Vol.8, No.1, March (2019), pp.45-58
http://dx.doi.org/10.29056/jncist.2019.03.05

블록체인의 태동, 현재 그리고 미래

The Beginning, Present and Future of the Blockchain

한형성[1], 배수진[2]*, 김진태[3]

Hyung-Sung Han[1], Su-Jin Pae[2]*, Jin-Tae Kim[3]

요약

본 연구는 블록체인의 역사를 태동기, 확장기, 확산기로 구분하여, 각 시기별로 블록체인 기술의 주요 특징과 쟁점들을 살펴보았다. 2008년 비트코인으로 시작된 블록체인은 네트워크 사용자간의 직접적인 P2P방식을 통하여 거래의 효율성, 신속성, 보안성을 실현할 수 있는 기술적 특징을 가지고 있는 것으로 평가되었지만, 발행량 제한, 블록크기 제한, 에너지 과소비, 사용자 비친화적인 특성 등이 문제로 제기되었다. 2013년 '탈중앙화된 블록체인 플랫폼'을 목표로 만들어진 이더리움의 탄생은 블록체인의 확장기로 볼 수 있다. 이더리움은 블록체인의 태동기에 만들어진 비트코인의 한계점을 보완하는 기술로 발전하였다. 이러한 이더리움은 다양한 산업영역에서 적용할 수 있는 디앱(Dapp)의 개발과 스마트 계약을 가능하게 했지만, 거버넌스 문제, 스마트 계약의 비가역성 문제, 수수료 기반 처리시스템이 가진 문제 등이 해결해야 할 과제로 나타났다. 2017년부터 시작된 확산기에는 다양한 알트코인이 비트코인과 이더리움이 가지고 있던 한계들을 뛰어 넘어 블록체인 기술이 다양한 산업분야에서 적용될 수 있는 가능성을 보여주었다. 그러나 암호화폐와 블록체인과의 관계, 블록체인 알고리즘의 결정 문제, ICO의 법적 허용 여부와 관련한 문제가 해결해야 될 쟁점들로 부각되었다. 2008년부터 현재까지 진행된 블록체인 기술의 각 시기별 특징과 문제점을 살펴본 본 연구는 블록체인 기술의 역사적 발전과정과 블록체인과 관련하여 현재 제기되는 쟁점들을 이해하는 것을 도와서 향후 블록체인 연구를 위한 기초자료를 제공할 수 있을 것으로 기대된다.

핵심어 : 블록체인, 비트코인, 이더리움, 알트코인, 암호화폐

Abstract

This study divided the history of the blockchain into the beginning, expanding and spreading period, looking at the major features and issues of blockchain technology for each period. In 2008, Bitcoin was assessed to have technical features that enable the efficiency, speed and security of transactions through direct P2P transaction between network users. However, issues such as limited quantity of coin mining, small block size, overconsumption of energy, and user-unfriendly characteristics were also problematic. Ethereum was developed in 2013 with the aim of 'decentralized blockchain platform' to enable DApp(decentralized application) and smart contract by using Ethereum. However, governance in network,

1 Da Vinci College of General Education, Chung-Ang University, Seoul, Korea [Professor]
e-mail : han176411@cau.ac.kr
2 Da Vinci College of General Education, Chung-Ang University, Seoul, Korea [Professor]
e-mail : sjpae@cau.ac.kr (Corresponding author)
3 Da Vinci College of General Education, Chung-Ang University, Seoul, Korea [Professor]
e-mail : jtkim0811@cau.ac.kr

Received(February 06, 2019), Review Result(1st: February 21, 2019), Accepted(March 08, 2019), Published(March 31, 2019)

ISSN: 2384-101X JNCIST

the irrevocability of smart contracts and transaction processing based on fees were issues to be addressed. Various kinds of Altcoin showed the possibility that blockchain technology can be applied to various industries during the spreading period that started in 2017. On the other hand, however, issues such as the relationship between cryptocurrency and blockchain, the decision of the blockchain algorithm and whether ICO(initial coin offering) should be legally permitted have emerged as issues. Examining the characteristics and problems of each historical period of the blockchain technology from 2008 to the present, this study is expected to provide the basis for future blockchain studies by helping to understand the blockchain development process and issues raised with blockchain technology.

Keyword : Blockchain, Bitcoin, Ethereum, Altcoin, Crypto Currency

1. 서론

모든 금융거래와 경제활동은 정부, 은행, 카드사 등의 중앙집중식 인증 체계에 의해 통제·조정되지만, 암호화폐와 블록체인 기술의 시작은 이러한 중앙집중식 기존 질서에 대한 반발로부터 시작되었다[1]. 암호화폐는 1980년대 중반 이후에 미국을 중심으로 등장한 사이퍼펑크(cypherpunk) 운동에서 그 기원을 찾을 수 있다[2][3]. 사이퍼펑크는 암호를 뜻하는 사이퍼(cipher)에 저항을 의미하는 펑크(punk)를 붙인 합성어로, '암호화 기술에 기반하여 기존의 중앙집권화된 국가나 기업 등 대규모 구조에 저항하는 문화'를 의미한다. 사이퍼펑크 활동가인 Eric Hughes는 사이퍼펑크 선언문을 통해, 익명성을 유지해 프라이버시를 보호하면서 열린 거래와 커뮤니케이션을 가능하게 하는 암호기술을 개발할 것을 제시하였다[1].

2008년 미국 발 서브프라임모기지 사태는 아시아와 유럽을 비롯한 전 세계에서 경제 상황에 따라 화폐의 상대적 가치가 예측할 수 없을 만큼 급락하는 상황이 발생될 수 있음을 보여주었다. 이 시기에 리먼브라더스, 메릴린치, 베어스턴스 등 미국 최대 규모의 중앙화된 금융기관들이 파산하거나 다른 회사에 인수되었고, 이를 통해 탈중앙화 블록체인과 암호화폐의 정당성이 부각되었다. 이처럼 세계금융위기는 사람들의 금융시스템에 대한 인식의 변화를 가져왔으며, 비트코인 블록체인은 2008년 기존 화폐 및 금융 시스템에 대한 신뢰를 새롭게 구축할 수 있는 대안으로 탄생했다.

블록체인의 태동은 비트코인의 탄생으로 시작이 되었으며, 이로 인해 블록체인과 비트코인을 혼용하여 사용하고 있다. 비트코인은 해킹에 대한 보완성이 강하다는 특징으로 인해 비트코인을 암호화폐라고도 한다. 비트코인은 블록페인 기술을 기반으로 한 암호화폐의 하나이다. 즉, 블록체인 기술은 비트코인에서 이더리움으로 그리고 이더리움에서 하이퍼이레져로 지속적으로 발전하고 있으며, 향후 민간은 물론 정부 및 공공 서비스에서도 활용이 가능할 것으로 예상되는 기술이다.

이와 같은 관점에서 본 연구는 블록체인 기술의 한 종류인 암호화폐를 중심으로 블록체인에 대한 역사적 변천과정을 살펴보고자 한다. 이와 같은 연구목적을 달성하기 위하여 본 연구는 블록체인 기술의 개념과 특성을 우선 살펴보고, 블록체인 기술의 한 종류인 암호화폐에 대하여 태동기(2009~2013년), 확장기(2013~2016년), 확산기(2017~현재)로 시기를 나누어 각 단계에서의 기술적 특

징과 한계가 무엇인지에 대한 역사적 고찰을 하고자 한다.

2. 블록체인 개념과 변천과정

2.1 블록체인의 개념과 장점

블록체인은 데이터를 기록한 원장(Ledge)를 P2P(peer-to-peer) 네트워크에 분산하여 모든 거래 참가자가 공동으로 기록하고 관리하기 때문에 분산장부기술이라고도 불린다[4]. 이러한 블록체인은 거래 원장의 복사본이 각 네트워크 구성원에게 '분산되어(Distributed)' 새로운 거래가 발생할 때마다 구성원들의 동의를 통해 해당 거래를 인증한다[5].

기존 거래 방식의 경우 거래 참가자들의 거래를 명확하게 하기 위한 중앙 집중화된 시스템이 필요했다. 또한 이러한 시스템을 통해 거래가 이루어지기 때문에 거래가 상대적으로 복잡하며, 비용이 수반되는 한계점이 존재했다. 그러나 블록체인은 중앙 집중화된 시스템 없이 P2P 네트워크 방식에 기반하여 거래가 인증되기 때문에 상대적으로 거래의 효율성이 높고 비용이 적은 장점이 있다.

블록체인에 기반한 거래에서는 모든 거래가 네트워크 참여자들에게 개방되며 새로운 정보 또한 실시간으로 동시에 업데이트된다. 따라서 하나의 거래정보를 임의로 변경하는 형태의 해킹이 불가능하다. 즉, 해킹을 통해 거래를 왜곡하기 위해서는 모든 네트워크 참여자들의 정보를 해킹해야만 하는데, 이는 현실적으로 불가능하다[5].

한국은행 금융결제국[6]이 밝힌 블록체인 기술의 장점은 다음과 같다. 첫째, 블록체인의 분산원장기술은 암호화된 데이터와 암호화된 키(key) 값으로만 거래가 이루어지기 때문에 보안성이 높다. 또한 새로운 블록은 기존의 블록과 연결되기 때문에 전체 블록 안의 데이터에 대한 해킹이 불가능하다. 둘째, 거래의 인증과 증명과정에서 제3자를 배제시키는 실시간 거래가 이루어지기 때문에 거래기록의 신뢰성이 높으며, 거래의 효율성 및 속도가 향상된다. 셋째, 기존 거래의 경우 중앙 집중화된 시스템이 필요하기 때문에 비용이 수반되지만, 블록체인 기술은 중앙 집중화된 시스템이 필요로 하지 않기 때문에 상대적으로 비용이 낮다. 넷째, 블록체인 기술은 네트워크 참여자들의 실시간 거래 모니터링이 가능하기 때문에 가시성이 높다.

2.2 비트코인의 탄생 및 특징

비트코인은 2008년 10월 Satoshi[7]가 “Bitcoin: A Peer-to-Peer Electronic Cash System”이라는 제목의 논문을 인터넷에 공개하면서 알려지게 되었다. 그는 기존의 인터넷을 통한 전자지불 방식이 비가역적인 거래가 사실상 불가능하기 때문에 금융기관이 금융분쟁을 중재해야만 하는 내재적 약점

이 있다고 했다. 그리고 금융기관의 이러한 중재비용은 거래 수수료 인상, 실질적 최소 거래금액의 제한, 소액거래의 가능성에 대한 제약 등의 원인으로 더 많은 비용을 발생한다고 보았다. 그는 암호화 기술에 기반한 전자지불 시스템을 이용하여 두 거래자가 제3자인 신용기관 없이 직접적인 거래를 통해 해결이 가능하다고 보았다.

Satoshi[7]는 전자 화폐를 디지털 서명의 연속으로 정의하였다. 즉, 각 암호키 소유자들은 거래 내역에 다음 소유자의 공개키를 덧붙인 뒤 자신의 비밀키로 암호화하는 디지털 서명을 하고 넘기며, 돈을 받는 사람은 서명 소유자들의 체인과 서명을 검증할 수 있다. 돈을 받는 사람이 이전 소유자가 그 전에도 어떤 거래에도 서명을 하지 않았는지를 확인할 방법이 있다면 중앙기관이 거래에 개입될 필요가 없어지게 되는 것이다. 따라서 모든 거래가 공개적으로 알려지게 되고, 참여자들이 시간 순서에 따라 단일 거래내역으로 수용하는 시스템이 존재한다면, '이중지불(double spending)'에 대한 문제는 발생하지 않으며 중앙기관이 거래에 개입할 필요성도 없어지게 된다. 네트워크의 동작은 다음과 같은 과정으로 이루어진다.

① 새로운 거래 내역이 모든 노드에 알려진다.
② 각 노드들은 새로운 거래 내역을 블록에 취합한다.
③ 각 노드들은 그 블록에 대한 작업증명을 찾는 과정을 수행한다.
④ 어떤 노드가 작업증명을 성공적으로 수행했을 때, 모든 노드에게 그 블록을 전송한다.
⑤ 노드들은 그 블록이 모든 거래가 이전에 쓰이지 않고 유효한 경우에만 승인한다.
⑥ 노드들은 자신이 승인한 블록의 해시를 이전 해시로 사용하여 다음 블록을 생성하는 과정을 통해 그 블록이 승인되었다는 의사를 나타낸다.

비트코인은 2009년 1월 3일 최초로 발행(Genesis Block)되었으며, 2009년 10월 5일에는 법정통화로 환전이 가능해졌다. 2010년에는 실제 매장에서 암호화폐를 이용한 최초의 결제가 이루어졌다. 이어 2010년 7월에는 일본의 암호화폐거래소인 마운트곡스가 비트코인 환전서비스를 개시했다[8]. 비트코인 가격은 2011년 2월 최초로 1달러를 넘었고, 이후 2013년 1,000달러를 돌파했다. 2013년 마운트곡스의 거래량은 전세계 비트코인 거래량의 약 70%에 달하는 최대 거래소로 자리 잡았다. 그러나 2014년 초 마운트곡스는 85만 비트코인, 당시 가치로는 4억 7,300만 달러가 해킹당하는 사건으로 모든 거래를 중단하였고[9], 이후 청산절차를 밟았으며 현재는 기업회생절차로 전환되었다.

블록체인 기술의 핵심적 특징은 다음과 같다[10]. 첫째, 탈 중개성(분산성)이다. 탈 중개성이란 신뢰된 제3자 없이 분산형 네트워크(P2P) 환경에서 개인 간 거래가 가능하도록 한 것이다. 이는 불필요한 거래수수료를 절감하고 결제처리속도를 향상(신속성)시킬 수 있다. 둘째, 효율성이다. 중앙집중형 시스템을 운영하므로 시스템 오류, 해킹 등 보안사고 방지를 위한 유지보수비용이 절감되

어 운영의 효율성이 강화된다. 셋째, 확장성이다. 쉽게 블록을 구축하여 연결할 수 있어 새로운 아이디어의 손쉬운 수용이 가능하여 확장성이 탁월하다. 넷째, 투명성이다. 모든 거래기록을 공개하므로 투명성이 높으며 거래 양성화에 적합하다. 다섯째, 보안성이다. 모든 참가자에게 원장이 공개되기 때문에 원천적으로 정보 유출 소지가 없어 안전하다. 여섯째, 안정성이다. 블록체인은 모든 참여자에게 동일한 정보가 담긴 파일을 분산 저장 관리함으로, 일부 참가 시스템에 오류나 성능저하 발생 시에도 전체 네트워크에 미치는 영향이 미미하여 안정적이다. 마지막으로, 취소불능 및 불변성에 있다. 블록체인은 변경이 불가능하고(신뢰성) 거래가 취소불능하기 때문에 기록의 정확성이 증가된다.

한국은 2017년부터 2018년 초까지 비트코인 열풍에 휩싸였다. 비트코인을 포함한 암호화폐 시장에 글로벌 투자자금의 유입이 크게 증가하였으며 비트코인의 가격이 급격히 증가하여 2017년 12월 시가총액이 사상 최고치인 3,261억 달러를 기록하였다. 그러나 이후 지속적으로 하락하여 2018년 9월말 현재 1,138억 달러(1BTC=6,578.77달러)로, 전년 최고가 대비 60% 이상 규모가 축소됐다. 한국의 경우 비트코인의 시세는 2018년 1월 초에는 2,500만 원까지 상승해 사상 최고가를 기록했다가, 2018년 9월 말 현재 730만 원대를 기록하여 최고가 대비 70% 가격이 하락했다.

2.3 비트코인의 기술적 한계

비트코인의 전체 발행량은 2,100만개로 제한되어 있고, 대략 4년마다 발행량이 절반씩 줄어드는 반감기를 거치기 때문에, 어느 특정 시점이 되면 인플레이션을 유발할 가능성이 있다[11]. Satoshi[7]는 이와 관련하여 “채굴자(miners)는 채굴한 전체 코인양이 사전에 설정된 통화량에 이르면 거래 수수료로 보상받게 된다”고 밝혔다. 그러나 거래 수수료의 상승은 결국 비트코인의 이용 가능성을 떨어뜨리는 부작용을 낳을 수 있다.

비트코인의 블록크기는 1MB로 제한되어 있기 때문에 블록체인 네트워크의 거래량이 증가할 경우에 거래처리 속도가 느려진다는 기술적 한계가 있다. 이 문제를 해결하기 위해서는 블록 크기를 현재의 1MB에서 늘려서 각 블록이 담을 수 있는 거래 수를 늘리거나 기존의 블록구조를 그대로 유지하면서 비트코인 블록에서 서명 부분만을 떼어내어 체인을 만들고, 비트코인의 거래 내역을 담은 블록 테이터는 별도로 저장하는 세그윗(Segwit)이라는 방법이 있다[11]. 비트코인의 블록크기 확장과 관련하여 어떤 방법을 사용할 것인가를 두고 비트코인 네트워크에서 갈등과 이에 따른 분열이 나타났다.

비트코인의 합의알고리즘은 작업증명(PoW: Proof of Work)방식을 채택하고 있는 데, 이 방식은 많은 전기에너지를 필요로 한다. 디지코노미스트가 발표하는 ‘비트코인 에너지 소비 지표’에 따르면, 2018년 7월 31일 현재 비트코인을 채굴하는 전체 컴퓨터가 소비하는 전력은 연간 73.12 테라와트시(TWh)으로, 이는 한국의 2017년 주택용 연간 전력 사용량 72.09 테라와트시(TWh)보다도 크다.

이론적으로 비트코인 네트워크 전체의 51% 지분을 가진 단체나 조직이 존재한다면 비트코인 블록체인 상의 모든 채굴 풀(mining pool)을 공격하거나 최소한 어지럽힐 수 있다[12]. 전문가들은 우지한(吳忌寒)이 '비트코인 캐시(Bitcoin Cash)'로 하드포크에 성공한 것을 사례로 들어 비트코인 네트워크에서의 민주주의에 대하여 우려를 표명한다.

비트코인은 보통사람이 접근하기 어려운 사용자 비친화적 인터페이스를 가지고 있다[12]. 따라서 개발자들이 비트코인 블록체인을 이용하여 전자화폐 결제 용도 이외의 다른 용도에 이용할 새로운 소프트웨어를 개발하기 어렵다는 문제가 있다.

2.4 이더리움의 기술적 특징

Vitalik[13]은 비트코인의 핵심 프로토콜이 소프트웨어 개발자가 사용자 친화적인 애플리케이션을 만들기에는 너무 까다롭게 되어있다는 점을 지적하며, 개발자들이 시장에서 필요하다고 생각하는 모든 형태의 애플리케이션을 직접 만들 수 있는 '탈중앙화된 블록체인 플랫폼'을 제안했고, 이 플랫폼을 이더리움이라고 불렀다. 이더리움 블록체인은 기존의 비트코인 블록체인과는 다른 다음과 같은 기술적 특징이 있다.

첫째, 이더리움의 가장 큰 기술적 특징은 내부 프로그래밍 언어가 '튜링 완전성'을 가지고 있기 때문에 다양한 디앱(DApp: Decentralized Applications)'을 만드는 것이 가능하다는 것이다[14]. 즉 이더리움에서는 컴퓨터로 동작시킬 수 있는 모든 소프트웨어 프로그램을 만들어 실행할 수 있다. Vitalik[13]은 이더리움의 목적이 "분산 애플리케이션을 만들기 위한 대체 프로토콜을 만드는 것"이며, "튜링완전언어를 내장하고 있는 블록체인이라는 필수적이고 근본적인 기반을 제공함으로써 이 목적을 이루고자 한다"라고 밝혔다. 2014년 북미 비트코인 컨퍼런스에서 Vitalik[13]이 "디앱(DApp)을 위한 안드로이드를 만들고 싶었다"는 말은 이더리움이 구글의 스마트폰 운영체제처럼 개방된 플랫폼으로서 기능하며, 사람들이 원하면 어떠한 애플리케이션이든 이더리움을 기반으로 만들 수 있다는 것을 의미한다[14].

둘째, 스마트 계약이 가능하다. 스마트 계약은 사전에 정해진 계약조건에 따라서 자동으로 거래가 이루어지는 것을 말하며, '코드가 곧 법(code is law)'이라는 말은 스마트 계약의 핵심을 가장 잘 표현한다. 현재의 계약체계에서는 계약 내용을 종이에 적고, 계약 당사자가 서명을 하며, 상대방이 계약사항을 지키지 않을 때는 법률적 강제에 의하여 분쟁을 해결하지만, 스마트 계약에서는 계약 이행을 위한 조건이 소프트웨어의 코드(code)로 되어 있기 때문에 조건이 만족되면 계약이 '자동적'으로 집행되며, 조건이 지켜지지 않는 경우에는 계약이 집행되지 않기 때문에 법률적 강제가 필요 없다[11].

셋째, 전통적 조직에서는 경영자나 관리자가 있고 그들이 다양한 판단을 함으로써 조직을 운영한다. DAO에서는 관리자를 따로 두지 않고 DAO 멤버들이 자산을 공유하고 운용결정에 참여하며,

경영은 사전에 합의한 코드에 따라서 자율적으로 결정하고 실행하기 때문에 경영자가 없어도 되는 자율조직이 만들어 진다[15].

2.5 이더리움의 문제점

Vitalik[13]을 비롯한 이더리움 초기 개발자들의 과도한 부의 축적과 이더리움 네트워크에서의 지배적 영향력은, 이더리움 초기 개발자들의 이익과 다른 사용자들과의 이익이 충돌할 경우 거버넌스(governance)에 문제가 생길 수 있다는 것을 의미한다[14]. 대표적인 사례가 2016년 6월의 DAO 해킹사건으로 DAO 스마트 계약의 취약점을 이용하여 당시 발행된 이더의 10%인 360만개의 이더를 해킹한 사건이다. Vitalik[13]을 비롯한 이더리움 창시자들은 해커가 더 이상 자금을 빼내는 것을 막기 위해서 이더리움 블록체인에 대한 '하드포크(hard fork)'를 단행하여, 해커들의 거래내역을 모두 무효화시키고 이더리움의 이전 버전과 호환이 불가능하게 만들었다. '하드포크'에 대해서 반대한 그룹은 DAO를 공격한 해커의 기록이 그대로 담겨있는 하드포크 이전의 버전으로 이더를 계속 채굴하고 거래하기로 결정했다. 그들은 이 버전을 '이더리움 클래식(ETC)'이라고 하여 2016년 7월 암호화폐 거래소에 전격 상장하여, 결국 이더리움은 ETH와 ETC라는 두 개의 블록체인으로 나뉘게 되었다. DAO 해킹사건에 대한 대처과정에서 나타난 이더리움 블록체인의 내부 분열은 네트워크 참여자들의 이익이 상충될 때 누가 어떻게 해결해야 하는가라는 이더리움 블록체인의 거버넌스에 대한 의문을 제기했다.

이더리움의 스마트 계약은 코드에 따라서 계약이 자동적으로 실행되면 취소하거나 변경할 수 없다. 그러나 일상생활의 실제 계약에서는 계약의 특성이나 계약 상대방의 처지와 조건에 맞추어서 계약내용이 변경되거나 조정될 수 있다. 예를 들어, 채무자가 원금과 이자 상환의 의무를 해태한 경우에 채권자는 손실을 줄이기 위하여 채무자의 부채 일부를 경감해주거나 만기를 연장해줄 수 있다. 그러나 이더리움의 스마트 계약은 소프트웨어 코드에 정한 모든 조건이 충족되면 자동으로 집행되며 변경이 불가능하기 때문에 사람들은 자동화된 스마트계약이 가지는 불가역성, 즉 수정불가능성에 불편을 느낄 수 있다[14].

이더리움 블록체인을 이용한 거래에서 수수료를 부과하는 이유는 채굴자의 노력에 대한 보상이자 디도스 공격을 방지하기 위한 것이다[11]. 수수료가 너무 낮으면 공격자들이 네트워크 자체를 마비시키기 위한 목적으로 인위적으로 대량 거래를 만들어서 네트워크를 마비시키는 디도스 공격에 취약해지는 약점이 있으며, 수수료가 너무 높으면 이용자의 이더리움에 대한 접근가능성을 떨어뜨리는 딜레마를 가지고 있다[11]. 또한 이더리움의 수수료는 이용자가 스스로 정할 수 있는데, 수수료를 높게 책정할수록 그 거래가 이더리움 블록체인에서 우선적으로 승인될 가능성이 높기 때문에[15], 낮은 수수료를 지급하는 디앱(DApp)은 그 기능이 우수하더라도 처리가 상대적으로 지연되거나 실행되지 못할 가능성이 있다.

2.6 알트코인의 기술적 특징

2009년 비트코인의 탄생 이후 수많은 알트코인이 나타났으며, 2018년 9월 말 현재 코인마켓캡(coinmarketcap)에 등록된 암호화폐의 수는 2,004개에 달하며, 각 암호화폐는 고유의 기술적 차별성과 활용 가능성을 강조하고 있다. 지금 단계에서는 어느 알트코인이 기존의 비트코인과 이더리움 블록체인의 한계를 뛰어 넘어 그 기술적 타당성과 이용 가능성을 보여줄지를 판단하기 힘들다. 따라서 현재 암호화폐 거래소에서 비트코인과 이더리움 다음으로 시가총액 비중이 높은 리플(Ripple), 비트코인캐쉬(Bitcoin Cash), 이오스(EOS), 스텔라(Stellar), 라이트코인(Litecoun)을 중심으로 그 기술적 특징을 기술한다. [표 1]은 주요 알트코인의 종류와 특징을 요약한 것이다.

[표 1] 주요 알트코인의 종류와 특징
[Table 1] Category and Characteristic of Altcoin

알트코인 (Altcoin)	시가총액($) Market Value($)	가격($) Price($)	총 발행한도(개) total Issuance limit(EA)	합의 알고리즘 (algorithm)
리플 (XRP)	21,241,397,580	0.53	100,000,000,000	RPCA
비트코인캐쉬 (BCH)	9,017,191,497	519.00	21,000,000	PoW
이오스 (EOS)	5,122,505,879	5.65	없음	DPOS
스텔라 (XLM)	4,673,318,350	0.24	없음	SCP
라이트코인 (LTC)	3,518,189,264	60.14	84,000,000	PoW

3. 블록체인과 관련된 주요 쟁점

3.1 암호화폐가 없는 블록체인

암호화폐와 블록체인을 별개로 다루는 것이 가능한가라는 쟁점은 공개형 블록체인(public blockchain)과 허가형 블록체인(permissioned blockchain) 가운데 어느 형태의 블록체인이 확산되어야 할지에 대한 물음과 직접적으로 관련되어 있다. 최근 한국의 중소벤처기업부가 '벤처기업 육성에 관한 특별조치법 시행령' 개정안을 발표하면서 '암호화폐 매매와 중개업'을 벤처기업에서 제외한 조치에 대하여, 블록체인 관련협회와 단체들이 "암호화폐 거래소가 블록체인 생태계의 핵심인데 이를 막고 4차 산업을 독려하겠다는 것은 앞뒤가 맞지 않는다"며 크게 반발한 것도 암호화폐와 블록체인의 관계를 둘러싼 갈등이 심각함을 보여준다[16]. [표 2]는 공개형 블록체인과 허가형 블록체인의 차이를 요약한 표이다.

[표 2] 공개형 블록체인과 허가형 블록체인
[Table 2] Open Blockchain and Permission Blockchain

구분 (Classification)	공개형 블록체인 (Open Blockchain)	허가형 블록체인 (Permission Blockchain)
거래 참가자에 대한 제한	없음. 자유롭게 참가 가능	있음. 특정 범위의 참가자로 제한
거래 승인에 대한 참가 제한	없음. 자유롭게 참가 가능	있음. 특정 범위의 참가자로 제한
중앙 관리자 존재	없음. 프로그램이 규정	있음. 전체 네트워크 통제
네트워크 참가승인	승인 필요 없음	승인 필요
다른 명칭	public blockchain	consortium/private blockchain

암호화폐와 블록체인을 분리하는 것이 가능하지 않다고 주장하는 사람들은 블록체인과 암호화폐와의 관계를 자동차와 연료의 관계로 비유한다. 즉 암호화폐라는 연료가 없다면 블록체인이라는 자동차는 고철에 불과하다는 것이다. 김재윤[17]은 비트코인 블록체인을 창시한 Satoshi의 천재성은 블록체인 네트워크의 탈중앙화 실현과 해킹에 대한 보안을 '기술'에서 찾은 것이 아니라 블록체인 네트워크에 참여하는 참여자들(노드)의 '경제적 동기'에서 찾았다는 것을 강조한다. 즉 비트코인 블록체인의 핵심은 암호화폐이며, 비트코인이라는 경제적 보상이 주어지지 않는다면 참여자는 탈중앙화 된 블록체인을 유지하고 외부의 해킹 공격으로부터 네트워크를 유지하기 위하여 자신의 컴퓨팅 자원을 제공하지 않을 것이다. 결국 블록체인에서 암호화폐가 없다면 분산된 네트워크의 참여자에 의해서 거래검증이 가능한 경제적 보상 시스템이 무너지는 것이고, 이는 결국 소수의 참여자만 이용하는 '허가형 블록체인'으로 귀결될 것이라고 주장한다. Casey and Vigna[14]는 "2008년 세계금융위기의 근본 원인이 전통적인 금융기관들로 대표되는 문지기(gate keeper) 권력 때문이었으며 이에 대한 대안으로 탈중앙화 된 블록체인이 등장한 것인데, 이 사실을 간단히 무시해버리고. 허가형 블록체인을 도입하겠다는 것은 2008년의 위기로 되돌아 가겠다"는 것이라고 주장한다.

암호화폐 없는 블록체인이 가능하다고 주장하는 사람들은 블록체인 참여자들의 합의구조에서 반드시 암호화폐가 필요한 것은 아니라고 주장한다. 그들은 허가형 블록체인에서는 참여자의 신원확인이 가능하고, 외부로부터의 보안성이 뛰어나며, 공개형 블록체인과 비교하여 비용절감과 효율성 제고를 가져올 수 있으며, 전체 시스템의 통제와 관리가 비교적 용이하다는 장점이 있다고 주장한다[14]. Nakajima[18]는 금융 분야에서는 높은 보안성이 가장 우선적으로 요구되며, 만약 금융거래에서 어떤 문제가 발생했을 때 부정한 거래를 적발하고, 부정거래자를 네트워크에서 배제하며, 책임주체를 명확히 하기 위해서는 공개형 블록체인의 도입이 힘들다고 주장한다.

암호화폐에 대한 투기적 수요와 암호화폐 거래소에 대한 해킹 등의 문제가 발생했던 한국의 경우, 공개형 블록체인의 도입은 더욱 신중할 필요가 있으며, 공개형 블록체인만 인정할 수 있다는 주장은 너무 독단적일 수 있다. 또한 공공분야의 효율성을 높일 목적으로 국가 주도로 블록체인을

도입하는 경우, 공개형 블록체인에서 강조하는 블록체인 네트워크 참여자의 경제적 보상구조가 상대적으로 중요하지 않을 수 있다.

그러나 공개형 블록체인이 없는 상태에서 허가형 블록체인만이 유일한 대안이라고 생각하는 것은 단기적 시야의 편의주의적 발상으로 볼 수도 있다. 허가형 블록체인만으로도 비용 절감과 효율성 제고의 목적을 달성할 수 있지만 이것은 공개형 블록체인이 가져올 수 있는 전체 혜택의 일부분에 불과하며 장기적인 관점에서의 효용성도 제한될 것이라는 주장이 설득력을 가진다.

3.2 블록체인의 합의알고리즘

공개형 블록체인과 허가형 블록체인 가운데 어느 하나를 선택하는 것은 합의알고리즘의 선택과 직접적으로 관련이 있다. 공개형 블록체인은 불특정 다수가 참여하기 때문에 작업증명(PoW) 방식처럼 참여자의 시간과 노력이 많이 들도록 하여 악의적 참여자를 거래에서 배제할 수 있는 합의알고리즘을 선택해야 하는 반면에, 허가형 블록체인에서는 신뢰할 수 있는 일부 참가자의 합의에 의해서 거래를 승인할 수 있기 때문에 리플과 같은 자체적으로 개발한 간단한 합의 알고리즘을 선택할 수 있다[18]. [표 3]은 블록체인 알고리즘의 유형별 특징과 적용된 암호화폐가 무엇인지를 보여주고 있다.

[표 3] 볼륵체인 합의 알고리즘

[Table 3] Consensus Algorithm of BlockChain

합의 알고리즘	특징 (Characteristic)	적용 암호화폐 (cryptocurrency case)
작업증명 (PoW)	컴퓨터로 암호를 풀어, 가장 먼저 푼 참여자가 블록을 생성하는 방식. 고성능컴퓨터가 필요하기 때문에 높은 전기에너지를 사용하며, 거래승인속도가 상대적으로 느리다.	비트코인(Bitcoin) 비트코인 캐쉬(Bitcoin Cash) 이더리움(Ethereum)
지분증명 (PoS)	지분을 많이 가진 참여자가 네트워크의 가치를 하락시키는 일을 하지 않으리라는 가정아래, 참여자의 화폐 소유 지분이 클수록 블록생성 권한을 더 많이 부여하는 방식(임종철 외 2018). PoW처럼 막대한 전기요금을 부담할 필요가 없으며, 거래처리속도가 상대적으로 빠르지만 소수에 의한 네트워크지배가 가능하다는 단점이 있다.	피어코인(Peercoin) 이더리움(Ethereum)은 PoW에서 PoS로 변경 예정
위임지분증명 (DPOS)	검증 노드와 비검증 노드를 구별하여, 일정 비율 이상의 검증 노드의 합의에 의해서 거래를 승인하는 방식. 검증 노드끼리의 합의로 거래가 승인되어 신속하고 확실한 가치의 이전이 가능하며, 일정 시간에 많은 거래를 처리할 수 있다.	이오스(EOS) 비트쉐어(Bitshares) 스팀(Steem)

블록체인이 처음 세상에 모습을 드러냈을 때는 기존 플랫폼의 인간 또는 자본에 의한 중앙 집중식의 의사결정구조를 자동화된 코드와 분권화된 의사결정구조로 대체할 수 있을 것으로 기대했

지만, 비트코인, 이더리움이 채택하고 있는 작업증명(PoW)방식의 합의알고리즘은 연산량이 늘어나면서 자본력이 없는 개인에게 진입 장벽이 높아지고, 대량채굴 전용 칩과 비교적 싼 전기료를 사용하는 채굴자에게 권력이 집중되는 문제를 낳았다[19]. 지분증명(PoS), 위임 지분증명(DPOS) 방식 등 대안이 나오고 있지만, 블록체인의 합의 알고리즘이 앞으로 어떻게 되어야 할지에 대한 근본적 합의는 아직 이루어지지 않았다.

3.3 자금조달방식

현재 대부분의 블록체인 프로젝트들은 ICO(Initial Coin Offering)을 통해서 초기 자금을 조달하고 있으며, 암호화폐공개(ICO)의 적법성에 대한 논쟁이 뜨겁다. 한국은 2017년 9월 '금융위원회'가 암호화폐 시장의 과열을 막고 우후죽순으로 ICO가 추진되는 것을 막기 위하여 모든 형태의 ICO를 금지한다고 밝혔다. 그러나 블록체인 관련 단체와 전문가는 블록체인의 조속한 확산을 위해서는 ICO가 법적으로 허용되어야 한다고 주장한다. 실제로 일부 기업은 ICO가 합법화 된 스위스나 싱가포르 등의 해외에서 법인이나 재단을 만들어서 우회적으로 ICO를 추진하는 상황이다[20].

리플의 CEO인 갈링하우스(Brad Garlinghouse)와 같이 ICO 합법화에 반대하는 사람들은 "대부분의 ICO가 뚜렷한 목적 없이 그저 블록체인이 모든 해답을 줄 것이라는 기대감에서 이뤄지기 때문에 실패할 수 밖에 없다"고 지적했다[21]. 실제로 암호화폐 전문매체 '비트코인닷컴(Bitcoin.com)'의 보도에 따르면, 2017년에 진행된 ICO 가운데 418개가 이미 실패한 것으로 판명되었고 113개의 ICO는 실패가능성이 상당히 높은 것(failures-in-the making)으로 나타났는데, 이는 2017년의 전체 902개 ICO의 59%에 해당하는 수치이다[22].

ICO 합법화에 찬성하는 사람들은 무조건적인 ICO 금지가 4차 산업혁명시대에 역행하는 규정이며, 투자자 보호를 전제로 한 ICO 허용을 통해서 '한국형 ICO 가이드라인'을 속히 만들어야 한다고 주장한다. '한국금융ICT융합학회' 오정근 회장은 "100개~200개의 한국 블록체인 기업이 해외에서 ICO를 통해서 모은 자금이 최소 1조원으로 추정되며, 이 자금이 인건비와 법인세를 해외 현지에 지불하고 나면 실질적으로 한국에 들어오게 되는 자금은 현저히 적다"며 심각한 국부유출의 위험성을 경고했으며, "ICO 금지 때문에 ICO 관련 법률·회계 자문, 컨설팅 등 관련 서비스업의 발전이 저해되며, 이는 11만개의 신규 일자리 창출 기회를 놓치는 것"이라고 밝혔다[23].

ICO에 대한 법률적 규제와 관련하여 현재 한국에서는 무조건적 금지와 무조건적 허용이 아닌, '규제 샌드박스' 또는 '특구 지정'이 절충적 대안으로 제시되고 있다. '규제 샌드박스' 방안은 한국의 ICO도 우선 '자본시장법'을 개정한 '규제 샌드박스' 안에서 실험한 뒤에 결과가 좋으면 허용하자는 방안이며, '특구지정' 방안은 원희룡 제주지사 등이 중심으로 주장하는 대안으로 특정 도시나 지역을 지정하여 블록체인과 암호화폐 ICO의 허브도시로 만들자는 제안이다.

4. 결론

2008년 비트코인의 탄생으로부터 시작된 블록체인 태동기에서, 비트코인은 기존의 금융기관을 매개로한 중앙 집중식 금융거래에 수반되는 거래의 복잡성, 해킹의 가능성, 높은 수수료 등의 문제들을 극복하고 분산화된 네트워크 사용자간의 직접적인 P2P방식을 통하여 거래의 효율성, 신속성, 보안성을 실현할 수 있는 기술적 특징을 가지고 있는 것으로 평가되었다. 그러나 비트코인은 발행량 제한으로 인한 유동성 부족 문제, 블록크기 제한에 따른 처리속도의 지연, 과다한 에너지 소비, 사용자 비친화적인 특성 등의 이유로 전자화폐 결제 이외의 다른 분야에 적용하기는 힘들었다.

이러한 비트코인의 한계점은 2013년 '탈중앙화된 블록체인 플랫폼'을 표방한 이더리움의 개발로 보완이 된다. 따라서 이더리움의 개발을 블록체인 확장기로 볼 수 있다. 이더리움은 블록체인에 기반 해서 작동하는 소프트웨어인 디앱(DApp)의 개발과 소프트웨어 코드를 통한 자동화된 스마트 계약의 실행이 가능하다는 것이 확인되었다. 그러나 이더리움은 2016년 DAO 해킹사건에서 드러난 내부 갈등의 해결과정에서 나타난 거버넌스 문제, 스마트 계약의 비가역성 문제, 수수료 기반 처리 시스템이 가진 문제 등이 향후 해결해야 할 과제로 나타났다.

2017년부터 시작된 확산기에는 비트코인과 이더리움 이외에도 리플, 비트코인 캐쉬, 이오스, 스텔라, 라이트 코인과 같은 다양한 종류의 알트코인이 주목을 끌었다. 알트코인은 비트코인과 이더리움이 가지고 있던 한계들을 뛰어 넘어 블록체인 기술이 여러 산업영역에서 적용될 수 있는 가능성을 보여주고 있으며, 이와 더불어 블록체인을 둘러싼 논쟁도 현재 진행형이다. 대표적 쟁점으로는 암호화폐와 블록체인과의 관계, 블록체인 알고리즘의 결정 문제, ICO의 법적 허용 여부와 관련한 쟁점들이 있다.

2008년 세상에 비트코인이 처음 모습을 드러냈을 때 "비트코인은 악마와도 같다"며 비판했던 노벨 경제학상 수상자 Paul Krugman는 10년이 지난 2018년 8월 블록체인 관련 콘퍼런스에서 "금은 죽었다. 비트코인은 금보다 유용성이 크고, 앞으로 가치 있는 것이 될 가능성이 크다"며 기존의 태도를 바꿔서 전 세계에 놀라움을 안겼다[24]. 이는 지난 10년 동안에 블록체인 기술이 얼마나 많이 변화해 왔는지를 상징적으로 보여주는 사례이다.

블록체인 기술과 암호화폐에 대한 각 시기별 특징과 문제점을 살펴본 본 연구는 블록체인 기술의 역사적 발전과정과 블록체인과 관련한 현 단계에서의 쟁점들을 이해하는 것을 도와서 향후 블록체인 연구를 위한 기초자료를 제공할 수 있을 것으로 기대한다.

References

[1] http://it.chosun.com/site/data/html_dir/2018/01/22/2018012285005.html, Retrieved: Feb 25 (2019)

[2] http://www.edaily.co.kr/news/read?newsId=01361206619076408&mediaCodeNo=257, Retrieved: Feb 25 (2019)

[3] http://www.edaily.co.kr/news/read?newsId=01512086619146600&mediaCodeNo=257&OutLnkChk=Y, Retrieved: Feb 25 (2019)

[4] J. H, Jin, G. J, Koo, The Direction for the Application of Blockchain Technology in the Health and Welfare Sector, health and welfare forum, (2018), Vol.258, pp.96-106.

[5] J. Y, Lee, Technology Trends and Implications of Block Chain, Science and Technology Policy, (2017), Vol.34.

[6] http://techm.kr/bbs/board.php?bo_table=article&wr_id=4732, Retrieved: Feb 25 (2019)

[7] www.bitcoin.org, Retrieved: Feb 25 (2019)

[8] Yoshiharu Akahane, Manabu Ikei, Block Chain Structure and Theory, wikibook, (2017)

[9] http://magazine.hankyung.com/business/apps/news?nkey=2018082101186000351&mode=sub_view, Retrieved: Feb 25 (2019)

[10] BPtechtrade, Block Chain Changes Industry Map, (2017)

[11] Y. I, Choi, Encryption-enclosure revolution, Etherium blockchain. Durimedia, (2018)

[12] D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, (2016)

[13] https://blog.ethereum.org, Retrieved: Feb 25 (2019)

[14] M. J. Casey, P. Vigna, The Truth Machine, HarperCoiins, (2018)

[15] Yukio Noguchi, Bitcoin and the Future of Blockchain, (2017)

[16] http://www.investchosun.com/2018/09/21/3230432, Retrieved: Feb 25 (2019)

[17] J. Y. Kim, Invest in the blockchain in the era of the Fourth Industrial Revolution , MateBooks, (2018)

[18] Nakajima Masahi, After Bitcoin: The Next Leader in Virtual Currency and Blockchain, khbp (2017)

[19] Y, S, Lee, The reason why encryption is an important platform technology. In-depth Diagnosis: Evolution of Block Chain, Tech M, (2018), Vol.59.

[20] J. G. Kang, How do we do blockchain enactment encryption?, Tech M, (2018), Vol.60.

[21] https://news.joins.com/article/22442733, Retrieved: Feb 25 (2019)

[22] https://news.bitcoin.com/46-last-years-icos-failed-already/, Retrieved: Feb 25 (2019)

[23] https://decenter.sedaily.com/NewsView/1S3JT4HJTN, Retrieved: Feb 25 (2019)

[24] https://news.joins.com/article/23011997, Retrieved: Feb 25 (2019)