트워크상의 충분한 데이터 전파를 고려하여 블록 생성 시간을 평균 10분으로, 블록의 크기를 1MB로 제한하였는데, 그 결과 초당 처리 가능한 트랜잭션이 7개에 불과한 등의 한계를 보였다. 이러한 한계로 인하여 비트코인은 제한된 응용에만 사용될 수 있었다.

비트코인의 낮은 확장성을 해결하고자, 서명부분을 따로 witness란 데이터 영역으로 분리시켜 더 많은 거래를 처리 가능하도록 업데이트하는 SegWit(Segregated Witness)[16], 사용자들이 상호 약속하여 비트코인 블록체인에 따로 브로드캐스팅하지 않고 별도의 채널을 만들어 비트코인을 전송 및 결재하는 기술인 Lightning network[17] 등과 같은 개선 방식들이 연구되고 있다. 또한, 보안성 제공도 블록체인에서는 큰 이슈가 되고 있는데, 꾸준히 보안성 공격 취약 유형들이 발견되고 있다(Brute force attack, 50% hash power or gold finger, Wallet theft, DDoS 등). 그러나 블록체인이 어느 정도 안전하고 안정적인지, 또 이를 달성하는데 필요한 조건이 무엇인지는 아직까지 명확하게 밝혀지지 않고 있는 실정이다.

마. 1세대 블록체인 사례들

1세대 블록체인의 사례들을 나열하면 〈표 1〉과 같다.

〈표 1〉 1세대 블록체인 사례들

사례	적용 분야	합의 알고리즘	거래 처리속도	블록 생성 시간 (블록크기)
Bitcoin	암호 화폐	PoW (SHA-256 기반)	7TPS	10분(1MB)
Litecoin	암호 화폐	PoW (Scrypt 기반)	56TPS	2.5분(4MB)
Ripple	국제 송금	리플 프로토콜 (노드들간 직접 합의)	1,500TPS	당사자끼리 직접 거래
Stellar	국제 송금	SCP(Stellar Consensus Protocol)	1,000TPS	당사자끼리 직접 거래
Monero	암호 화폐	PoW (Cryptonight 기반)	Unknown	2분(크기 제한 없음)

2. 제 2세대: 이더리움

이더리움은 2015년 Vitalik Buterin에 의해 제안되어[18], 블록체인에 화폐 거래 기록뿐만 아니라 계약서의 추가 정보를 기록하도록 하여 SNS, 이메일, 전자투표 등 다양한 정보를 기록하는 시스템을 구축할 수 있다.

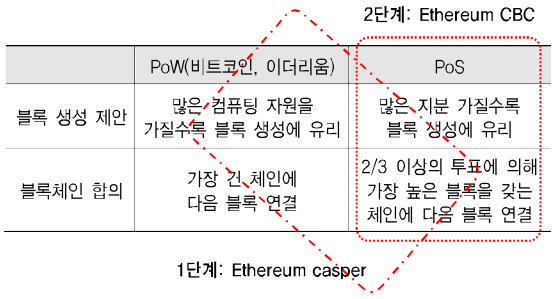
가. 운영 구조

이더리움의 운영 구조는 비트코인과 유사하나, 플랫폼 형태로 제공되는 점과 스마트 컨트랙트 기능이 제공되는 점이 가장 큰 차이점이다. 이더리움 플랫폼 참조 모델은 (그림 4)와 같이 여러 계층으로 구분할 수 있는데[19], 합의 구조와 스마트 컨트랙트에 대해 설명하면 다음과 같다.

이더리움은 비트코인에서 사용한 PoW의 한계를 개선하기 위해 수정된 PoW 방식인 Ethash를 사용한다. Ethash의 장단점은 합의 알고리즘 부분에서 기술한다.

이더리움의 또 다른 특징인 '스마트 컨트랙트'는 Nick

(그림 4) 이더리움 플랫폼 참조 모델



(그림 5) 이더리움의 합의 알고리즘

Szabo가 1994년에 최초로 제안한 개념으로[20], 디지털 명령으로 계약을 작성하여 조건에 따라 컨트랙트 내용을 자동으로 수행할 수 있다. 이더리움에서 사용하는 스마트 계약은 사용자간 계약을 튜링 완전성(Turing-completeness)을 제공하도록 자체 개발한 프로그래밍 언어인 Solidity를 통해 자동 실행되어 제공된다. 그러나 루프가 있기 때문에 같은 명령을 프로그램에게 반복하여 실행하도록 하는 반면 이 기능으로 인해 명령 쇄도로 네트워크가 망가지는 가능성을 제공하기도 한다. 또한 사용자는 무한루프를 통해 쉽게 DoS 공격을 실행할 수 있는 보안 취약성을 가질 수 있다. 이더리움에서는 'GAS'라는 거래 수수료 서비스를 통하여 무한루프를 방지하는 방법으로 이 문제를 해결한다.

나. 합의 알고리즘

이더리움에서 사용하는 합의 알고리즘인 Ethash는 대거-해시모토(Dagger-Hashmoto)라 불렸던 방식으로, 컴퓨터 메모리상의 일정 양의 데이터를 읽은 후 이를 넌스와 함께 해시 계산을 함으로써 메모리 IO 중심의 작업 증명을 수행한다. 약 12초에 하나의 블록을 생성하는 것이 알고리즘의 궁극적인 목표인데, 현재는 메모리 계산을 위해 2차원 배열 데이터의 DAG(Directed Acyclic Graph) 파일이 사용을 사용하고 10~15초마다 하나씩 블록을 생성한다.

Ethash는 비트코인의 합의 방식의 단점을 개선했다고는 하지만 보완 수준이고 여전히 에너지 소모가 큰 PoW를 사용하고 비자(Visa) 카드보다 거래 처리속도가 느리며 사용자가 높은 수수료를 부담해야 하는 것과 같은 한계점을 가진다.

이더리움에서는 PoW 방식의 한계점을 개선하고자 지분증명 방식(PoS: Proof of Stake) 합의 알고리즘으로 바꾸는 작업을 진행 중이다[21], [22]. 하지만 바로 PoS로 바꾸기보다는 블록 생성은 PoW로, 체인 합의는 PoS 방식에 의해 진행하는 이더리움 Casper를 거쳐 최종적으로는 블록생성과 합의 모두 PoS 방식인 이더리움 CBC 방식을 적용할 예정이다[(그림 5) 참조]. 2018년 이더리움의 발표에 따르면 Casper는 PoS와 PBFT를 결합한 구조를 가질 예정이다.

다. 거버넌스

거버넌스는 이더리움에서도 여전히 해결하지 못했고 거버넌스 부재로 인해 문제가 발생한 상황이다. 그 대표적인 사례로, 2016년 DAO(Decentralized Autonomous Organization) 해킹 사건으로 인해 하드포크를 진행하여 현재는 이더리움 클래식과 이더리움으로 분리되었다[23].

라. 확장성 및 보안성

비트코인과 마찬가지로 이더리움 역시 확장성과 보안성 문제를 안고 있다. 이더리움은 15TPS 정도의 거래 처리 성능을 제공하는 것으로 알려져 있다(2018년 4월 기준 20TPS 정도). 따라서 트랜잭션(사용자 간 거래 기록) 용량 제한에 의한 문제 해결과 확장성 확보를 위해

이더리움은 블록체인으로부터 별도의 채널을 만들어 모두의 합의를 거치지 않아도 되는 거래 기술인 Raiden network[24], 전체 네트워크를 분할한 뒤 트랜잭션을 영역별로 저장하고 이를 병렬적으로 처리하여 블록체인에 확장성을 부여하는 기술인 sharding[25], 별도의 체인을 만들고 최소한의 데이터만 이더리움의 메인 블록체인과 동가화하는 방법인 plasma[26], 블록체인의 연산 증가에 초점을 둔 이더리움 스마트 계약 확장성 솔루션으로 제시된 TrueBit[27]와 같은 방법들을 도입하고 있다.

마. 제2세대 블록체인 사례들

제2세대 블록체인의 대표 사례들의 특성을 소개하면 〈표 2〉와 같다. 이들의 특성을 간단히 기술하면 합의 알고리즘이 전술한 PoW의 한계점을 극복하기 위한 다양한 방식이 도입되었다는 점이다. 또한, 적용 분야도 1세대의 금융화폐에서 확장되어 SNS를 포함하여 다양해진 점도 특징으로 보인다. 그러나 거래 처리 속도는 시간에 따라 개선되고 있기는 하지만 아직 한계가 있다고 판단된다.

〈표 2〉 2세대 블록체인 사례들

사례	적용 분야	합의 알고리즘	거래 처리속도	블록 생성 주기 (블록크기)
Ethereum	범용	PoW(Ethash 기반) →PoS로 변경 예정	20TPS	15초(크기 제한 없음)
Steemit	SNS	DPoS(20인의 증인)	10만TPS (목표)	3초
Ethereum classic	범용	PoW→PoS로 변경 예정	56TPS	21초
NXT	범용	PoS	100TPS	1분(32KB)
ARK coin	범용	DPoS(51인의 증인)	7TPS	8초

Ⅲ. 블록체인 기술의 현재

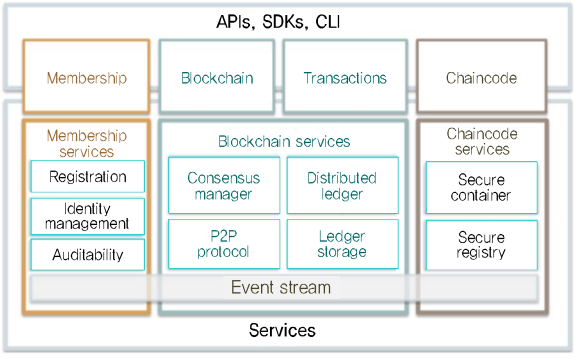
본 장에서는 블록체인 기술 발전 현황을 파악하기 위해, 현재 블록체인 기술들을 대표할 수 있는 Hyperledger, EOS, QTUM, Cardano, NEO, IOTA의 기술 개념과 이들이 목표 또는 구현하고 있는 기술적인 특징들을 개별적으로 분석하고자 한다.

1. Hyperledger

리눅스 재단과 IBM의 주도로 2015년 12월부터 하이퍼레저 프로젝트가 시작되었다. 시스코, JP모건 등 글로벌 기업들이 공동으로 참여하는 것으로, 기업 결재, 상품 추적 및 관리 등을 위한 오픈 소스 분산 원장 프레임을 개발하고 글로벌 블록체인 기술 표준화 작업을 진행하고 있다. 하이퍼레저 프로젝트 중 블록체인의 엔진을 포함하여 블록체인의 기반 기술을 개발하는 하이퍼레저 패브릭의 구조 및 현황을 설명한다. 하이퍼레저는 프라이빗 블록체인 플랫폼으로서 기업 비즈니스 환경을 목표하고 있으며 여러 사업에 범용적으로 도입 가능한 기술 표준을 제공하는 특징이 있다. 현재 1.3 버전까지 나와 있다[28].

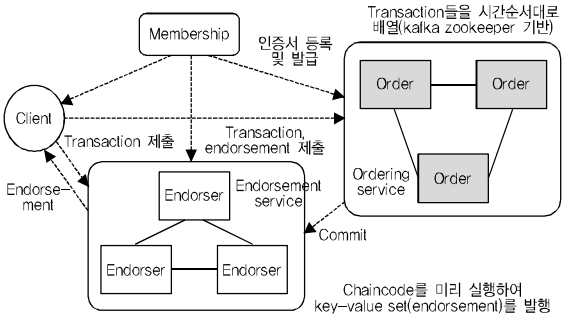
가. 합의 알고리즘

하이퍼레저 패브릭의 아키텍처는 크게 가입이나 참여자의 신원 확인 및 인증을 담당하는 멤버십 서비스, 사용자의 스마트 계약을 실행하는 것과 관련한 기능인 체인 코드 서비스, 분산 원장을 저장/관리하는 것과 관련



(그림 6) 하이퍼레저 패브릭의 아키텍처

[출처] Hyperledger Fabric, Available: https://www.hyperledger.org/projects/fabric, CC BY 4.0.



(그림 7) 하이퍼레저 패브릭의 합의 구조

한 블록체인 서비스로 구성된다[(그림 6) 참조].

하이퍼레저 패브릭의 동작은 (그림 7)과 같이, 실행 결과들을 블록체인의 다른 노드에 보내주는 endorser, 합의를 수행하는 orderer, 멤버들의 신원 확인과 접근 권한을 관리하는 membership 노드, 거래를 확정시켜 블록체인을 유지하는 committer들이 유기적으로 협동하여 클라이언트의 요청을 처리하는 구조를 가진다. 합의 알고리즘은 플러그인으로 모듈화하는 구조로 되어 있어, Kafka, Zookeeper, PBFT 등 필요에 따라 다양한 방법이 사용될 수 있다. 그러나 허가형 블록체인인 만큼 굳이 어려운 알고리즘을 안 쓰는 방향으로 개발된다.

나. 거버넌스

하이퍼레저 패브릭은 프라이빗 블록체인으로, 거버넌스 이슈로부터는 자유롭다.

다. 확장성

하이퍼레저 패브릭은 프라이빗 블록체인으로 운영되므로 거래 처리 속도가 높다. 15노드 기준으로 10만 TPS를 목표로 한다.

2. EOS

EOS는 이더리움과 경쟁하기 위해 Block.one이 2016년에 개발 착수한 오픈 소스 기반 블록체인 아키텍처(EOS.IO)로, 이더리움상에서 개발된 DApp은 EOS상에서도 동작 가능하다[29].

EOS는 이더리움의 DApp 기능을 제공하면서도 이더리움의 낮은 거래 처리 속도와 높은 거래 수수료 문제를 해결하여 '이더리움 킬러'로 불리지만, 합의 알고리즘이나 확장성 등에서 극복해야 할 이슈들이 있다.

가. 합의 알고리즘

EOS는 DPoS(Delegated PoS)와 PBFT를 기반으로 하는 합의 알고리즘을 사용한다. DPoS 방식으로 플랫폼 전체를 대표하는 21명의 블록 생성자를 선출하고 이들 간에는 PBFT 방식으로 투표를 통해 0.5초마다 블록을 하나씩 생성한다. 합의 절차에 소수의 합의 주체만 참여하기 때문에 PoS을 사용하는 블록체인보다도 빠른 처리 성능을 제공할 수 있다. 하지만 소수의 블록 생성자에게 주어지는 권한이 크기 때문에 21명의 블록 생성자 중 일부가 담합하여 블록체인을 공격하여 심각한 문제를 초래할 가능성도 있다.

나. 거버넌스

EOS는 DPoS 합의 알고리즘에 의한 운영 방식을 사용하여 지분 소지자들이 투표를 통하여 분리된 블록 생성자에게는 표를 주지 않을 것이므로 하드포크가 발생하지 않는다고 한다.

다. 확장성

분산 합의 알고리즘의 우수한 성능으로 인해 EOS는 현재 3,000TPS 정도의 성능을 제공한다. 또한, EOS는 분산 응용 사용자 대신 응용 서비스 제공자가 수수료를 부담하는 방식을 제안한다. 그 결과, 일반 사용자는 EOS 코인이 없더라도 EOS 어플리케이션을 쉽게 사용할 수 있는 반면, 서비스 제공자는 EOS 코인을 보유하고 있어야 하며 보유한 코인에 비례하는 만큼의 거래 처리 속도를 사용 가능하다.

3. QTUM

2016년 싱가포르에서 퀀텀 재단 설립으로 시작된 퀀텀은 비트코인과 이더리움의 장점을 결합한 하이브리드 블록체인 플랫폼으로 인식된다[30].

퀀텀은 비트코인의 UTXO 방식과 이더리움의 EVM을 연결하여 이더리움 플랫폼처럼 산업별 특성에 맞춰 블록체인 운영이 가능하다. 퀀텀은 비트코인의 UTXO 모델을 도입하여 높은 보안성과 결제의 신속성을 확보하고, 이더리움의 EVM을 기반으로 무한 응용 가능한 스마트 컨트랙트를 구현하여 비트코인의 확장성 문제를 해결한다. EVM과의 호환으로 이더리움의 모든 스마트 컨트랙트 및 응용이 최소한의 변환으로 퀀텀 블록체인에서 운용 가능하다.

또한, 이더리움 네트워크에서는 온체인 데이터만 스마트 컨트랙트를 실행시키는 촉매제가 되는 한계가 있는데, 퀀텀에서는 이 문제를 극복하기 위해 마스터 컨트랙트 개념을 개발하여 오프체인 데이터에 의해서도 실행 가능하다. 또한 퀀텀은 모바일 응용에 최적화된 인프라를 제공하여 모바일을 통한 블록체인의 장점도 누릴 수 있도록 설계하였다.

가. 합의 알고리즘

퀀텀은 PoS를 합의 알고리즘으로 사용한다. PoS는 각 자산을 보유하는 노드들이 자신이 합의하는 블록에 자산을 증명함으로써 데이터를 업데이트하는 것으로, 자신이 옳다고 생각하는 블록에 동의를 하면서 자신이 가진 지분을 해당 블록에 보여주고 증명하는 것이고 그 결과 과반수의 자산이 동의한 블록이 더 빠르고 더 길게 블록체인을 형성한다. 퀀텀은 비트코인 빌딩 블록을 사용하여 퀀텀 지분 비율에 따라 확률적으로 블록을 생성한다. 최근 퀀텀은 인센티브 지분증명방식(IPoS: Incentive Proof of Stake) 방식으로 업그레이드할 계획이라고 발표했으나 구체적인 방식은 소개하지 않은 상태이다.

나. 거버넌스

퀀텀은 블록체인 파라미터들이 기존의 생태계를 파괴하지 않으면서 쉽게 수정 가능하도록 분산형 관리 프로토콜인 DGP(Decentralized Governance Protocol)를 도입한다[31]. DGP는 스마트 컨트랙트를 통해 파라미터들을 조정하도록 함으로써 필요할 때마다 새로운 규칙으로 대체하거나, 업그레이드하여 하드포크를 방지할 수 있다. DGP를 통한 파라미터 변경이 이루어지면 가장 긴 체인을 만들어낸 결과값으로 조정된다.

다. 확장성

퀀텀은 PoS를 합의 알고리즘으로 선택하면서 성능보다는 보안성에 중점을 두고 있다. 공식적으로 TPS는 나와 있지 않지만, 이더리움 성능의 3~4배인 것으로 알려져 있다.

4. Cardano

카르다노 재단에서 관리하는 모바일 암호화폐 플랫폼인 카르다노(Cardano)[32], [33]는 금융 기관을 이용하지 않아서 신용 등급이 없는 사람들도 자유롭게 금융 거래를 할 수 있는 환경을 만들고자 개발되었다.

가. 합의 알고리즘

카르다노는 PoS 합의 방식의 취약점인 grinding 공격을 방지하도록 설계된 수학적으로 증명된 안전한 지분 증명 방식인 우르보로스(Ouroboros)[34]를 합의 알고리즘으로 사용하는 것이 주요한 특징이다. 알고리즘의 핵심은 PoS에서 마지막 블록 생성자가 다음 블록 생성자를 랜덤하게 선택할 때 조작 가능성을 없애기 위해 네트워크 구성원 각각의 랜덤한 정보를 서로 공유하고 그 결과를 복합적으로 합쳐 다음 블록 생성자를 선출하는 방식을 사용하는 점이다. 그 결과, 혹시 발생할 수 있는 조작 결과도 다른 구성원들의 랜덤한 결과에 의해 그 영향을

없애게 된다. 우르보로스 알고리즘 절차는 다음과 같다.

- Phase 1: 각 구성원은 랜덤 변수를 생성, 각 조각을 네트워크에 전달한다.
- Phase 2: 자신의 랜덤 변수를 암호화하여 전달하면, 이를 받은 노드는 본인의 랜덤 변수를 반환한다. 암호화된 변수를 전달한 노드는 다시 암호화된 변수를 해독하는 키를 전달한다.
- Phase 3: 모두의 랜덤 변수를 바탕으로 최종 변수를 계산하여 다음 블록 생성자를 선택한다. 이때 조작 노드가 있더라도 나머지 노드들에서 기존에 주고받은 정보들을 조합하여 결과를 산출한다.

카르다노는 우르보로스 방식을 통하여 합의 노드의 협의체를 선출하는 탈중앙화된 방법을 제공하며 여러 협의체를 동시에 선출하고 트랜잭션들을 다른 협의체로 분할할 수 있도록 하였다. 또한 모든 거래 참여자 중에서 투표시스템을 통해 블록 생성자를 선출하고 득표수에 따라 선출된 블록 생성자가 블록을 생성하여 효율성을 향상시킨 DPoS 방식을 사용할 수도 있다.

나. 거버넌스

카르다노는 모바일에 최적화된 암호화 플랫폼으로, 사용자가 블록체인의 주요 개선 사항 또는 포크에 대한 투표 권한을 갖는 온체인 거버넌스를 갖는 장점이 있다. Cardano 화폐인 Ada를 소유한 사람은 프로토콜 변경 방법, 이해관계자 의도를 파악하는 방법, 파편화 가능성을 줄이는 방법 등에 투표할 수 있다. 소유자 의견을 수렴한 투표 결과를 소프트 포크로 구현하여 민주적인 변화를 이끌어내는 블록체인으로 평가받고 있다.

다. 확장성

카르다노의 거래 처리 속도는 258TPS 정도로 알려져 있다[35]. Cardano가 플랫폼 역할을 하기 위해서는 5,000TPS 이상이 되어야 하는 점을 감안하면 확장성 이슈는 아직 진행 중인 상태로 볼 수 있다.

5. NEO

NEO는 중국에서 활발히 개발되고 있는 중국판 이더리움으로 불리는 블록체인이지만, NEO는 모든 실물 자산이 디지털화되어서 블록체인 위에서 거래되는 'Smart economy'를 구현하는 것을 목표로 한다[36]. NEO는 이더리움과 유사하게 NeoVM 위에서 NEO 컨트랙트를 기반으로 운영된다. NEO 컨트랙트는 개발자의 접근성을 높이기 위해 Java, Go, 파이썬 등 기존에 널리 쓰이는 언어들을 지원한다. NEO에서 사용하는 코인은 블록체인 등록을 위해 사용하는 NEO 코인과 실제 거래에 필요한 수수료로 사용되는 GAS 코인을 지원한다.

가. 합의 알고리즘

NEO는 DBFT(Delegated BFT) 합의 알고리즘을 사용한다. DBFT는 위임된 BFT 방식으로, NEO 참여자들이 투표를 통해 합의 권한을 위임할 북키퍼(Bookkeeper)들을 선출하고 북키퍼들이 PBFT 방식으로 새로운 블록을 생성하고 블록체인에 연결하는 방식이다. DBFT 합의 방식으로 새로운 블록을 생성하는데 15~20초가 소요된다.

하지만 실제 NEO 블록체인이 운영되는 방식에는 주요한 문제점이 있다. 북키퍼가 되기 위해서는 NEO 재단의 승인을 받아야 하는데, 북키퍼로 동작하는 노드가 7개에 불과하며 대부분이 중국 내에 위치한 NEO 위원회라는 점이다. 이러한 사실은 블록체인의 탈중앙화 철학에 위배되는 것으로 판단된다.

나. 거버넌스

NEO는 DBFT 알고리즘을 사용하므로, 승인된 북키

퍼들이 블록체인을 운영하는 구조로 하드포크가 아예 불가능한 구조로 되어 있다. 또한 블록체인을 사용하기 위해서는 NEO 코인을 이용한 등록이 반드시 필요하다. 등록 및 사용수수료 모두 북키퍼한테 돌아가는 구조라 안정적으로 운영 가능하다고는 하지만 동시에 많은 한계점도 가지고 있다.

다. 확장성

최근 발표된 NEO 3.0에서는 100,000TPS의 거래 처리 성능을 목표로 하는데, 현재는 1,000TPS 미만 수준이다. NEO 3.0에서는 코드와 코어 모듈 재정렬, 네트워크 프로토콜 최적화, 기본 정보 저장 파일 및 네오 컨트랙트를 위한 허가 시스템 도입, dynamic sharding 기술, state persistence와 block persistence 분리 등으로 TPS를 증가시킬 계획이다.

6. IOTA

IOTA는 소액 결재가 어렵고 거래마다 높은 수수료를 지불하는 비트코인이 IoT 환경에서 부적합함을 인식하고 새로운 접근 방식을 활용하여 개발된 것이다. IOTA는 선형적으로 블록을 생성하는 방식이 아닌 DAG (Direct Acyclic Graph)의 구조를 가지는 탱글(Tangle)이라는 공공 분산 장부 기술을 사용하여 IoT 환경의 거래에 활용한다[37].

가. 합의 알고리즘

IOTA는 거래를 하는 모든 당사자가 직접 합의 절차에 참여한다. 탱글은 DAG 구조로 생성된 거래 1개가 다른 곳에서 이미 이루어진 2건의 거래를 직접 컨펌하는 방식에 의해 운영되고, 다른 하위 탱글에 있는 다른 거래들을 간접적으로 참조한다. 이러한 방식은 다른 블록체인이 선형적인 블록들의 추가에 의해 블록 보상과 거래 수수료를 획득하는 방식과 비교하면, 검증이 병렬화되고 네트워크는 완전히 분산화되어 채굴자가 따로 필요하지 않으며 거래 수수료가 존재하지 않는다는 장점을 가진다. IOTA도 PoW 방식을 채용하기는 하지만 이것은 비트코인에서 사용하는 용도와는 다르게, 시빌(Sybil) 공격과 스팸(Spam)을 방어하기 위한 해시 캐시에 가깝다.

나. 거버넌스

IOTA는 블록체인과 같이 분산형 스토리지, P2P 네트워크, 합의 메커니즘에 기반을 두고 있긴 하지만 완전 분산형 방식에 의해 운영된다. 따라서 확장성과 수수료 문제에 초점을 맞추고 구조를 설계한 것으로 아직 거버넌스 이슈에 대한 내용은 언급되고 있지 않다.

다. 확장성

IOTA는 DAG 구조 채용에 의해 검증을 병렬화시켜 많은 수의 거래를 동시에 처리할 수 있다. 또한, 탱글의 규모가 커지고 참가자들의 거래가 늘어날수록 전반적인 시스템은 더 안전해지고 거래 처리 속도가 빨라지며 거래의 최종 확인까지 걸리는 시간이 단축된다.

7. 요약

본 장에서는 현재의 블록체인 기술을 대표하는 사례들 각각에 대해 운영방식 및 합의 알고리즘, 거버넌스, 확장성 측면에서 살펴보았다. 이들 중 확장성 목표는 여전히 낮은 성능을 보임으로써 개선이 필요한 상황임을 알 수 있었다. 분산 합의 알고리즘은 성능이나 보안성에 직접적인 영향을 주는 블록체인 기술 요소로서, 개선을 위한 많은 노력이 이루어지고 있음을 볼 수 있었다. 블록체인 초기에 적용된 PoW가 가지는 한계점들을 극복하고자 PoS, DPoS 등의 방식들이 도입되었고, 최근에는 최종확정성 이슈를 해결하기 위해 PoS나 DPoS 등과 기존의 분산 시스템에서 사용되던 PBFT 알고리즘과 결

〈표 3〉 분산 합의 알고리즘들의 특징 및 한계점

합의 방식	특징	한계점
PoW	– 각 노드의 연산 능력을 증명하여 새 블록 생성	– 연상능력 보유에 의한 중앙화 가능: 참여노드 연산능력에 비례하여 블록 생성 – 개별 노드 연산능력 증명을 위한 전력소모
PoS	– 소유 지분 양에 비례하여 블록 생성 권한을 부여 받을 확률을 높인 방식 – Ouroboros 알고리즘 등 PoS의 한계점 극복을 위한 시도들이 많음 – Ethereum casper는 PoS+PBFT 방식 도입 예정	– PoW의 단점을 보완 – 보유 지분량에 의한 중앙화 가능
DPoS	– 블록 생성 권한을 소수 대리인에게 위임 – 빠른 합의 속도와 낮은 비용	– 보안성 낮음 – 대리인에 대한 공격 취약성 존재
PBFT	– 비잔틴 노드가 존재하는 분산 네트워크 환경에서 노드들 간의 합의 방식 – 최종확정성과 성능 문제 해결	– 노드 증가에 따라 성능 감소(수십 개의 노드가 한계)
Tendermint (DPoS+PBFT)	– 가장 지분이 많은 n(101)개 노드 간의 투표로 새 블록 합의: 미리 정해진 순서대로 새 블록 제안 – 노드가 보유한 지분에 비례한 투표 권한 행사	– 블록제안 노드 예측 가능으로 특정 대상 공격에 취약 – 모든 노드 합의 참여로 과다한 통신비용 발생
Zilliqa (PoW+PBFT	– PoW에 성공한 n(800)개의 노드 간 투표를 통해 새 블록을 합의하는 방식: 고정된 1개 노드가 블록 제안, 나머지 노드들은 투표	– 고정 노드의 새 블록 제안으로 특정 대상 공격에 취약 – 모든 노드 합의 참여(투표)로 과다한 통신비용 – PoW 문제에 종속

〈표 4〉 분산 합의 알고리즘의 특성 수치 비교

합의 방식	탈 중앙화	전력 소모	공격감내성	최종 확정성	성능 (응답시간)
PoW	○	○	≤25%	×	낮음
PoS	○	×	알고리즘에 의존	×	낮음
DPoS	△	×	알고리즘에 의존	×	높음
PBFT	×	×	≤33%	○	높음
Tendermint	×	×	≤33%	○	높음
Zilliqa	×	○	≤25%	○	높음

합하는 시도들도 많이 있다.

〈표 3〉은 현재까지 블록체인을 위해 제안된 대표적인 합의 알고리즘을 요약한 것이고 〈표 4〉는 합의 알고리즘의 장단점을 비교 분석한 것이다. 이로부터 알 수 있는 바와 같이, 각 알고리즘은 3세대에 적용되기에는 한계점을 가지고 있는 바 아직 대세가 될 만한 대안은 보이지 않는다고 할 수 있다.

Ⅳ. 향후 블록체인 기술 발전 전망

지금까지 블록체인 기술들의 특성 및 한계점들을 세대별로 살펴보았다.

1세대와 2세대 블록체인 기술들은 시장 점유율은 높지만 아직까지 블록체인 기술 자체의 우수한 장점들이 다양한 산업분야에까지 적용되기에는 분명한 한계가 있음을 알 수 있었다. 우선 다양한 분산 합의 알고리즘들의 한계점과 불안정성, 낮은 거래처리 성능 외에도 거버넌스의 부재로 인한 하드포크 발생은 기존 금융 분야에 적용하는 것조차 어렵게 만드는 약점이 있었다.

현시점에서의 블록체인 기술들은 1, 2세대 블록체인의 기술적 한계점을 극복하기 위한 노력에 초점을 맞추고 있다. 이러한 노력은 합의 알고리즘을 개선하고, 시스템에 자체 의사결정 기능을 탑재하여 거버넌스 기능을 강화하며, 트랜잭션 처리 성능을 개선하여 확장성을 향상시키고자 하는 점으로 요약할 수 있다. 그러나 아직까지는 단순히 목표와 방향성을 정의하거나 구현 중인 상태로 그 실체들이 명확하지 않음을 보여준다. 또한 이들은 이더리움에 비해 성능 등의 개선은 있지만, 획기적인 발전을 이룰 정도는 아니라고 할 수 있다.

블록체인은 짧은 역사인 만큼 성숙되지 않은 기술로서, 4차 산업혁명의 핵심 기술로 자리잡고 다양한 산업

분야에 적용되는 3세대 블록체인 기술로 넘어가기 위해서는 아직까지는 해결해야 할 이슈들이 많이 남아 있는 상태로 판단된다. 현재의 이슈들이 해결된 성숙한 제3세대 블록체인 기술은 뛰어난 확장성, 보안성, 상호운용성을 제공하여 원하는 응용의 특성을 안전하게 지원할 수 있는 환경을 제공해줄 것으로 기대된다.

이를 위해 3세대 블록체인은 블록체인 인프라의 전송 최적화 및 안정성 확보를 위한 기반 기술, IoT 등 다종 데이터 연동 처리가 가능한 확장 기술, 산업 실적용을 염두에 둔 실증 문제 해결을 위한 서비스 기술이 조화를 이루어 발전되고 성숙될 수 있도록 산학연이 협동할 필요가 있다.

현재 전세계적으로 많은 기업들은 블록체인 시장의 주도권을 잡기 위해서 많은 투자와 노력을 기울이고 있고, 국가 차원에서도 지원이 이루어지고 있다. 국외의 경우는 블록체인과 관련한 다양한 플랫폼 개발 및 응용 서비스 개발이 진행 중이다. 국내도 최근 블록체인에 대한 관심이 고조되며 블록체인 기술의 도입에 적극적이다. 그러나, 금융 이외 서비스 제공을 위한 기술 개발은 아직 초기 단계로 알려져 있다. BOScoin[38], ICON[39], 그라운드 X[40], 블로코[41] 등에서 플랫폼 개발에 주력을 다하고 있지만 아직은 풀어야 할 주요 이슈들이 남아 있는 것으로 파악된다. 따라서 이 시점에서 블록체인 핵심 원천 기술 개발을 통한 원천 기술 확보 및 블록체인 시장을 주도하려는 노력이 시급한 상황이다.

이러한 상황을 기반으로, 한국전자통신연구원에서는 블록체인의 기반 기술 중 하나로 분산 합의 알고리즘에 대한 연구를 수행하고 있다. 분산 합의 알고리즘은 블록체인 시스템의 확장성 향상과 밀접한 관련이 있는 것으로, 성능에도 직접적 영향을 끼치는 가장 중요한 기반 기술 요소이다. 한국전자통신연구원의 접근법은 확률 기반으로 기존의 PoW를 포함한 기존 방식들의 한계점을 극복하고자 한다.

V. 결론

블록체인은 정보의 위변조가 불가능하며 인터넷상에서 중개인 없이 당사자 간의 직접적 가치 전송을 가능하게 함으로써 기존의 비즈니스 방식을 근본적으로 바꾸는 파급력이 큰 기술이다. 이러한 블록체인 기술은 모든 종류의 자산들을 등록, 보관하는데 적용가능하며, 전세계 4차 산업혁명의 핵심 패러다임으로 인식되고 있다.

그러나, 본고에서 살펴본 바와 같이, 블록체인 기술은 짧은 역사를 거친 만큼 아직은 성숙되지 않고 계속 진화하고 있는 기술이다. 블록체인 기술이 산업의 기반 기술로 안정적으로 활용되기 위해서는 해결되어야 할 이슈들이 많이 존재한다.

이러한 상황에서 블록체인의 발전 방향을 이해하고 기반 기술의 확보를 위해 도전하는 것은 시장에서의 경쟁력 제고 및 주도권 확보를 위해서도 매우 중요한 과정이라 판단된다.

용어해설

블록체인 모든 구성원이 분산형 네트워크를 통해 정보 및 가치를 검증/저장/실행함으로써 특정인의 임의적인 조작이 어렵도록 설계된 분산 컴퓨팅 기술.

분산 합의 알고리즘 P2P 네트워크와 같은 분산 시스템 환경에서 분산된 노드 간의 합의 문제를 해결하기 위해 수행하는 알고리즘.

약어 정리

AI	Artificial Intelligence
BFT	Byzantine Fault Tolerant
DAG	Direct Acyclic Graph
DBFT	Delegated Byzantine Fault Tolerant
DGP	Decentralized Governance Protocol
DPoS	Delegated PoS
FBA	Federated Byzantine Agreement
ICO	Initial Coin Offering
ICT	Information & Communication Technology
IoT	Internet of Things
IPoS	Incentive Proof of Stake
PBFT	Practical Byzantine Fault Tolerant

PoS	Proof of Stake
PoW	Proof of Work
TPS	Transactions Per Second
UTXO	Unspent Transaction Output

참고문헌

[1] D. Chaum, "Blind Signature for Untraceable Payments," in *Advances in Cryptology,* Springer: Boston, MA, USA, 1982, pp. 199-203.

[2] W. Dai, "b-money," 1998. Available: http://www.weidai.com/bmoney.txt

[3] N. Szabo, "Bitgold," Wikipedia, 1998. Available: https://en.wikipedia.org/wiki/Nick_Szabo

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Oct. 2008. Accessed 2017, Available: http://nakamotoinstitute.org/static/docs/bitcoin.pdf

[5] CoinMarketCap, "Top 100 Cryptocurrencies by Market Capitalization," Available: https://coinmarketcap.com/

[6] Crunchbase, Available: https://www.crunchbase.com/

[7] IITP, ICT R&D 기술 로드맵 2023(블록체인 분야), 2018

[8] 김진호, "블록체인 진화의 끝은? 세대별 발전 과정 살펴보니…," 동아사이언스, 2018. 2. 22.

[9] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," Ripple Labs Inc., 2014, pp. 1-8.

[10] Litecoin, "What is the Difference between Litecoin and Bitcoin?" Available: https://www.coindesk.com/information/comparing-litecoin-bitcoin/

[11] C. Dwork and M. Naor, "Pricing via Processing or Combating Junk Mail," In *Lecture Notes in Computer Science*, vol 740, Springer: Berlin, Heidelber, 1992, pp. 139-147.

[12] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Programming Languages Syst.*, vol. 4, no. 3, July 1982, pp. 382-401.

[13] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *Proc. Symp. Oper. Syst. Des. Implementation*, New Orleans, LA, USA, Feb. 1999, pp. 1-14.

[14] Bitcoin, "Bitcoin Developer Guide," Available: https://bitcoin.org/en/developer-guide

[15] C. Harper, "2018 Recent and Upcoming Bitcoin Hard Forks: What You Need to Know," Coin Central, Dec. 18, 2017. Available: https://coincentral.com/the-upcoming-bitcoin-hard-forks-what-you-need-to-know/

[16] J. Cross, "Segregated Witness," GITHUB. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[17] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments(draft)," Nov. 20, 2015. Available: https://www.weusecoins.com/assets/pdf/library/Lightning%20Network%20Whitepaper.pdf

[18] V. Buterin, "A Next Generation Smart Contract & Decentralized Application Platform," Ethereum white paper, 2015. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[19] 박재현, "코어 이더리움," Available: https://www.slideshare.net/jaehyun/ss-80672715.

[20] N. Szabo, "Smart Contracts," 1994. Available: http://szabo.best.vwh.net/smart.contracts.html

[21] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," Sept. 11, 2017. Available: http://517shangke.com/static/file/4236615__qq__com__1505925043620719.pdf

[22] V. Zamfir, "A Template for Correct-by-Construction Consensus Protocols (draft v0.01)," Nov. 2, 2017. Available: https://github.com/ethereum/research/blob/master/papers/cbc-consensus/AbstractCBC.pdf

[23] D. Siegel, "Understanding the DAO Attack," June 25, 2016. Available: https://www.coindesk.com/understanding-dao-hack-journalists/

[24] D. Dedi, "Ethereum's Raiden Network: An Off-Chain Solution to Scalable Payments," CryptoSlate, Jan. 1, 2018. Available: https://cryptoslate.com/ethereums-raiden-network- off-chain-solution-scalable-payments/

[25] GITHUB, "Ethereum Sharding," Accessed 2017. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[26] J. Poon and V. Buterin, "Plasma: Scalable Autonomous Smart Contracts(working draft)," Aug. 11, 2017. Available: http://plasma.io/plasma.pdf.

[27] J. Teutsch, C. Reotwiessner, "A Scalable Verifi-cation Solution for Blockchains," Nov. 16, 2017. Available: https://people.cs.uchicago.edu/~teutsch/papers/ truebit.pdf

[28] Hyperledger Fabric, Available: https://www.hyperledger.org/projects/fabric.

[29] G. Lee, "EOS.IO Technical Whitepaper V2.0," GITHUB, June 5, 2017. Available: https://github.com/EOSIO/ Documentation/blob/master/TechnicalWhitePaper.md

[30] P. Dai et al., “Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform,” Technical Report, Mar. 2017. Available: https://qtum.org/user/pages/03.tech/01.white-papers/Qtum%20Whitepaper.pdf

[31] J. Scianna, “Qtum introduces Decentralized Governance Protocol to Manage Blockchain Network,” June 6, 2017. Available: https://www.prnewswire.com/news-releases/qtum-introduces-decentralized-governance-protocol-to-manage-blockchain-network-300469513.html

[32] XBT Network, “What is Cardano?” June 21, 2018. Available: https://xbt.net/blog/what-is-cardano

[33] Cardano, “Why we are Building Cardano-Introduction,” Available: https://whycardano.com/

[34] A. Kiayias et al, “Ouroboros: A Provably Secure Proor-of-Stake Blockchain Protocol,” Aug. 21, 2017, *Proc. Crypto 2017*, pp. 357-388.

[35] Energist, “카르다노, 에이다] #2 확장성(1),” Steemit, 2018. Available: https://steemit.com/ada/@energist/2-1

[36] NEO, “NEO Whitepaper: A Distributed Network for the Smart Economy,” Available: http://docs.neo.org/en-us/index.html

[37] S. Popov, “The Tangle,” Oct. 1, 2017. Available: http://iotatoken.com/IOTA_Whitepaper.pdf

[38] BOScoin 백서, “BOScoin White Paper 2.0,” Available: https://boscoin.io/about/#papers

[39] ICON 백서, “ICON: Hyperconnect the World,” Available: https://icon.foundation/?lang=en

[40] Ground X, “그라운드 X, 블록체인 플랫폼 ‘클레이튼(Klaytn)’ 공개,” Avaliable: https://tconomy.io/1989.

[41] 블로코, “OpenKeyChain Whitepaper,” Avaliable: https://coinstack.zendesk.com/hc/ko/articles/215479208-OpenKeyChain-Whitepaper