일반연구논문

블록체인 비교연구: 비트코인·네임코인·메디블록■

김지연*

■ 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2016S1A5A2A03927422).

* 고려대학교 과학기술학연구소 연구교수 전자우편: spring900@gmail.com, redgrass@korea.ac.kr

2008년 등장한 비트코인(Bitcoin)은 중앙의 신뢰기관 없이 직접 거래가 가능한 전자 화폐 시스템이다. 당시 비트코인은 단지 개념상의 화폐에 불과했지만, 이제는 현실 화폐만큼의 지위를 누리게 되었다. 비트코인의 대중화 덕분에 블록체인 기술은 대중적 관심의 대상이 되었다. 블록체인 기술은 화폐 기능만이 아니라, 다양한 영역으로 확장해가고 있다. 블록체인의 가능성은 구성 중이다. 이 논문에서는 블록체인 응용 중에서 비트코인, 네임코인(Namecoin), 메디블록(MediBloc) 사례를 비교함으로써 블록체인의 기술적 성격과 사회적 상호 구성의 경과를 살펴보고자 한다. 2013년 등장한 네임코인은 현행의 중앙집중적 인터넷 도메인 네임 시스템(DNS)을 대체할 목적으로 설계되었다. 도메인 네임 관리 방식에 대해서는 오래전부터 논쟁이 있었지만 이미 수립된 체제를 대체하는 일은 쉽지 않다. 한편 메디블록은 의료데이터의 분산적 관리를 제안하고 있다. 메디블록은 의료데이터의 핵심 생산자는 환자이므로 데이터의 관리도 환자에게 권한을 줘야 한다고 주장한다. 블록체인 기술은 현행의 관리 권한을 분산함으로써 더 민주적인 의사결정 형성을 도울 것인가? 아니면 단지 더 자동화된 기술적 해법에 그칠 것인가? 시민으로서 우리는 블록체인을 의제화함으로써 이 기술의 현실적 구현 과정에 개입할 수 있다. 그것이야말로 기술의 사회적 구성이 될 것이다.

주제어 | **블록체인, 타임스탬프, 거버넌스, 자동화, 시민과학**

1. 서론

정부기관과 같이 현대의 시스템들은 거의 대부분 중앙에 관리권한을 집중하고 있다. 단일한 중앙기관 관리 방식은 나름의 효율성과 안전성을 보증했고 분쟁 발생 시 중재 역할도 해왔다. 그런데 이런 관리 방식이 막대한 비용을 발생시키기 시작했다. 특히 악의적 의도를 가진 공격자들에게 취약했기 때문에 이를 방어하는데 많은 비용이 필요해졌다. 그래서 중앙의 단독관리보다는 여러 사회집단이 참여하는 거버넌스 방식이 주목받고 있다. 사회적 차원에서만이 아니라 기술적 차원의 해법도 등장하고 있다. 블록체인 기술은 중앙의 단독 관리로 인해 발생하는 문제에 대한 기술적 차원의 대안이라고 할 수 있다.

블록체인 기술은 비트코인 열풍과 함께 대중적인 관심사로 부상했다. 블록체인은 이제 기술 분야만이 아니라 경제, 사회 등 다양한 학문 분야의 관심사가 되었다. 한편에서는 "블록체인 특성은 온라인 거래에 있어 완전한 투명성을 제공한다(김의석, 2018)" 또는 "블록체인을 사용하면 더 이상 어떤 기록이 진실이라는 것을 증명해 줄 공인된 기관이 필요하지 않다(마이클 외, 2018)" 등 긍정적 평가를 받는다. 다른 한편으로는 "비트코인은 결코 화폐가 아니다....(비트코인의 의도는) 엉뚱하고, 맹랑하며, 교활하다. 그리고 무서운 교활함과 속임수가, 간계·흉계가 숨어 있다(채만수, 2018)"는 공격적 주장도 있다. 또는 "(비트코인은) 급진적으로 사회를 전환하

려고 시도하며 블록체인 프로젝트들은 유토피아를 꿈꾸고 있다(Swartz, 2018)"는 접근도 있다. 웹툰 만화가 윤태호는 시민과학 프로젝트 세티(SETI)에 블록체인을 적용하면 더 효과적이고 의미있는 프로젝트가 될 것 같다는 감상을 전했다[1]. 한 방송국의 블록체인 토론회에서 찬반 논쟁은 많은 화제를 낳았다[2]. 이런 극명히 엇갈리는 다양한 평가가 동시에 존재한다는 것은 블록체인 기술이 여전히 변화 중이며 그 정체성이 완성되지 않았다는 것을 의미한다.

블록체인은 기본적으로 '공유 장부(shared ledger)' 기술이다. 이 장부는 종이 위에 쓰여지는 것이 아니라 암호화된 단위, 블록(block)의 형태로 공유되며 여러 컴퓨터(노드)에 동시에 저장된다. 모든 참가자들은 블록을 추가할 자격이 있고 블록이 추가되는 것을 관찰할 수 있다. 그래서 블록체인은 블록들의 체인이다(Swartz, 2017). 이 장부는 기본적으로 "쓰기만-가능한 장부(write-only ledger)"로서 그 목록을 삭제하거나 변경할 수 없다.

과학기술학(STS, Science and Technology Studies)은 기술과 사회의 상호구성에 대한 많은 분석 사례가 있다. 그런데 주로 이미 종결된 기술들을 다루어 왔고 반면에 진행 중인 기술 논쟁에 대해서는 덜 적극적이다. 과학기술학은 '종결된 기술'만이 아니라 지금 논쟁 중이고 구성 중인 기술을 분석하는데도 좀 더 적극적일 필요가 있다. 우리 사회는 지금 4차산업혁명이라는 언명 앞에서 어떤 태도를 취해야 할지를 요구받고 있다. 많은 사람이 대중 미디어의 태도에 따라서 때로는 극히 낙관하거나 때로는 극히 두려워하고 있다. 과학기술학 연구자들은 진행 중인 기술에 대한 적극적

1) '미생' 윤태호 "블록체인 공부 전엔 유시민이 옳다 생각"(한겨레, 2018. 5. 15일자)

2) JTBC 뉴스룸은 2018년 1월 18일 긴급토론회 "가상통화, 신세계인가 신기루인가"를 방영했다.

인 해석을 제시함으로써 사회적 의사결정 과정에 기여할 수 있다.

이 논문에서는 블록체인의 응용 형태 중에서 비트코인, 네임코인, 메디블록을 선택하여 비교하며, 상호보충하는 방식으로 블록체인의 기술적 구조와 사회적 양상을 살펴보고자 한다. 우선 해당 모델 개발자들이 제시한 설계도를 따라가 볼 것이다. 비트코인은 직접 거래를 가능하게 함으로써 중앙기관의 필요를 '제거'했다. 이를 위해 타임-스탬프(time-stamp)와 작업증명(proof-of-work)과 같은 기술적 과정을 설계했다. 네임코인은 현행 DNS(Domain Name System) 기술권력을 대체하기 위해서 개발된 블록체인 기반의 DNS 시스템이다. 현행의 기술시스템과 대안의 기술시스템 사이의 경합이 이제 막 시작되었다. 한편 메디블록은 의료 데이터 관리 권한을 재분배하고자 한다. 메디블록의 성공 여부는 블록체인 기술이 그렇듯이, 관련 사회집단(이해당사자)이 새로운 관리 방식을 수용할 것인지에 달려있다.

마지막으로 이 논문은 블록체인 기술이 선언한 바대로 중앙기관 관리 방식을 제거하여 참여자들에게 더 많은 자유와 권한을 부여할 지에 대해 살펴본다. 본래 그런 일은 주로 사회 시스템에게 기대했던 것이었다. 기존의 사회 시스템이 해왔던 역할을 블록체인이 수행할 수 있을지를 관찰할 필요가 있다. 블록체인 기술의 변화가 여전히 진행 중이기 때문에 이 관찰은 쉽지 않지만, 그 과정의 한 단면을 목격하고자 한다. 블록체인 시스템은 기존 체제의 권한을 분산함으로써 더 민주적인 의사결정 체제 형성을 도울 것인가? 아니면 인간사회의 신뢰를 자동화하는 기술적 해법에 불과한가? 블록체인 기술에 의한 사회관리의 자동화는 정당화될 것인가? 우리는 블록체인에 대한 사회적 의제화를 통해서 이 기술의

구현 과정에 개입할 수 있다. 그것이야말로 기술의 사회적 구성의 한 방법이라고 할 수 있다.

2. 비트코인

사토시 나카모토(Satoshi Nakamoto)는 비트코인 백서(Bitcoin: A peer-to-peer electronic cash system, 2008)를 발표함으로써 '단지 개념에 불과했던' 블록체인 기술을 실체적인 것으로 밀어올렸다. 사실상 블록체인은 비트코인에 의해서 세상에 알려졌다. 그래서 비트코인이라는 고유명칭이 블록체인과 동의어처럼 사용되곤 한다. 2009년 1월 나카모토에 의해 최초로 비트코인이 채굴된 이후 비트코인 가격은 지속적으로 증가했다. 2010년 비트코인 1개의 가치는 0.003달러였는데, 현재는 약 6,500달러에 거래되고 있다.

이후 다수의 암호화폐가 등장했지만, 비트코인은 여전히 '가장 지배적인 암호화폐' 네트워크를 가지고 있다. 초기 블록체인 열광자들이 유일하게 선택할 수 있는 것이 비트코인이었기 때문이다. 다수의 참여자가 유입되면서 비트코인 네트워크는 작은 세계를 조직했다. 그 참여자 대부분은 단지 작은 양의 컴퓨터 자원만을 가진 자들이었다(Liang, et al., 2018).

1) 직접 거래 전자 화폐 시스템

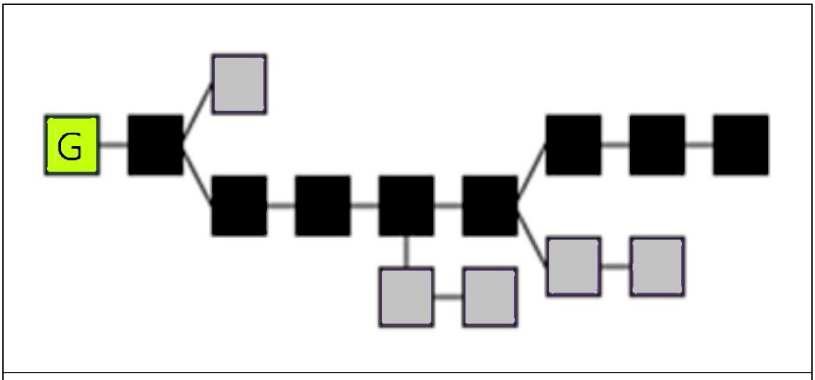
비트코인은 화폐 발행과 거래 내역(장부)을 다수 컴퓨터(참가자)가

동시에 관리하는 방법이다. 네트워크상에서 공동으로 장부를 관리하기 때문에 은행과 같은 중앙기관의 매개 없이 거래 당사자들이 직접 화폐를 교환한다.

> "인터넷 기반 상거래는 신뢰할 수 있는 제3자 역할을 금융기관에 의존해 왔다. 이 시스템은 대다수 거래에서는 잘 동작하지만, 여전히 신뢰 기반 모델의 태생적 약점을 가지고 있다. 금융기관은 분쟁 중재를 피할 수 없고, 완전히 비가역 거래가 실제로 가능하지 않다.....(생략).....우리에게 필요한 것은 신뢰 대신 암호학적 증명에 기반을 두고, 제3자 없이 거래의 두 당사자가 서로 직접 거래하게 해주는 전자 화폐 시스템이다(Nakamoto, 2008)."

실물 화폐 거래는 기본적으로 실제 화폐를 주고받음으로써 거래가 이루어지는데 비해서, 비트코인 거래는 거래내역을 장부에 기록함으로써 거래가 완료된다. 그래서 장부는 전통적 화폐 거래 시스템에서도 중요했지만, 비트코인 시스템에서는 더욱 중요하다. 실물 화폐는 장부와 화폐가 별도의 물리적 존재라면 비트코인에서는 장부와 화폐가 통합되어 있다.

블록체인의 일반적 개념과 마찬가지로 비트코인의 핵심은 분산과 공개다. 모든 거래는 하나의 공개 장부에 기록되고 사용자 모두에게 분산되어 저장된다. 이러한 공개장부의 단위가 '블록(block)'이다. 현재 비트코인 평균 블록 크기는 0.81 Mb다. 새로운 거래가 일어나면 새로운 블록이 생성되고, 그 블록은 전체 네트워크에 흩어져 있는 참가자(또는 채굴자)들에게 공개되어 검증이 이루어진다.



〈그림 1〉 최초 블록(G), 승인된 블록(검은색), 미승인된 블록(회색)

비트코인 거래 과정을 순서대로 살펴보면 다음과 같다. (1) 지갑 프로그램 설치와 주소 생성: 프로그램 또는 웹서비스 방식의 지갑 프로그램을 설치한다. 이 프로그램은 비트코인 거래를 위한 계정(개인키)과 수신자의 주소(공개키)를 생성한다[3]. (2) 송금지시: 송금 거래내역을 작성하고 개인키를 이용해서 거래내역에 서명한다. 거래내역에는 해시값, 비트코인 금액, 수신자의 주소가 포함된다. (3) 송금지시 발송: 거래내역과 서명값을 인접 노드에 전파하는데, 최종적으로 전체 네트워크에 전파된다. (4) 송금지시 검증: 네트워크에 전파된 거래내역을 다수의 채굴자들이 검증하기 시작한다. (5) 블록생성과 배포: 검증을 마친 채굴자는 검증한 거래내역을 포함하는 블록을 생성한다. (6) 블록체인 생성과 공유: 채굴자는 새로운 블록이 포함되어 길이가 1만큼 늘어난 블록체인을 주변 노드에 알린다. 그러면 이전의 짧은 블록체인을 가지고 있던 주변 참여자(노드)들은 새로운 블록을 전달받아 갱신한다(이혁준 · 이수미, 2016).

3) 비트코인 지갑 프로그램은 의사 난수 발생기(pseudorandom generator)를 사용해서 256비트의 개인키와 타원곡선암호 방식을 사용하여 512비트의 공개키를 생성한다(김원, 2018).

<그림 1>과 같이 블록체인은 최초의 블록(genesis block)과 승인된 블록, 그리고 미승인된 블록들로 이루어진다. 블록의 분기는 두 가지 경우에 발생한다. 하나는 해당 공동체 내 견해가 달라서 한 집단이 합의 프로토콜을 변경하는 경우에 일어난다. 다른 하나는 공격자들이 블록을 공격하기 위해서 위조 블록을 끼워 넣을 때 발생한다. 이렇게 블록체인의 가지가 생기면, 때로는 즉각적으로 포기되거나, 때로는 지지자들에 의해서 새로운 블록체인이 된다. 전자의 경우처럼 포기된 블록을 '고아 블록(orphan block)'이라고 한다. 후자의 대표적인 예시로는 비트코인에서 분기된 "비트코인 캐시"가 있다(Wander, 2011; Kamel Boulos, et al, 2018).

2) 타임-스탬프와 작업증명

비트코인 백서는 전자화폐를 전자서명의 연장이라고 정의한다. 거래를 하고자 하는 사람(송신자)은 이전 거래내역에 수신자의 공개키를 포함한 뒤 자신의 비밀키로 암호화(전자서명)함으로써 거래를 완료하기 때문이다. 그리고 정당한 거래로 승인되기 위해서는 타임-스탬프(time stamp)와 작업증명(Proof of work) 과정이 필요하다.

전자화폐 시스템에서 난점은 이중거래 문제(double-spending problem)[4]다. 나카모토는 이 문제를 타임-스탬프 기법으로 해결했다. 타임-스탬프는 시간 순서에 따라 참여자들이 거래내역을 수용하는 방법이다. 원래 백서에서는 타임-스탬프 서버 개념이 제안되었지만 실제 비트코인에서는 서버없이, 기능의 형태로만 구현되었다.

4) 이중거래 문제란, 코인 사용자가 자신의 코인을 지불한 후에도 해당 코인이 여전히 사용자의 것으로 남아 있어서 그 코인을 다시 사용할 가능성에 관한 문제다.

"우리가 제안한 해법은 타임스탬프 서버로 시작한다. 타임스탬프 서버는 아이템 블록의 해시에 타임스탬프를 찍고 신문이나 유즈넷 같이 해시를 널리 공표한다. 타임스탬프는 바로 그 시간에 바로 그 데이터가 해시 속에 부여된 순서로 존재한다는 것을 증명한다. 체인이 형성되면서 추가되는 개별 타임스탬프는 그 해시 안에 이전 타임스탬프를 포함하고 그 결과 이전에 생성된 코인을 강화한다(Nakamoto, 2008)."

타임-스탬프 개념은 비트코인의 거버넌스적 성격을 보여준다. 일반적으로 거버넌스에서는 인과성 추적이 필수적이다. 인과성이란 사건을 시간순으로 배열한 결과이다. 하나의 사건은 이전 사건의 결과로 기록되고 다시 이 사건은 후속 사건을 결정한다. 그래서 정부 문서들은 엄격하게 날짜를 기록하고 논란이 되는 경우 사후 조작 흔적이 있는지를 검증해야 하는 법적 성격을 가진다. 이러한 인과성 개념을 디지털 문서에 적용하는 해법이 타임-스탬프 개념이다.

이 개념은 이미 1990년대 등장했었다[5]. 하버와 스토네타(Haber & Stornetta, 1991)는 타임-스탬프를 수립하는 두 가지 접근법을 제안했다. (1) 연결 해법(linking solution); 문서의 해시값이 타임-스탬프 서비스에 등록되어 있고 이 값들을 순차적인 목록으로 연결하는 것이다. 그 결과 이 값들은 삽입되거나 대체될 수 없고 삭제될 수도 없다[6]. (2) 무작위-증인 해법(random-witness solution); 참가

5) 타임-스탬프는 시간 내역이 기록된 항목들의 블록해시를 종합하는 기능을 수행한다. 각 타임스탬프 내역은 이전 타임-스탬프로부터 건네받은 해시 내역을 포함시킴으로써 처리 흐름에 따른 순차성을 가질 수 있다. 그 결과에 의존하여 특정 시간에 그 데이터가 명백히 존재했다는 것을 입증한다.

6) 이후 새로운 필요들이 등장하면서, 삭제불가능성 부분은 다소 수정되어서 추가 서명 인증

자 중 일부가 해시값에 날짜를 기록하고 서명하도록 한다. 그 서명은 타임-스탬프가 포함된 인증으로서 모두에게 공개된다. 그 일을 수행하는 증인들은 유사무작위 생성기(pseudorandom generator)로 선정된다. 이 생성기는 최초에는 문서 자체의 해시값을 사용하여 난수를 생성한다. 이 방식은 증인을 선정하는 단계에서 의도가 개입되지 못하게 만들어 준다.

곧이어 바이어와 하버(Bayer & Haber, 1992)는 타임-스탬프의 연결 방식을 개선하여 해시 트리(hash trees) 개념을 제안했다. 상대방을 확인할 수 있는 토너먼트 경기 대전표처럼, 해시 트리는 승인된 사건은 물론이고 승인되지 못한 모든 사건도 기록으로 남긴다. 이로서 모든 사건 참여자들이 서로를 확인할 수 있게 된다. 무작위-증인 해법에서 최소한의 증인의 수가 얼마가 되어야 하는지 확정하기 어려웠는데, 가장 확실한 증인의 수는 전체 참가자가 증인이 되는 것이다. 해시 트리는 사실상 필요한 증인의 수를 전체 참가자로 확장했다. 그래서 참가자의 수가 빠르게 증가하더라도 타임-스탬프를 안정적으로 확인할 수 있다.

타임-스탬프를 포함하여 하나의 거래가 종료되면 그 거래를 블록에 저장하는 검증 절차를 거쳐야 한다. 이를 작업증명(proof-of-work)이라고 한다. 해시함수에 이전 거래 해시값과 임의의 값(nonce)을 계산하여 미리 정해진 값을 얻는 것이다. 이 과정은 매번 새롭게 제출되는 매우 어려운 수학문제와 같은데, 일방향성을 가지고 있어서 답을 안다면 그 답이 맞는지를 검증하는 것은 쉽지만 그 답을 찾는 것은 어렵다. 그 임의의 값을 찾을 때까지 일일이 값을 대입하면서 찾는데, 답을 찾을 때까지 이 과정을 계

과 같은 필요에 따라서 타임-스탬프를 갱신하는 것이 가능해졌다.

속해서 되풀이하기 때문에 엄청난 양의 반복계산을 해야 한다(Loible, 2014; 김의석, 2018).

이렇게 작업증명으로 검증된 블록만이 승인된 블록이 된다. 이를 흔히 채굴(mining)이라고 한다. 이 과정은 비트코인 네트워크 참가자들의 과반수 합의에 의해서 최종적으로 완료된다. 승인된 블록을 생성한 최초의 채굴자에게 새로운 코인을 보상으로 부여하는데 그것이 화폐로서 비트코인이다. 이런 보상 메커니즘 덕분에 특별히 조직화되지 않더라도 다수의 참여와 협력이 가능하다. 비트코인은 이 네트워크의 질서에 따라 작업을 수행하는 '선의의 채굴자'들이 전체 네트워크의 과반수를 점유하는 한 '지속가능'하다.

공격자가 의도적으로 위조 블록을 끼워 넣더라도 채굴자들의 작업증명에 의해 걸러질 수 있다. 승인되지 못한 블록은 즉시 '고아 블록'으로 남게 되고 그 블록 이후로는 체인이 형성되지 못한다. 그런데 만약 공격자들이 네트워크의 과반수 이상을 점유한다면 위조 블록이 정당한 블록으로 승인되어 체인을 형성하는 것이 가능해진다. 그래서 블록체인에서 참가자 네트워크의 규모는 매우 중요하다. 비트코인 네트워크의 규모가 클수록 공격자들이 과반수를 점유하기 어려워질 것이기 때문이다.

3. 네임코인

네임코인(Namecoin)은 최초로 도메인 네임 서비스와 블록체인을 결합한 암호화폐다(Karame & Androulaki, 2016). 이후 네임코인 외에도

이더리움 네임(Ethereum Name), 블록스택(Blockstack)과 같은 블록체인 기반 도메인 네임 시스템이 등장했다. 비트코인은 커다란 대중적 관심을 받고 있고 논문과 저술도 대량 발행되는데 비해서, 네임코인은 아직 사회적 관심을 받지 못하고 있고 관련 저술도 거의 없다.

1) 대안적 도메인네임시스템

"도메인 네임 시스템(Domain Name System: DNS)"은 인터넷 거버넌스의 대표적 영역이다. 그런 점에서 네임코인은 인터넷 거버넌스에 관한 기술이다. DNS는 일종의 '전화번호부' 같은 것으로서, 인터넷상에서 사용자가 특정 정보를 찾아갈 수 있도록 해주는 식별체계이다. 1988년 인터넷 개척자 공동체에서 출발한 IANA(Internet Assigned Numbers Authority)가 인터넷상에서 사용되는 IP주소, 도메인 네임, 관련 파라미터에 대한 전반적인 권위를 보유하고 있다. 1998년 IANA의 정책을 집행하는 별도의 기구, ICANN(Internet Corporation for Assigned Names and Numbers)이 만들어졌다. ICANN은 미국 상무부의 승인에 따라 탄생한 비영리 법인조직이다. 인터넷 도메인이 국제적 규모에서 사용되는데 그 집행주체가 미국 정부의 관할권 내에 있다는 점에서 공정성 문제가 계속 제기되어왔다(김지연, 2013).

가장 극적인 사건은 2010년에 일어났다. 미국정부 문서를 대량으로 폭로하여 유명해진 위키리크스 사이트가 며칠 간 다운되었는데 사람들은 단순한 오류가 아니라 의도적인 사건이라고 여겼다. 이 사건은 DNS 단독 관리의 위험을 널리 알렸는데, 그런 일은 단지 미국에서만 일어나는 것이 아니었다(Musiani, 2013). 국제

적으로 정부 저항적이거나 비법적 활동을 하는 웹사이트에 대한 DNS 호스팅 중단은 빈번하게 일어나고 있다. 터키 정부는 선거 전에 자국의 DNS 서버에서 트위터나 유투브를 차단했던 적이 있고, 중국 정부는 자국민의 도메인을 감지하는 DNS 캐시 공격(DNS cache poisning)을 한 적이 있다[7]. 현행 DNS 구조는 서버 운영자가 도메인 네임에 대한 거의 모든 권한을 가지고 있어서 정부의 검열과 개입 압력을 받기 쉽다.

표현의 자유가 통제될 수 있다는 우려가 계속 커지면서, ICANN의 단독 관리와 경합할 수 있는 "새로운 경쟁적 루트-서버(new competing root-server)"에 대한 논의들이 등장했다. 2001년 주코 윌콕스-오헨(Zooko Wilcox-O'Hearn)은 대안적 도메인 네임 시스템이 되기 위해서는 다음 3가지 특성 중 적어도 2가지를 만족해야 한다고 주장했다: (1) 국제적으로 고유할 것: 해당 네임 맵(name maps) 상에 하나만 존재하는 이름을 부여해야 한다. 그리고 누구도 다른 사람이 도메인 네임을 소유하는 것을 막을 수 없다. (2) 분산적일 것: 도메인 네임의 의미를 결정하는 중앙 기구가 없다. (3) 인간이-이해할 수 있는 의미를 가질 것: 도메인 네임은 인간이 기억하기에 충분이 짧은 임의의 문자열이어야 한다(Loible, 2014). 이를 주코의 이론(Zooko's theory)이라고 부른다.

그런 대안적 도메인 네임 등록 방식 중 하나는 사용자들이 직접 자신의 컴퓨터를 DNS 호스트로 만드는 방법이 있다. 일종의 분산적 P2P 시스템 방식이다[8]. 2010년 9월, 비트코인 포럼에서

7) DNS 캐시 공격이란, DNS 중앙 서버를 공격하는 것이 아니라 DNS를 임시로 저장하는 캐시 서버의 쿼리 정보를 위/변조하는 방법이다.

8) 인터넷 아키텍처 이사회(The Internet Architecture Board, IAB)는 기술문서 RFC 2826(2000. 5)

BitDNS에 관해서 토론을 시작했다. 그 해 12월 BitDNS 구현에 대한 보상이 공시되자 개발자들은 보상을 받기 위해서 더 적극적으로 움직이기 시작했다. 2011년 1월, 아론 스워츠(Aaron Swartz)는 주코의 이론을 비트코인 시스템에서 구현한 도메인 네임 시스템을 제안했고, 같은 해 4월, 빈센트 듀햄(Vincent Durham)이 네임코인(Namecoin)을 구축했다.

중앙기관이 루트 서버를 관리하는 현행 DNS와 달리, 네임코인은 P2P 네트워크에서 DNS 조회표를 공유한다. 네트워크에서 네임코인 소프트웨어를 운영하는 노드들이 있는 한, 그 노드들을 통하여 도메인 네임에 접속할 수 있다. 네임코인 초기 채굴자들은 블록 하나를 생성할 때마다 50 네임코인(NMC)을 보상받았다. 210,000개의 블록이 추가 생성될 때(약 4년 주기) 마다 보상금액은 절반으로 하향 조정된다. 코인 발행량은 21,000만 NMC(Namecoin Currency)로 한정되어 있다.

2013년 6월, 네임아이디(NameID) 서비스와 무료 소프트웨어가 제공되었다. 2014년 2월 FreeSpeechMe가 출시되어 윈도우즈, 리눅스 상에서 네임코인 주소를 자동으로 전환해주었다. 네임코인 도메인주소의 사용은 미미하다. 2015년 120,000개의 네임코인 도메인 네임이 등록되었는데 그중 단 28개만이 사용 중인 것으로 보고되었다(Karame & Androulaki, 2016). 네임코인 웹사이트에 따르면 2018년 10월 4일 현재, 채굴된 네임코인 블록은 420,000개에 불과하다[9].

를 통해서 DNS 루트의 고유성을 강조하며 대안적 루트 개발에 강력히 반대했다(Kalodner, et al. 2015). 그럼에도 불구하고 대안적 DNS 방법에 대한 시도는 계속되었다.

9) 구체적인 정보는 다음 링크에서 볼 수 있다. https://namecoin.cyphrs.com/block/420000

네임코인의 최상위 도메인 네임은 ".bit" 이고, 이 도메인 네임은 ICANN과 같은 중앙기관에 의한 개입 없이 해당 도메인 네임 소유자에게 완벽한 권리가 있다. 예를 들어 ICANN은 극단적 조건이라면 "google.com"을 차단할 수 있지만, 네임코인에서는 시스템 전체를 파괴하지 않고서는 "google.bit"를 차단할 수 없다.

2) 비트코인 기반 도메인 네임

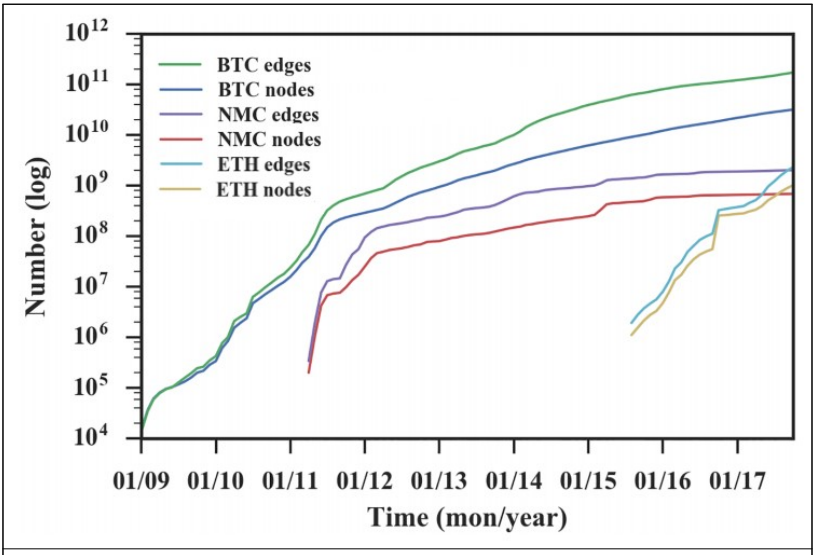
네임코인은 비트코인 코드에 기반을 두는데, 비트코인은 그 자체로 이미 주소기반 거래 메커니즘이다. 각 블록 내 공개키는 수신자의 주소가 되고 개인키는 발신자의 주소가 된다. 블록체인 네트워크의 모든 참가자는 거래 장부 전체 복사본을 공유하고 관리하는데 이것은 모든 노드가 그 주소를 보관하고 있다는 것을 의미한다. 이로써 비트코인은 이미 네임코인의 원형적 토대를 충분히 구현하고 있는 셈이다. 사용자들은 비트코인에서처럼 임의의 이름(키)과 추가된 데이터(값)를 기록하고 전송한다. 이들 키값은 네임코인 프로세스에 의해서 인간이 이해할 수 있는 이름(human-readable name) 형태로 번역된다. 따라서 네임코인 주코의 이론을 모두 충족한다(Loibl, 2014; Kalodner, et al. 2015).

네임코인 네트워크에 참여자들은 네임코인 클라이언트 프로그램을 내려받아서 기본 설정을 해야 한다. 이후 네임코인 네트워크에 연결되고 갱신된 블록체인을 내려받는 일은 자동으로 수행된다. 참여자들은 네임코인 블록체인의 완전한 복사본을 소유하며 P2P 네트워크에 연결된 동료 참여자들로부터 전해 받은 새로운 블록을 가져와서 검증하면서 동기화하는 일을 한다.

네임코인 도메인 네임 사용자들은 전용 프로그램을 설치해야 한다. 현행 DNS 시스템에는 ".bit" 도메인을 사용하지 않기 때문에, 이 주소를 웹브라우저 주소창에 입력하면 "NXDOMAIN"이라는 오류가 표시된다. 네임코인 도메인 조회 클라이언트 소프트웨어들이 몇 가지 있는데, 그 중 NMControl 프로그램이 잘 알려져 있다. 이 프로그램을 설치하면 해당 컴퓨터는 네임코인 네트워크 내에서 블록체인의 완전한 복사본을 동기화함으로써 스스로 지역 DNS 서버 역할을 한다. 네트워크상에 흩어져 있으면서 DNS 서버 역할을 하는 무수히 많은 컴퓨터 덕분에 별도의 중앙기관없이 ".bit" 도메인을 찾아 갈 수 있다[10].

비트코인과 비교하여 네임코인 네트워크는 상대적으로 작고 단순하다. 비트코인은 최초 2년 6개월 동안 10,000배 성장했는데 비해서 네임코인은 첫해 동안만 100배 성장했다. 비트코인 기반 블록체인이었지만 비트코인과 달리 네임코인은 첫해에만 성장했고 그 후 거의 같은 수준을 유지했다(Liang, et al. 2018).

10) 별도의 프로그램 설치 없이 현재 웹사이트 검색과 같은 방법으로 네임코인 주소를 접속할 수도 있다. 현행 DNS 메커니즘을 우회하는 방식이다. 예를 들어서 네임코인 주소 "http://example.bit"을 방문하고 싶다면, 현행 웹브라우저 주소창에 "http://example.bit.namecoinsuffix.dot-bit.org (네임코인 주소 + namecoinsuffix.dot-bit.org)"라고 입력한다. 그러나 이 방법은 안전하지는 않다. 현행 DNS 메커니즘 상에서 네임코인 주소는 찾을 수 없으므로 이 주소가 입력되면 웹브라우저는 오류 쿼리를 생성한다. 인터넷상의 자원자들이 운영하는 게이트웨이 서비스가 이 오류 쿼리를 수집해서 "http://example.bit"로 연결해 주는 것이다. 이렇게 오류 쿼리("NXDOMAIN")를 수집해서 원하는 도메인 주소로 연결해 주는 방식은 인터넷 개발자들에게는 널리 알려진 것인데, 웹브라우저 제작회사의 방침에 따라서 언제든지 방해받을 수 있다.



〈그림 2〉 비트코인(BTC), 네임코인(NMC), 이더리움(ETH) 네트워크 성장 양상(비트코인이 가장 먼저, 이더리움이 가장 나중에 출현했다) (Liang, et al. 2018)

또한, 네트워크 노드의 연결 스타일에서도 차이가 있다. 비트코인 네트워크는 전체 노드의 약 60%가 LLC(Largest Connected Component)와 연결되었다. 네임코인은 전체 노드의 5% 미만만이 LLC와 연결되어 있다. 비트코인 LLC는 상대적으로 크고, 낮은 연결 차수를 가진 새로운 노드들이 높은 연결 차수를 가진 노들들과 연결되는 역동적 경향이 있다. 상대적으로 네임코인 LLC는 규모가 작고 연결된 노드들 사이 다양성도 적다. 네임코인 네트워크의 이런 특징들은 네임코인 사용을 주장하는 열광적인 사용자의 수가 아직 적기 때문이다(Liang, et al., 2018). 네임코인은 비트코인과 달리 도메인 등록이라는 특정 기능을 가지고 있다는 점이 네트워크 형성에 영향을 주는 것으로 보인다.

4. 메디블록

메디블록팀은 2017년 백서를 통해서 또다른 블록체인 기반 암호화폐, 이더리움(Ethereum) 기반의 의료 데이터 관리 플랫폼을 공개했다. 메디블록(MediBloc) 백서는 “의료기관 중심의 관리에서 환자 중심 관리로 전환하여 투명하고 안전한 의료데이터 교환”이라는 목표를 제기했다. 환자가 자신의 의료데이터를 통합하여 관리하고, 연구자와 의료기관 등 다른 이해당사자들(사회집단)과의 관계에서 데이터 교환을 주도할 수 있다고 주장했다. 메디블록은 2018년 12월 정식 출시 예정이다.

1) 의료데이터 권한의 재분배

의료데이터 교환의 필요성은 의료계뿐만 아니라 환자와 여러 전문가에 의해서 꾸준히 제기되어 왔고 다양한 프로젝트도 있었지만, 아직 성공적인 모델은 없다. 현재 미국 정부 주도의 “블루 버튼 커넥터(Blue Button Connector)”, 애플의 모바일 헬스, 삼성전자의 헬스 앱 등이 있다. 의료데이터 서비스는 보안성, 신뢰성, 개방성이 필수적이고 환자, 의료기관 등 상충하는 여러 이해당사자들의 참여가 중요하다.

의료데이터의 파편화는 최선의 진료 수행을 어렵게 하고 반복적인 검사로 환자의 의료비용을 증가시킨다. 이전 병원에서 작성된 데이터가 새로운 병원에 전달되지 않기 때문이다. 의료데이터 공유는 환자 본인이 요청하는 경우로 한정되어 있고 이조차도 절차적으로 상당히 느리게 진행된다. 개별 의료기관 관점에서 의료데이터 공유가 큰 이득이 없기 때문이고, 의료데이터가 법적 규

제 대상이기 때문이다. 의도하지는 않았지만 결과적으로 의료기관들만이 독점적으로 데이터를 관리하게 되었다. 현재 연구 목적이나 헬스케어 프로그램 목적으로 의료기관과 기업 사이 의료데이터 교환이 있지만, 이 경우도 문제가 있다. 환자 자신이 이런 교환을 인지할 수 없기 때문이다.

의료데이터 공유가 이뤄지면 응급실에서 기본적으로 진행되는 검사를 50%까지 감축할 수 있다는 보고도 있다(메디블록팀, 2017 재인용; 고우균, 2018). 또한 현재 의료데이터 관리 체계는 허위 보험 청구, 의료 데이터 허위 기재, 임의 변경 등을 방어하지 못할 수 있다. 소수 전문가 집단이 의료데이터를 독점적으로 점유하기 때문에 의료데이터의 신뢰성이 공개적으로 보증될 수 없고, 전문가와 의료기관의 윤리 의식에만 의존해야 한다. 의료데이터가 완전히 디지털화되지 않은 상황도 데이터 공유를 어렵게 한다. 이런 문제를 해소하기 위해서 국제적으로 전자의무기록(EMR, Electronic Medical Record) 시스템이 확산되고 있지만 충분하지 않다. 미국조차도 전자의무기록(EMR)을 갖춘 의료기관은 전체의 절반 정도에 불과한 것으로 조사되었다.

의료 데이터 관리 문제를 논의하기 위해서는 우선 데이터에 관한 소유권 문제가 재정의되어야 한다. 의료데이터는 누구의 소유인가? 환자에 대한 기록이므로 환자의 것인가? 기록하고 관리하는 곳이 의료기관이므로 의료기관에게 소유권이 있나? 양자 모두에게 권리가 있다고 볼 수 있다. 한편으로 환자는 의료데이터의 원천이라는 점에서 권리가 있고 다른 한편으로 의료기관은 데이터를 생성하고 관리하고 있다는 점에서 권리가 있다. 환자와 의료기관 양자 모두 정당한 자격이 있는데 그동안 환자는 그 권리를

충분히 행사하기 어려웠다. 이것이 의료데이터 관리권한의 재분배가 필요한 배경이다.

의료데이터 권한의 재분배와 의료 기록의 위변조를 방지하기 위해서 미국 정부와 기업들은 의료데이터 시스템을 블록체인으로 재구축하는 다양한 시도를 하고 있다. 국내에서도 교보생명은 블록체인 플랫폼으로 보험청구에 필요한 정보를 참여자들이 공유하는 서비스를 계획하고 있다(유성민, 2017). 그리고 EMR 시스템을 블록체인으로 전환하려는 연구도 있다(박홍식 외, 2017). 최근 블록체인 기술은 인공지능과 결합하면서 강력해지고 있다.

의료 데이터 관리의 재분배 또는 환자-중심 의료 체계는 개별 환자를 위한 의료서비스의 질을 향상시킬 것이다(Kamel Boulos, et al, 2018; Zhang, et al, 2018). 메디블록은 역시 단일 주체의 중앙집중적 단독 관리는 한계가 있다는 점을 강조하며, 탈중앙화를 상징하는 블록체인 기술로 현행 의료데이터 체계를 재구현하고자 한다. 일반적으로 의료데이터 블록체인 서비스는 의료데이터를 공유할 수 있고, 누가 데이터에 접근했는지, 환자와 제공자의 신원과 신뢰성 보증, 건강 공급망의 관리 최적화, 연구자와 의료적 실험을 위한 데이터 공유와 합의, 보험, 사기 사건 탐지와 예방 등을 기대할 수 있다.

메디블록 백서가 '환자 중심'이라는 단어를 자주 사용하지만 그렇다고 해서 기존 의료기관 행위자의 이익에 반하는 것은 아니다. 그런 점에서 맥락적으로 단지 '환자 중심'이라기 보다는 '모든 이해당사자 참여적 플랫폼'에 더 가깝다. 사실 의료데이터 플랫폼은 기존의 의료기관을 포함하여 새롭게 데이터의 소유권을 행사할 환자와 대량의 데이터를 원하는 연구자들까지 모든 이해당사

자가 동의해야 수립 가능하다. 만약 가장 많은 의료데이터를 가지고 있는 의료기관들이 적극 반대한다면 이 플랫폼은 잘 작동하지 않을 수 있다. 또는 환자들이 자신의 데이터를 적극적으로 관리하기 위해 참여하지 않는다면 이 플랫폼은 활력을 잃을 것이다.

이 기술에서 가장 큰 어려움은 흩어져 있는 환자 데이터를 관리하는 것이다. 계속 생성되는 의료데이터의 양도 많고 블록체인이 분기하면서 다수의 블록체인이 수립될 수도 있다. 게다가 이 서비스는 보안과 사생활 문제도 일으킬 수 있다. 그래서 최근 의료 분야 블록체인 서비스들은 혼합적 접근 방법을 개발하고 있다 (Kamel Boulos, et al, 2018; Zhang, et al, 2018). 의료 분야 블록체인은 블록체인 기술을 이용해서 역설적으로 데이터의 통합을 지향하지만, 그렇다고 해서 반드시 물리적으로 데이터가 집중될 필요는 없다. 흩어져 있는 환자의 데이터에 대한 환자 자신의 권한을 구현하면 충분하다[11].

메디블록도 혼합적 방법으로 데이터를 관리하도록 설계되었다. 전체 데이터는 별도의 데이터베이스에 저장되고 기본 색인 정보만을 블록체인 플랫폼상에서 교환한다. 메디블록 플랫폼은 의료기관이 작성한 의료데이터만이 아니라 환자 개인이 작성한 의료 데이터 (PGHR, Patient-Generated Health Record)를 통합하여 저장하고 관리할

11) 예를 들어 "옴니PHR(OmniPHR)"은 개인건강기록(PHR, personal health record) 분산과 상호운영성에 초점을 둔 모델이다. 이 모델은 네트워크 전체 노드들 안에 들어 있는 암호화된 데이터블록에 PHR을 저장한다. 각 블록은 정보를 기입한 주체(건강관리전문가, 환자, 관리사, 의료 장치)에 의해서 서명된다. 완전히 분산적으로 환자 정보를 관리한다. 블록체인 건강관리 회사, 해시드 헬스(Hashed Health)는 기존의 신뢰받은 기관을 위한 기록 장부를 단일하게 관리하고 그 외 기관들을 위해서는 간소한 형태의 장부를 허락한다. MIT의 메드렉(MedRec)은 비트코인 블록체인과 전통적인 데이터베이스의 중간 형태를 취한다. 여기서 데이터를 생성한 노드는 스스로 자기 데이터를 관리한다. 그래서 모든 노드들은 메드렉 데이터 저장소이면서 서버이고 블록체인 관리자가 된다(Kamel Boulos, et al, 2018).

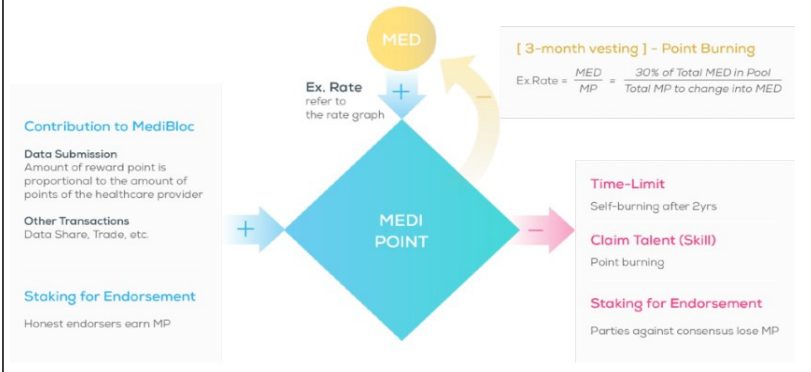
수 있다. 여기서 환자는 자신의 데이터를 생산함으로써 지식 생산에 참여하게 된다. 이렇게 통합된 데이터는 병원 진료에 응용될 뿐만 아니라 일상적인 헬스케어 서비스 분야로도 확장될 수 있다.

2) 메디 포인트와 메디 코인

메디블록 플랫폼은 모든 이해당사자가 참여할 수 있는 의료 데이터 관리와 공유를 위해서 모든 참여자에게 적정한 역할과 권한을 배분하고 그에 상응하는 보상을 지급한다. 이 플랫폼에 존재하는 데이터는 크게 3가지다. 의료데이터, 개인 데이터, 그리고 메디블록 플랫폼 활동과정에서 생성되는 메디 데이터(MED data)다. 참여자들은 먼저 계정을 생성해야 한다. 메디블록 계정은 일반 사용자, 의료공급자, 의료연구자로 구분한다. 기술적으로는 모두 같은 방식으로 생성되지만, 역할의 차이가 있고 계정 주체는 역할에 맞는 기능과 권한, 신뢰도를 형성해야 한다.

모든 계정은 기본적으로 자신의 의료데이터에 대한 읽기와 쓰기 권한을 가진다. 응급상황에 대비하기 위해서 계정 소유자는 자신의 가족 등에게 사용 권한을 부여할 수도 있다. 의료공급자와 연구자는 적정한 신뢰를 얻는 경우 타인의 의료데이터 읽기와 쓰기 권한을 가질 수 있다. 이 과정을 지원하기 위해서 메디블록 플랫폼은 의료데이터 검색 기능을 제공한다. 타인의 의료데이터를 열람하는 경우는 대개는 다음 두 가지에 해당한다. 의료공급자가 의료 서비스 제공 목적으로 열람을 요청하는 경우와 의료데이터를 이용해 의료 연구를 수행하고 헬스케어 서비스를 개발하려는 경우다. 이 경우 별도의 인증과 해당 계정 소유자의 승인이 필요

하다. 의료연구자는 스마트 계약 방식으로 계정 소유자와 데이터를 교환할 수 있다.



〈그림 3〉 메디 포인트(MP)와 메디토큰(MED) 교환관계 (메디블록팀, 2017)

메디 블록 플랫폼상에서 통용되는 화폐 개념으로는 메디포인트(MP, Medi Point)와 메디토큰(MED, Medi Token)이 있다. 메디포인트(MP)는 메디블록 플랫폼 상에서 수행하는 활동을 통해서 획득할 수 있다. 이것은 일종의 참여도, 평판, 기여도에 대한 지표로서, 사용자간 교환이 불가능하고 플랫폼 외부로 가지고 나갈 수도 없지만, 일정 기간 보유하면 메디토큰(MED)으로 교환할 수 있다. 그 반대 방향으로도 구매가 가능하다.

메디토큰(MED)은 메디블록팀이 토큰 표준에 따라 발행하고 플랫폼 기여도에 따라 분배하고 판매도 한다. 메디토큰(MED)은 사용자간 교환이 가능하고 다시 현실 화폐로 전환도 가능하다. 전체적 흐름을 보면 플랫폼 활동을 통해서 획득한 메디포인트(MP)는 메디토큰(MED)으로 바꿀 수 있고 메디토큰(MED)은 다시 현금

이 될 수 있다. 반대로 현금으로 메디토큰(MED)을 구매하고 메디토큰(MED)으로 메디포인트(MP)를 구매할 수 있다.

메디블록은 별도의 공급자 인증 시스템을 계획하고 있다. 인증방법은 현행의 기관 인증을 그대로 허용하는 방법이 있고, 다른 하나는 플랫폼 내부에서 진행하는 방식이 있다. 플랫폼 내에서 이미 인증된 사람들로부터 투표 방식으로 인증 과정을 거치는 것이다. 이 방식의 신뢰성을 높이기 위해서 이 과정에 참여하려면 참여자는 자신의 메디포인트(MP)를 보증금으로 걸어야 한다. 최종 투표결과와 동일한 투표를 한 참가자는 추가 메디포인트(MP)를 보상으로 받고, 그렇지 못한 참가자는 보증금으로 걸었던 메디포인트(MP)를 잃게 되는데, 이는 참가자들의 정직성에 대한 보상과 벌금에 해당한다. 투표 결과는 공개하지 않는다.

메디블록팀은 이런 보상체계를 통하여 모든 이해당사자를 유인할 수 있다고 본다. 예를 들어서 의료공급자가 자신의 의료데이터를 메디블록 플랫폼에 등록한다면, 해당 계정으로 대량의 메디포인트(MP)를 보상으로 받을 수 있다. 의료공급자는 이것을 다시 메디토큰(MED)으로 바꾸고 이어서 현금으로 전환할 수 있다. 따라서 의료 데이터를 많이 보유하고 있는 의료공급자들은 추가적인 경제적 이익을 얻을 수 있다.

5. 토론: 블록체인과 사회의 상호 구성

2008년 리먼 사태는 가장 신뢰할 수 있어야 하는 금융기관이 가

장 신뢰할 수 없을 때 얼마나 위험한지를 단적으로 드러냈다. 그 과정에서 비트코인은 기존의 지배적 시스템을 비판하면서 대안의 기술시스템을 선언했다. 비트코인은 사회문제를 제기하면서 등장했고, 또한 다수의 참여가 필수적이라는 점에서 사회적 지지를 필요로 한다. 그런 점에서 블록체인은 기술시스템이면서 사회시스템이기를 희망하고 있다.

1) 비트코인, 거버넌스의 자동화

비트코인은 암호화된 열쇠가 주소 기능을 함으로써 그것만으로도 충분히 식별할 수 있기 때문에 개별 비트코인의 소유자와 수신자는 익명 상태로 있을 수 있다. 모든 거래는 공개되지만 개별 주체의 신원은 거래 당사자들조차도 알 수 없다. 중앙기관 없는 직접 거래, 그리고 당사자들에게도 익명성을 부여함으로써, 비트코인은 궁극적으로 사회적 의사결정 과정, 즉 거버넌스를 자동화했다.

> "이 네트워크의 견고함은 비구조화된 단순성에 있다. 노드들은 거의 조정 없이 한 번에 모두 동작한다. 노드들은 식별될 필요도 없다. 메시지는 특정 경로 지정 없이 단지 최선의 노력 기반(best effort basis) 방식으로 전달되면 그만이다(Nakamoto, 2008)."

물론 '거버넌스의 자동화'는 블록체인이 처음 구현한 것은 아니다. 전통적인 정부 시스템, 사법 시스템, 병원 시스템 등은 모두 의사결정을 절차화하는 사회적 시스템이다. 절차화는 자동화를 의미했고 그런 만큼 효율적이었기 때문에 누적적으로 진화해왔다. 블록체인은 그러한 거버넌스의 자동화를 단일 기술로 구현하고자 했다.

특히 비트코인의 보상 메커니즘은 자동화에 중요한 구성 요소다. 참가자들은 작업증명을 수행하고서 비트코인을 보상으로 받는다. 그 외 거래 수수료도 받을 수 있다. 비트코인이 현실 화폐와 교환되면서 참가자들의 동기부여는 더욱 강해졌다. 그러나 보상은 신뢰를 유지하는 여러 가지 방식 중 하나일 뿐이다. 단지 보상만으로 블록체인 네트워크가 잘 작동할 것이라고 확신하기는 어렵다.

블록체인은 다수의 참가자가 네트워크를 형성할 때 잘 작동할 수 있다. 일정 수 이상의 참가자들이 없다면 블록체인은 아무것도 할 수 없다. 마이클 외(2018)는 블록체인 기술이 신뢰의 필요성을 완전히 없앨 수 없다고 표명했다. 무엇보다도 비트코인은 다수의 참가자로부터 신뢰받을 때 강화될 수 있기 때문이다. 그런 점에서 비트코인은 기술적이면서 동시에 사회적이다.

비트코인 시스템은 급진적으로 사회를 전환하려는 목적으로 출발했다고 평가받기도 한다. 비트코인에 대한 기대는 열광자들에게서만 나타나는 것이 아니라 상당히 두꺼운 지지층을 형성하고 있다. 비트코인은 자율적인 시장 거래를 구현함으로써 독자적인 통치성과 동료 정신이라는 사회성을 생산하고 있다. 비트코인 열광자들은 그 협력적 플랫폼을 상호적으로 구축하는데 가치를 두고 있다. 이런 "기반시설 차원의 상호주의(infrastructural mutualism)"는 이미 자유 소프트웨어, P2P 기술 생산, 공유 실천 등 오랜 역사가 있다(Swartz, 2017; 2018: 85).

한편 역설적으로 블록체인이 대체하고자 했던 제3자 없는 시스템, 또는 새로운 거버넌스 모델이 상당히 어렵다는 것도 확인되었다. 지난 10년 동안 비트코인은 여러 내부 분쟁을 겪으며 다

양하게 분화했다. 예를 들어 비트코인은 분쟁 끝에 결국 비트코인 캐시와 분리되었다. 이 분야 개발자들은 창의적이고 적극적이어서, 블록체인이 어떤 한계점이 보이면 어떻게든 조금씩 수정을 가하고 싶어했다. 그런데 그 덕분에, 논쟁과 분화의 소란스러운 과정에서도 비트코인 공개장부가 임의적 수정과 변조로부터 안전하다는 것이 확인되기도 했다(마이클 외, 2018).

지난 10여년의 짧은 비트코인 역사를 돌이켜 볼 때, 비트코인은 기술적인 차원에서만이 아니라 사회적 차원에서 완전하지 않다는 것을 보여주었다. 그렇지만 그 과정에서 기술사회적으로 용인할 만큼의 안전성을 '공개적으로' 입증함으로써 단일 기술로서 '거버넌스의 자동화'를 수립했다.

2) 네임코인, 자동화되지 않는 것

네임코인은 비트코인 보다 '성공'하기 더 어려울 수 있다. 사실 비트코인은 다른 화폐 시스템과 공존할 수 있다. 오히려 비트코인은 현행 화폐시스템의 대안이라기보다는 추가적인 시스템이라고 할 수 있다. 비트코인은 현행 화폐들과 교환 가능하고 그런 만큼 병존할 수 있다. 그러나 네임코인의 경우는 다르다. 네임코인은 도메인 네임의 성격상 현행 DNS 시스템과 공존하기 어렵다. DNS 시스템은 웹상에서 완전히 고유한 식별주소를 배포해야 하기 때문에 유일한 시스템이어야 한다. 그 때문에 네임코인은 서서히 성장하는 것이 어렵고, 이미 지배적인 관리 방식을 거의 일시에 완전히 대체해야만 존립할 수 있다. 이것이 바로 현재 네임코인 사용자가 거의 없는 이유이기도 하다[12].

또한 네임코인은 비트코인이 가지고 있는 모든 구조적 취약점을 공유한다. 공격자가 네임코인 네트워크 채굴 파워의 51% 이상을 통제한다면 그 공격자는 거래 명령을 배제하거나 수정할 수 있다. 공격자는 블록을 수정하고 수정된 거래 위에서 새로운 블록체인을 구축할 수 있다(Loibl, 2014; Wang, et al, 2017). 네임코인처럼 작은 네트워크는 그런 공격에 더 쉽게 노출될 수 있다.

그럼에도 불구하고 네임코인은 상당한 호소력이 있다. 현행 DNS 시스템 관리기구인 ICANN은 미국 정부에 의해서 탄생했고, 최근까지도 미국 정부의 권한위임 계약에 의해 운영되어 왔으며, 지금도 여전히 캘리포니아 주법 관할권 내 법인이다(김지연, 2013; Loibl, 2014). 현재 ICANN은 일국적 이미지를 벗기 위해서 미국 정부에게 보고서를 제출하는 대신 모든 인터넷 사용자들에게 연간 보고서를 공개하고 있다. 이에 비해서 네임코인은 중앙집중적 독점적 기관이 없을 뿐만 아니라 일국적 영향을 받지 않는다.

네임코인은 잠재성 있는 대안이다. 비용 측면에서 현행 DNS 도메인 네임 등록 가격보다 훨씬 저렴하다. 현행 DNS 도메인 네임 등록 가격은 매년 약 10달러인데, 네임코인의 도메인 등록 비용은 무료 거래도 가능하다. 다만 도메인 네임 접속을 위해서 채굴자에게 네임코인 거래 비용이 지불되어야 한다[13].

12) 한편 ICANN은 2014년 네임코인에 대해서 언급한 바 있고, 네임코인을 직접 공격하지 않고 있다. 우연인지 의도적인지 확인할 수는 없지만, 현행 DNS 시스템상에서 네임코인의 최상위 도메인(.bit)을 사용하지 않고 있다. ICANN DNS 루트존에 이 도메인을 할당하지 않음으로써 네임코인의 영역을 간접적으로 보증해주는 효과가 있다. 따라서 현행 DNS 서버는 .bit 도메인 요청에 응답하지 않고 오류 쿼리를 내보낸다. 네임코인 게이트웨이 서비스 제공자는 인터넷상에서 이 오류 쿼리를 수집해서 해당 요청자에게 네임코인 도메인 주소를 회신해줄 수 있다.

13) 2012년 이후 네임코인 등록 비용은 많이 내렸고 지금은 거래 비용을 제외하면 무료다. 현재 새로운 .bit 도메인 비용은 0.015 NMC (name_new) + 0.005 NMC(name_firstupdate) + 0.005

네임코인 초기에 도메인 거래 비용은 다소 비싸게 책정된 적이 있었는데, 그 이유는 도메인 스쿼팅(domain squatting)을 방지하기 위해였다. 네임코인의 등록비용이 너무 적어서 한 사람이 수천 개의 도메인을 보유하는 것도 가능하다[14]. 도메인 스쿼터들은 스스로는 필요하지 않은 도메인을 대량 구매해서 실제 사용자(저작권자 또는 상표권자)에게 비싸게 재판매하려고 한다. 현행 ICANN은 도메인 스쿼팅을 불공정한 행위로 보고 이를 조정하는 업무를 수행하고 있다.

이 문제는 어떤 DNS 시스템에서나 출현할 수 있는 문제지만, 네임코인은 특히 이 문제에 취약하다. 네임코인은 중앙기관이 없기 때문에 스쿼팅으로 발생하는 분쟁을 조정할 수 없다. 누군가가 자신의 상표명에 해당하는 도메인네임을 다른 사람이 부당하게 '소유'하고 있다고 주장한다면 정말 그런지를 판정하는데 상당한 노력을 들여야 한다. 해당 도메인네임을 가지고 있는 사람 역시 자신의 정당성을 주장할 것이기 때문이다. 이 문제를 해소하기 위한 몇 가지 기술적 해법이 제시되고 있다. 그들은 기본 시장이 합리적이라면 이 문제는 축소될 수 있다고 낙관한다(Kalodner, et al., 2015).

네임코인 모델은 DNS의 일반적인 과정은 자동화할 수 있지만 도메인 네임 사용자 간 분쟁 조정까지 자동화하기 어렵다는 것을 보여준다. 최근 일부 연구자들(Kalodner, et al. 2015)은 DNS의 이런 특성을 고려하여, 분산형 플랫폼과 중앙집중식 서비스를 혼합한 모델을 제기하기도 한다. 예를 들어서 스쿼팅과 같은 분쟁을 조정하는

NMC (name_update) = 0.02 NMC이다.

14) 현재 새로운 .bit 도메인 비용은 0.015 NMC (name_new) + 0.005 NMC(name_firstupdate) + 0.005 NMC (name_update) = 0.02 NMC이다.

일은 중앙기관을 배치하고 나머지는 네임코인 모델에 따르는 것이다.

블록체인의 기술적 합리성이 사회 문제를 모두 해소할 수는 없지만, 적어도 문제를 제기하는 좋은 방법이 될 수는 있다. 더 나아가 블록체인이 일상적으로 사용되는 상황이 형성된다면 사용자들은 네임코인 방식에 더 익숙해질 수 있고 그렇다면 네임코인을 더 쉽게 받아들일 수 있다.

3) 메디블록, 모든 이해당사자에게 환영받기

메디블록 역시 기능적인 완성만으로 충분하지 않을 것이다. 기존에도 의료 관련 응용프로그램들은 다수 존재했었지만 그다지 성공하지 못했었다. 관련 이해당사자들(사회집단)이 그 필요에 동감하고 참여하지 않거나 또는 참여할 수 없었기 때문이다. 의료 관련 플랫폼의 성공은 의료데이터와 관련된 모든 이해당사자로부터 환영받는 것이 필수적이다. 어떻게 대안적 체계가 모든 이해당사자에게 환영받을 수 있을 것인가?

메디블록도 동일한 문제에 직면한다. 메디블록은 현행 의료 시스템의 문제를 지적하는 대안적 체계이므로, 현행 의료기관은 이 시스템에 대해서 아무 이득이 없거나 더 나아가 손해라고 판단할 수 있다. 대안적 체계(환자 중심 관리)가 현재 지배적인 이해당사자(의료기관)에게 특별한 매력이 없거나 더 나아가 이해관계를 침해한다면, 그들은 대안 체계에 협조하지 않거나 때로는 적극적으로 반대할 것이다. 현재 가장 많은 의료데이터를 보유하고 있는 의료기관이 자신의 데이터를 제공하지 않는다면 메디블록 플랫폼은 빈약해질 것이고 궁극적으로 충분한 참가자를 모을 수 없을 것이다.

이 문제를 해결하기 위해서, 우선 메디블록은 일반 사용자, 의료공급자, 의료연구자와 같이 관련 이해당사자들이 모두 참여할 수 있는 조건을 설정했다. 이들 3유형의 이해당사자는 계정을 생성함으로써 메디블록 플랫폼상에서 동등한 참여자로 간주된다. 이 플랫폼에서는 의료공급자만이 아니라 환자도 자신의 상태를 기록함으로써 의료데이터 생산자가 될 수 있다. 각 계정 주체는 자신의 역할에 맞게 신뢰도를 형성함으로써 그에 맞는 권한을 가질 수 있다.

다음으로 메디블록은 모든 이해당사자에게 환영받기 위해서, 모든 참여자에게 그에 상응하는 보상(메디포인트와 메디토큰)을 지급한다. 원리적으로 이 시스템이 제공하는 보상은 '실재'가 아니라 '가상'이다. 다시 말하자면 현실 화폐를 한쪽에서 다른 쪽으로 이동하는 것이 아니라 새로운 가상 화폐를 생성해서 분배하는 것이다. 누구도 자신이 이미 가지고 있는 자원을 잃지 않고도 추가적인 보상을 얻는 것이다. 따라서 현행 지배적인 이해당사자(의료기관), 즉 의료데이터를 많이 가지고 있는 의료기관은 자신의 데이터를 공유함으로써 많은 보상을 받을 수 있다. 일반 사용자들도 자신의 건강 데이터를 등록함으로써 보상을 받을 수 있다. 따라서 이 플랫폼에서는 '추가적인 보상'만 존재한다.

마지막으로 메디블록의 보상은 '실재'가 될 수 있어야 한다. 모든 이해당사자가 만족할 수 있는 플랫폼을 설계하는 것은 단지 기술적인 노력만으로 충분하지 않다. 참가자들에게 지급되는 보상이 단지 가상의 숫자에 머물지 않고, '실재적 가치'를 가질 수 있는지 여부에 달려있다. 그것은 사회적 차원의 문제가 된다. 메디블록 네트워크에 다수의 참여자들이 참여해서 보상의 규모가 상당히 성장해야 하고, 네트워크 외부에 있는 사회구성원들이 메디

토큰(MED)과 현실 화폐를 교환하고자 욕망해야 한다. 외부 사회 구성원들은 메디블록 네트워크의 규모와 역동성을 관찰하면서 그런 욕망을 형성할 것이기 때문에 메디블록 네트워크 내부와 외부는 서로를 구성해야 한다.

결과적으로 메디블록 플랫폼이 모든 이해당사자로부터 환영받을 수 있는 동력은 의료데이터가 메디토큰(MED)을 거쳐서 현실 화폐로 전환되는 것이다. 동시에 그 과정은 사회적 정당화를 필요로 한다. 환자는 의료데이터의 원천으로서 지위를 회복하고 또한 의료데이터 생산자로서 의료기관과 동등해질 수 있다. 이것은 전통적인 지식생산자(의료기관, 의료전문가)의 지위에 대한 도전인데, 추가적인 보상이 그로 인한 저항을 해소할 가능성이 있다.

그러나 무엇보다도 다수의 환자(의료 소비자)들이 이 과정을 원해야만 한다. 그들이 자신의 의료데이터를 의료기관(병원)에만 맡기기보다는 스스로 통제하길 원해야 한다. 그런데 자신의 의료데이터를 직접 관리하는 일은 많은 주의와 노력을 수반하는 일이다. 여전히 대부분의 사람은 의료전문가가 그런 일을 대신해 주길 기대한다. 메디블록은 기술과 사회 양쪽 모두에서 실험 중이다.

6. 결론

블록체인은 단지 기술적 체계만이 아니라 사회적 체계이어야 한다. 비트코인 초기 그룹과 열광적 지지자들은 비트코인 네트워크를 실체적인 것으로 만들어 냈다. 그 결과 비트코인은 사회적 의

사결정 과정(거버넌스)을 자동화하는데 접근했다. 그러나 비트코인은 여전히 불안정하며 여러 가지 구조적 취약점을 가지고 있다. 선의의 참여자들이 네트워크 채굴 파워의 51% 이상을 유지해야만 한다. 비트코인의 경험은 내부 분쟁이 합의에 이르기 어렵다는 것도 드러냈다. 창의적이고 적극적인 블록체인 개발자들은 다양한 변이 모델을 개발했고 결국 갈라져 나갔다.

네임코인은 도메인 등록이라는 특정한 기능 때문에 비트코인보다 보상 구조가 약하고, 현행 시스템과 공존하기보다는 완전히 대체해야 한다는 난관이 있다. 특히 네임코인의 사례를 통해서 이해당사자 간 분쟁 조정은 자동화하기 어렵다는 것을 보여주었다. 그럼에도 불구하고 네임코인은 잠재성을 가지고 있다. 독점적 DNS 관리 구조를 분산적 관리로 전환할 수 있고 비용 측면에서도 현행보다 저렴하다. 블록체인의 기술적 합리성이 사회 문제를 모두 해소하지 못하더라도 문제를 제기하는 좋은 방법이 될 수 있다. 대안적 체계가 등장하는 것만으로도 현행 관리 방식에 강한 영향을 줄 수 있다.

블록체인은 이론적으로 다양한 이해당사자들 사이의 관계를 재설정할 수도 있다. 메디블록은 의료데이터와 관련된 모든 이해당사자로부터 환영받을 수 있는 논리적 구조를 설계했다. 현행 의료체계에서 의료공급자와 환자의 지위는 불균형했었는데, 메디블록 플랫폼은 그런 지위를 재조정하려고 한다. 이 플랫폼에서는 의료공급자만이 아니라 환자도 자신의 상태를 기록함으로써 의료데이터 생산자가 될 수 있다. 메디블록이 모든 이해당사자를 흡인하는 동력은 보상 메커니즘이다.

이런 보상은 블록체인 플랫폼이 자동으로 작동할 수 있는 근원이다. 그런데 더 중요한 것은 보상으로 주어지는 '가상 화폐'

가 '실재 화폐'가 될 수 있어야 한다는 것이다. 모든 이해당사자가 만족할 수 있는 플랫폼을 설계하는 것은 기술적인 노력이지만, 참가자들에게 지급되는 보상이 실재적 가치를 가지는 것은 사회적 작용이다. 블록체인 네트워크 내부 참가자와 외부 사회구성원들이 서로를 관찰하면서 상호 구성될 때 블록체인의 거버넌스는 궁극적으로 작동할 수 있다.

한국에서 올해 초, 격돌했던 문제 중 하나는 "블록체인과 화폐매커니즘을 분리할 수 있나?"라는 문제였다. '찬성'측은 "분리할 수 없다"고 했고 '반대'측은 "분리할 수 있다"고 주장했다. 우리는 찬성과 반대 입장이 나뉘는 상황에 직면할 때 어느 한쪽이 정답이고 나머지는 오답일 것이라고 전제한다. 그러나 본 논문의 설명에 근거한다면 양자의 입장은 각각 부분적으로 옳다. 다시 말해서 논리적 차원에서는 분리할 수 있지만 현실차원에서 분리한다면 사실상 작동하지 않을 수도 있다. 블록체인과 화폐매커니즘의 분리는 보상이 없는 상황을 의미하기 때문이다.

그럼에도 불구하고 보상 메커니즘이 블록체인 성공의 유일한 내용이 될 수는 없을 것이다. 우리는 사회작용이 보상과 처벌에 의해서만 작동하지 않는다는 것을 잘 알고 있다. 네임코인과 메디블록은 그런 대안을 지지하는 다수의 참여자가 등장할 때, 그런 사회적 필요가 정당화될 때 실체적인 것이 될 수 있다. 따라서 블록체인은 시민 참여적 거버넌스와 진지한 결합을 고민할 필요가 있다. 참가자들을 단지 보상을 원하는 개별 행위자로 상정하기보다는 사회적 의미를 생성하는 시민(공동체)으로 고려할 필요가 있다. 그들은 블록체인이 구현한 자동화로 인한 이득만 아니라, 그로 인한 위험도 감당해야 하는 주체들이기 때문이다.

참고문헌

- 고우균 (2018), 「MEDIBLOC: 블록체인 혁명 그리고 의료의 미래」, 『고려대학교 과학기술학 콜로키움 발표자료(2018. 6. 7)』.
- 김원 (2018), 「비트코인 블록체인 동작원리 및 진화」, 『ITFIND』, [구글검색 2018. 9. 25]
- 김의석 (2018), 「블록체인 혁신성 연구」, 『한국전자거래학회지』 23(3), 173-187쪽.
- 김지연 (2013), 「인터넷 거버넌스와 전문성의 정치: 도메인네임시스템(DNS)의 '중심'과 '경계'」, 『경제와사회』 98, 304-340쪽.
- 박홍식·정재우·김응모 (2017), 「블록체인(이더리움)을 이용한 의료정보 교류 시스템 구축 방안 연구」, 『*Proceedings of KIIT Summer Conference*』, 436-437쪽.
- 마이클 J. 케이시 · 폴 비냐 (2018), 『트루스 머신: 블록체인과 세상의 모든 것의 미래』. 유현재·김지연 옮김. 미래의 창.
- 메디블록팀 (2017), 「메디블록 백서(MediBloc Whitepaper)」, www.medibloc.org
- 이혁준·이수미 (2016), 「비트코인의 신뢰구조와 이중지불의 위협」, 『정보보호학회지』 26(2), 25-30쪽.
- 유성민 (2017), 「블록체인을 인한 서비스 플랫폼의변화」, 『NIA 지능화 연구 시리즈』. [구글검색 2018. 10. 4]
- 채만수 (2018), 「비트코인은 화폐인가–엉뚱한 동기, 황당한 파장, 혹은, 황당한 동기, 엉뚱한 파장」, 『정세와노동』 143, 46-73쪽.
- Bayer, D. & Haber, S. (1992), "Improving the Efficiency and Reliability of Digital Time-Stamping". [구글 검색 2018. 1. 16]
- Haber, S. & Stornetta, W. S. (1991), "How to Time-Stamp a Digital

Document", A.J. Menezes & S.A. Vanstone (eds.), *Advances in Cryptology - CRYPT0 '90, LNCS* 537, pp. 437-455.

- Kamel Boulos, M. N., Wilson, J. T., & Clauson, K. A. (2018), "Geospatial Blockchain: Promises, Challenges, and Scenarios in Health and Healthcare", *International Journal of Health Geographics*, p. 17, p. 25.
- Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J. & Narayanan, A. (2015), "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design". [구글검색 2018. 9. 24]
- Karame, G. & Androulaki, E. (2016), *Bitcoin and Blockchain Security*. Artech House: Boston·Lodon.
- Nakamoto, S. (2008), Bitcoin White Paper, "Bitcoin: A Peer-to-Peer Electronic Cash System", http://bitcoin.org/bitcoin.pdf
- Musiani, Francesca (2013), "A Decentralized Domain Name System? User-Controlled Infrastructure as Alternative Internet Governance". [구글검색 2018. 10. 4]
- Swartz, L. (2017), "Blockchain Dreams: Imagining Techno- Economic Alternatives After Bitcoin", in Manuel Castells et al(eds.), *Another Economy is Possible: Culture and Economy in a Time of Crisis.* Polity: Malden, MA. pp. 82-105.
- Swartz, L. (2018), "What was Bitcoin, what will it be? The Technoeconomic Imaginaries of a New Money Technology", *Cultural Studies*, 32(4), pp. 623-650.
- Liang, J., Li, L., & Zeng, D. (2018), "Evolutionary Dynamics of Cryptocurrency Transzction Networks: An Empirical Study", *PLoS ONE*, 13(8), e0202202.

- Loibl, A. (2014), “Namecoin”. [구글검색 2018. 9. 15]
- Vitalik Buterin (2015), Ethereum White Paper, “A Next Generation Smart Contract & Decentralized Application Platform”. [구글검색 2018. 6. 25]
- Frankenfeld, P. J. (1992), “Technological Citizenship: A Normative Framework for Risk Studies”, *Science, Technology, & Human Values*, 17(4), pp. 459-484.
- Wander, M. (2011), “How Bitcoin Works”. [구글검색 2018. 7. 23]
- Wang, X., Li, K., Li, H., Li, Y., & Liang, Z. (2017), “ConsortiumDNS: A Distributed Domain Name Service Based on Consortium Chain”, *2017 IEEE 19th International Conference on High Performance Computing and Communications.* [구글검색 2018. 7. 23]
- Zhang, P., Schmidt, D., White, J. & Lenz, G. (2018). “Blockchain Technology Use Cases in Healthcare”, in Raj, P. & Deka, G. C.(eds.), *Blockchain Technology: Platforms, Tools and Use Cases.* Elsevier: Cambridge, MA, pp. 1-42.

논문 투고일	2018년 10월 09일
논문 수정일	2018년 11월 04일
논문 게재 확정일	2018년 11월 10일

A Comparative Study of Block Chain : Bitcoin · Namecoin · MediBloc

Kim, Ji Yeon

ABSTRACT

Bitcoin, which appeared in 2008, was merely a conceptual virtual currency, but it now enjoys the status as actual money. Bitcoin is an electronic money system that can be traded directly without a central trust institution. Thanks to the popularization of Bitcoin, blockchain technology has become a widespread concern. That technology is expanding not only the currency mechanism, but also a variety of other services. The possibility of a blockchain in relation to actual currency is ongoing. This paper investigates the technological characteristics and social construction of the blockchain by comparing the cases of Bitcoin, Namecoin, and MediBloc among blockchain applications. Namecoin emerged in 2013 is an attempt to replace the centralized Internet Domain Name System(DNS). There has been controversy over that current system for a long time, but replacing the already established system is not easy. Nevertheless, Namecoin has potential as an alternative. Meanwhile, MediBloc is an application that involves distributed management of medical data in South Korea. MediBloc claims that the key producers of medical data are patients themselves. This is to challenge to the question who is a knowledge producer of medical data. Through these three cases, it has discussed that blockchain technology does supports to form more democratic decision-making or simply provide a technical solution as automation. As a citizen, we can intervene in the realization of blockchains by presenting social agenda. This will be a method of the social construction of technology.

Key terms | Blockchain, Time stamp, Governance, Automation, Citizen Science