[2018 대한민국 정책컨벤션&페스티벌 싱크탱크 세션 세미나]

나카모토 사토시가 구상한
비트코인의 체계와 약간의 법적 고찰

일시: 2018년 11월 9일 (금) 오후 4시~6시
장소: 국회 의원회관 2층 제2간담회실
주관: (사)한국기업법연구소

좌장: 최준선 성균관대학교 법학전문대학원 명예교수
발제: 김태진 고려대학교 법학전문대학원 교수
토론: 심영 연세대학교 법학전문대학원 교수
토론: 최승노 자유기업원 원장
토론: 한석훈 성균관대학교 법학전문대학원 교수

(사)한국기업법연구소

나카모토 사토시(中本哲史)가 구상한 비트코인의 체계와 약간의 법적 고찰
- "Bitcoin: A Peer-to-Peer Electronic Cash System(2008)" 논문을 중심으로 -

김태진 (교수, 고려대학교 법학전문대학원)

I. 서설

가상통화 정보업체인 코인마켓캡(coinmarketcap)에 의하면 2018년 6월 19일 현재 가상통화의 합계는 총 1,627개이고, 그 시가총액은 316조 5,468억 원이상이며 이러한 가상통화는 코인 형태가 832개, 토큰 형태가 795개라고 한다.[1] 이러한 가상통화의 원조는 비트코인이다. 비트코인과 관련해서는, 2008년 11월 1일 나카모토 사토시(Satoshi Nakmoto; 中本哲史)[2]는 metzdowd.com 내의 암호이론에 관한 메일링리스트에 아래와 같은 이메일을 보내면서 전자통화로서의 비트코인에 관한 논문을 발표하기 시작하였는바,[3] 그 이메일에서 소개한 것이 바로 "비트코인: P2P 방식에 의한 전자적 통화 체계(Bitcoin: A Peer-to-Peer Electronic Cash System)"이라는 제목의 총 9페이지 상당의 논문이다.

[표 1: 나카모토 사토시가 보낸 이메일 원문]

Bitcoin P2P e-cash paper Satoshi Nakamoto Sat, 01 Nov 2008 16:16:33 -0700 I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. The paper is available at: http://www.bitcoin.org/bitcoin.pdf The main properties: Double-spending is prevented with a peer-to-peer network. No mint or other trusted parties. Participants can be anonymous. New coins are made from Hashcash style proof-of-work. The proof-of-work for new coin generation also powers the network to prevent double-spending. Bitcoin: A Peer-to-Peer Electronic Cash System (이하 논문의 내용이므로 생략함)

위 논문은 P2P 시스템을 통해 데이터블록을 연결한 블록체인과 작업증명(PoW)방식을 활

1) , "ICO의 개념과 규제 상황에 대하여," 법률신문 2018. 7. 9.자 법률정보 기사
자세한 내용은 , https://www.lawtimes.co.kr/Legal-Info/LawFirm-NewsLetter-view?serial=144637

2) 나카모토 사토시는 비트코인 프로토콜과 Bitcoin Core/Bitcoin-QT를 만든 인물이 칭한 이름이다. 국적, 성별, 개인인지, 그리고 위 이름이 본명인지 여부도 전부 현재 불명인 상황이다.

3) *"Satoshi's posts to Cryptography mailing list"*. Mail-archive.com. (Wikipedia 참조)
https://ja.wikipedia.org/wiki/%E3%82%B5%E3%83%88%E3%82%B7%E3%83%BB%E3%83%8A%E3%82%AB%E3%83%A2%E3%83%88#cite_note-1
그러나 그 당시 피드백으로 왔던 글들은 "가능성이 보이지 않습니다,""어려울 것 같습니다"라는 회의적인 의견들 뿐이었다고 한다.

용하여 이중지급 문제를 방지하기 위한 기술적 사상을 설명한 것으로서, 그로부터 몇 달이 지나지 않아 비트코인의 제네시스 블록이 생성되었는바,[4] 중앙통제가 없는 방식의 분산형의 암호화 통화가 등장하여 블록체인 기술과 더불어 전세계적으로 선풍적인 관심을 받았으며 이제 세계 각국은 이러한 중앙의 결제기관을 요하지 않는 블록체인형 가상통화를 어떻게 규제할 것인지를 고민하게 되었다.

나아가 최근에는 디지털 토큰을 발행하는 댓가로 이더리움 등 가상통화 등으로 투자금을 조달하는 등 마치 외부투자자들로부터 투자금을 조달하는 주식공개상장(IPO: Initial Public Offering)과도 유사한 "ICO"(Initial Coin Offering: 최초코인공개) 역시 많이 이용되고 있어 가상통화를 중심으로 한 법률관계나 규제에 대한 관심이 증가하고 있다.

한편 정부가 가상통화의 화폐기능을 일부 사실상 인정하였다는 보도에 대해서, 금융당국와 정부는 일단 신중한 태도를 보이고 있다. 즉 가상통화는 법정화폐가 아니며 어느 누구도 가치를 보장하지 않음을 밝히고, 대신 기반기술인 블록체인에 대해서는 연구개발투자를 지원하고 육성한다는 방침 하에서 G20 등 국제적인 가상통화 규제 논의 동향을 면밀히 보아가면서 국내 제도화에 대해 검토한다는 입장이며 다만 자금세탁 등 가상통화 거래와 관련한 불법행위의 경우 자금세탁방지 체계 하에서 엄격히 규제한다는 점은 분명하게 밝히고 있다.[5] 또한 2017년 9월 금융위원회는 한국에서는 ICO를 전면 금지하겠다는 원칙만을 선언한 후 구체적인 규제안에 대해 현재까지 별도의 입법적 조치나 현행 법률의 개정안을 내놓지 않은 상태이다. 이러한 급변하는 상황 속에서 '기본으로 돌아간다'는 마음가짐으로 가상통화와 블록체인 기술의 원조라 할 수 있는 나카모토 사토시라는 개인인지, 아니면 집단인지 알 수 없는, 그의 견해나 구상을 제대로 살펴보고자 한다.[6]

II. 「비트코인: P2P 방식에 의한 전자적 통화 체계」 논문의 개요

1. 체계 구상의 주안점

---

4) , "비트코인, 그 10년" 법률신문 2018년 11월 5일자 기사 참조 (최종방문일자 2018. 11. 5.) https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=147969&kind=
기존 블록체인 구조는 선형구조로서 암호통화의 이중지급 여부를 검증하기 위한 목적으로 고안된 것인바, 정보변경이 생기면 메인 블록체인에 제네시스블록이 추가되는 형태가 된다. 나카모토 사토시는 '은행들의 두 번째 구제금융을 앞둔 영국 재무장관'이라는 타임즈 1면 기사 제목(January 3, 2009 (The Genesis Block): "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.")을 제네시스블록에 메시지로 담음으로써, 정부가 대형 금융기관을 구제하는 현실을 비판하며 탈중앙화 정신을 강조했다.이상의 내용을 설명한 블로그(mablue) https://blog.naver.com/windells77/221365001788 (최종방문일자 2018. 11. 5.)

5) 금융위원회, "가상통화에 대한 정부입장", 2018. 1. 15.자 보도자료 및 금융위원회, "머니투데이 5. 28.일자 "정부, 가상통화 '화폐기능' 일부 인정"제하 기사 관련," 2018. 5. 28.자 보도참고자료 참조. 관련 내용은 아래 금융위원회 사이트 참조(최종방문일자 2018. 10. 11.).
http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=가상통화&r_url=&menu=7210100&no=32257
http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=가상통화&r_url=&menu=7210100&no=32491

6) 컴퓨터 프로그래밍이나 기타 기술적 측면에서 문외한이므로 번역에 따르는 오류 및 부족함은 모두 필자의 몫이다. 또한 이 글에서는 나카모토 사토시의 논문 중 '7. Reclaiming Disk Space, 8. Simplified Payment Verification, 9. Combining and Splitting Value, 11. Calculation' 부분은 생략하였다.

이 논문의 머리말에는 개요가 소개되어 있는데, 그 개요를 보면 나카모토 사토시가 무엇을 고민하였고 이를 해결하기 위해 어떠한 방식을 제안하였는지를 잘 알 수 있다.

우선 위 논문의 전체적인 개요는 다음과 같다:

첫째, P2P (peer-to-peer) 방식을 활용한 전자적인 통화가 실현된다면 금융기관을 매개로 하지 않고 당사자 사이에서 온라인 지급이 가능해진다.

둘째, 전자서명을 활용함으로써 부분적인 해결책이 될 수도 있지만, 그것만으로는 이중사용문제(double-spending)를 방지할 수 없다.

셋째, 그러나 신뢰받는 제3자(예컨대 금융기관 등)가 이중사용문제를 방지하기 위해 개입해야 한다면 전자적 통화의 잇점을 대부분 상실하게 되므로, 이러한 이중사용문제는 P2P 방식에 의해서 해결하는 방법을 제안한다.

그렇다면 이중사용문제란 무엇인가?

종이나 금속으로 이루어진 법화(달러, 엔화, 원화를 생각해보라)와 달리 가상통화는 디지털정보로만 구성되어 이 디지털정보를 복사하기만 한다면 얼마든지 계속적으로 사용할 위험성이 있었고 이것이 바로 이중사용(double spending) 문제이다.

또 금융기관 등 신뢰받는 제3자기관을 매개하게 되면 이러한 기관은 분쟁이 발생하게 되면 발생할 중재비용이 거래 비용보다 높기 때문에 완전하게 비가역적인 거래를 취급하지 않는다. 따라서 상인 스스로 조심해야 하고, 또 고객에게 많은 정보를 요구해야 하는바, 물론 이러한 손실이나 지급의 불확실성은 실물 통화를 사용함으로써 피할 수 있을 뿐 거래당사자들이 제3자 기관을 거치지 않고 통신채널을 경유하여 지급할 수 있는 메카니즘은 존재하지 않았던 것이다.

나카모토 사토시의 관점에서 필요하다고 본 것은 바로 거래할 때의 신용이 아니라 암호화된 증명에 근거한 전자거래시스템이고, 이러한 기술을 "블록체인"이라 할 것인바, 블록체인은 우리가 이메일을 보낼 때 이메일 주소, 내용, 첨부파일 등의 정보들을 기반으로 이메일 지문이 뜨면 그 지문을 떠서 옆에 붙여 보내면 받는 사람의 이메일 시스템이 수신시 그 지문을 대조해보는데, 이러한 원리를 암호화한 것으로 이해할 수 있다.[7] 이로써 희망하는 양 당사자는 신뢰받는 제3자기관을 거치지 않고 직접 거래할 수 있게 된다.

그리하여 컴퓨터상 사실상 비가역적인 거래를 함으로써 매도인을 사기로부터 보호하고, 용이하게 실시할 수 있는 관습적인 에스크로우(제3자기관에의 예탁)메카니즘에 의해 매수인 역시 보호된다고 보았다.[8]

따라서 나카무라 사토시는 논문의 개요에서 다음과 같이 밝히고 있다:

"순수한 P2P 전자통화에 의해 금융기관을 통하지 않고 당사자들이 직접 온라인 거래가 가능하게 된다. 전자서명은 문제의 일부를 해결하지만 신뢰받는 제3자기관에 의한 이중사

---

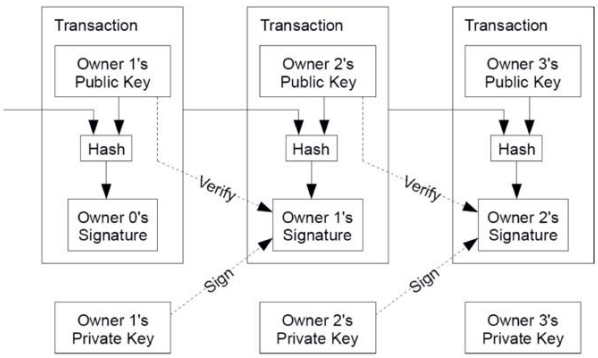
7) , "블록체인은 전자화폐로 통하는 열쇠"(제409회 월례강좌-블록체인과 가상화폐의 이해), 고려대 교우회보 No. 579, 2018. 10. 10.

8) Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008. 11. 1.) p1.

용 방지가 요구되기 때문에 이러한 혜택을 상실하게 된다. 이 시스템은 P2P 전자통화에 의한 이중사용 문제의 해결을 제안한다. 이 네트워크는 거래에 해쉬베이스의 계속적인 Proof of Work(*필자 주: '작업 증명'혹은 PoW으로 번역함)"체인에 해쉬값[9]으로서 갱신 일시를 기록하여 작업증명을 다시 고치지 않는 한 변경할 수 없는 이력을 작성한다. 가장 긴 일련의 체인은 거래이력을 증명할 뿐만 아니라 그것이 CPU 파워의 최대 pool에서 나왔다는 점을 증명한다. 대다수의 CPU파워가 네트워크를 공격하지 않는 노드(네트워크 접속포인트)에 의하여 통제되고 있는 한 가장 긴 체인이 작성되고 공격자를 물리친다. 네트워크 자체는 최소한의 구성으로도 충분하다. 메시지는 최선노력원칙으로 송신되고 노드는 자유롭게 네트워크로부터 이탈하거나 재접속할 수 있고, 이탈한 동안의 이벤트 증명으로서 가장 긴 작업증명 체인을 수신한다.[10]"

2. 거래(Transactions)

나카모토의 논문에 의하면, 하나의 전자코인(electronic coin)은 연속하는 디지털 서명의 체인(a chain of digital transaction)으로 정의된다. 전자코인의 각 소유자는 직전 거래의 해쉬와 다음 소유자의 공개키(public key)를 디지털서명으로 코인의 마지막에 추가함으로써 전자코인을 다음 소유자에게 전송하는데, 수취인은 일련의 서명을 검증함으로써 과거의 소유권을 검증한다.[11] 이처럼 거래이력은 블록의 형태로 기록되고 체인형상으로 꼬아져서 구성된다(이하 위 논문에 사용된 그림을 인용한다).



그러나 위 구조에서 나카모토 사토시가 문제점으로 지적한 것은 바로 위에서 나왔던 '이중사용' 의 문제, 즉 수취인이 과거의 소유자가 코인을 이중사용하지 않았음을 검증할 수 없다는 점을 들고 있다. 이에 대해 다음과 같이 기존의 집중관리형 시스템과 새로운 분산형 원장기술을 대비시키고 있다:

---

9) 앞의 블록 내용에서 해쉬함수를 이용하여 계산하여 생성된 일정한 값을 의미한다: 松嶋隆弘 渡邊凉介『仮想通貨とめぐる法律・税務・会計』(ぎょうせい, 2018) 35頁。연산속도의 의미로 이해하기도 한다.

10) Nakamoto, *Id,* p1

11) Nakamoto, *supra*, p2

"일반적인 해결책은 신용이 있는 중앙기관 혹은 조폐기관을 매개로 하여 전체 거래를 감시시키는 것이지만 각 거래시마다 코인이 조폐기관으로 돌아갔다가 다시 새로운 코인이 발행되고 조폐기관이 직접 발행한 코인만이 이중사용되지 않았다고 믿게 되는데, 이러한 해결방법은 전체 금전 체계(money system)가 조폐기관을 통해서 이루어지지 때문에 은행과 마찬가지로 조폐기관을 운영하고 있는 기업에게 금융시스템 전체의 운명이 좌우된다.

필요한 것은 코인의 수취인이, 여태까지의 소유자들이 이중서명하지 않은 점을 알 수 있는 방법이며, 이러한 목적 하에서는 최초의 거래만이 논점이기 때문에 모든 거래에 대해 검토하지는 않기로 한다. 거래가 없었다는 점을 명확하게 하기 위해서는 전체 거래를 알 필요가 있다. 조폐기관 모델에서는 조폐기관이 전체 거래를 알고 있고 가장 먼저 도래한 거래를 파악하고 있다. 제3자 기관 없이 이를 행하기 위해서는 거래가 공개되고 참가자들이 받은 순번의 유일한 거래이력에 합의할 수 있는 시스템이 필요하다. 수취인은 거래시마다 대다수의 노드(node)들이 그 코인이 처음으로 사용되었음에 동의한다는 증명이 필요하다.[12)]"

그러나 이와 관련하여, 나카모토 사토시가 구상한 대로 향후 이중사용(지급)의 문제가 일체 발생하지 않는다고 단언할 수 있는지는 의문이다.

다만 이러한 시스템을 통해 확인할 수 있는 것은 거래의 존재 사실 및 거래 이력에 대한 것으로 보이는바, 거래의 최초 출발점이 되는 "권리" 자체에 대한 것, 즉 이 권리가 어떠한 것인지, 또 권리 자체가 진실한 것인지, 권리의 내용은 무엇인지 등등의 권리의 내용에 대한 설정 자체는 어떻게 구성해야 할지 의문이 생긴다.

참고로 부동산, 동산, 채권, 주식 등 대부분의 재산권 영역에서 이중양도의 문제가 발생하고 있으며 이를 해결하기 위한 법리가 전개되고 있다. 예컨대 부동산의 이중양도를 살펴보자. 일반적으로 우리 판례는 오랫동안 부동산 매도인이 중도금을 지급받은 이후 목적물을 이중으로 매도한 경우 매도인의 배임행위에 해당하며 제2매수인이 적극 가담하여 이루어진 것이라면 그 토지의 2중 매매는 사회정의관념에 위배된 반사회적인 법률행위로서 무효라고 보았다(다만 이 경우 제2매수인이 단순히 매도인의 매도사실을 알았다는 것만으로는 무효가 되지 않는다).[13)] 물론 이에 대해 매도인의 계약 자유를 과도하게 제한하며 민사책임의 과도한 형사화라는 비난이 있어 최근까지도 논란이 많았으나, 여전히 대법원은 2018년 5월 17일 전원합의체판결을 통해 부동산 매도인인 피고인이 제1매수인 등과 매매계약을 체결하고 제1매수인 등으로부터 계약금과 중도금을 지급받은 후 매매목적물인 부동산을 제3자등(제2매수인)에게 이중으로 매도하고 소유권이전등기를 마쳐 준 사안에서 부동산매도인의 이러한 행위는 제1매수인 등과의 신임관계를 저버리는 임무위배행위로서 배임죄가 성립한다는 입장임을 밝혔다(다수의견).[14)]

---

12) Nakamoto, *supra,* p 2

13) 1994. 3. 11. 선고 93다55289 판결; 대법원 1981. 1. 13. 선고 830다1034 판결.

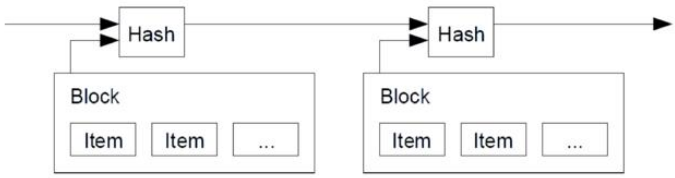
14) 대법원 2018. 5. 17. 선고 2017도4027 전원합의체판결. 다만 위 전원합의체판결의 다수의견에 대해서는,

그러나 이러한 비트코인, 블록체인 기술과 관련하여, 법적 논의를 전개하기 위해서는 먼저 그 대상의 법적 성질이 무엇인지가 규명되어야 비로소 이후의법리를 전개할 수 있으므로 그 법적 성질을 분석하는 작업이 가장 선결적으로 해결되어야 한다고 본다.

3. 타임스탬프 서버(Timestamp Server)

또한 위 논문에서는 타임스탬프 서버라는 해결방법을 제안하고 있다.

타임스탬프 서버란 타임스탬프되는 복수의 아이템을 포함한 데이터 블록을 해쉬로서 처리하고 그 해쉬를 신문이나 Usenet 포스트[2-5]처럼 광범위하게 공개한다. 타임스탬프에 의하여 그 데이터가 타임스탬프된 시점에 해쉬가 되기 위해 존재하였음이 증명된다. 각 타임스탬프는 그 해위 중에 직전 타임스탬프를 포함해 감으로써 체인을 형성하고 타임스탬프가 증가할 때마다 이전 타임스탬프를 강화해 간다. (이하 위 논문에 인용된 그림을 인용한다).



이와 같이 내트워크가 분산된 타임스탬프 서버(timestamp server)가 같이 작동하여 코인을 소비한 첫 번째 거래(transaction)를 기록하, 이는 확산되기는 쉽지만 억제하기는 어려운 정보의 본성을 이용한 것이다.[15]

4. 작업증명(Proof of Work)

(1) 컨센서스 (합의) 알고리즘

또한 나카모토의 논문에 의하면 P2P 베이스로 분산형 서버를 실행하기 위해 컨센서스(합의) 알고리즘으로서 작업증명(proof of work)을 제안하고 있다.

만약 네트워크 내 데이터가 불확실하다면 그 가상통화의 가치는 제로라 할 것이므로 바로

일방 당사자가 상대방에게 계약의 내용에 따른 의무를 성실하게 이행하고, 그로 인해 상대방은 계약상 권리의 만족이라는 이익을 얻는 관계에 있더라도 그 의무의 이행이 위와 같은 의미의 '타인의 사무'에 해당하지 않고 '자기의 사무'에 불과하여 배임죄 성립을 부정한 반대의견이 있다(대법관 김창석, 대법관 김신, 대법관 조희대, 대법관 권순일, 대법관 박정화의 반대의견).

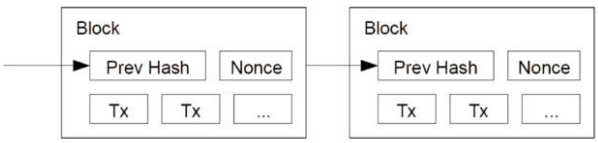
15) 따라서 이로 인한 결과로서, 단일실패지점 (single point of failure: 시스템 전체를 다운시키는 하나의 고장 요소)이 없는 분산화된 시스템을 구축하게 되며, 이중지불을 확인하기 위한 P2P 네트워크의 도움으로 사용자들은 그들의 돈을 소유하고 다른 사람과 곧바로 거래하기 위해 암호 키(crypto keys)를 보유한다. 이상의 내용은 나카모토 사토시가 2009년 2월 11일 P2P foundation에 작성한 글에 소개되어 있다("Bitcoin open source implementation of P2P currency" Posted by Satoshi Nakamoto on February 11, 2009 at 22:27)

합의 알고리즘이란 이러한 블록체인 합의 알고리즘을 통해 블록을 생성할 때 특정한 방식으로 데이터의 무결성, 즉 공유하는 데이터의 정당성을 보증하고 달리 해석될 여지가 없도록 하나의 뜻으로 확정하는 체계를 뜻한다. 예컨대 비트코인은 일정한 시간에 일어난 거래(transaction)을 이전 블록을 참조하여 검증하고 새로운 블록에 담아 생성한 후 51% 이상의 합의를 얻게 되면 기존 장부에 연결하게 되는바, 이와 같이 절대적인 하나의 장부가 존재함으로써 데이터의 무결성이 유지되는 것이다.

이러한 합의 알고리즘을 통해 분산된 환경 하에서 복수의 노드 간에 단일한 결과를 합의를 형성함에 있어서 참가한 관계자가 악의를 가지고 데이터를 조작, 소거, 부인하는 등으로 완결성이 손상되어 버릴 리스크(이것을 '비잔티움장애'라 한다)를 해결한다.[16]

이와 같이 프로세스를 효율화하고 블록체인 콘텐츠를 통제하려는 범죄적 시도를 방지하기 위한 합의 알고리즘에는 크게 두 가지가 있다.

첫째, 나카모토의 논문에서 제안하고 있는, 작업증명(proof of work) 방식이다. 이는 많은 계산량이 필요한 문제를 최초로 풀어낸 자(miner 혹은 채굴자)가 블록을 형성할 수 있는 구조이다. 비트코인의 경우 각각의 블록에 대해 예컨대 SHA-256[17]과 같은 암호학적 해쉬함수는 해쉬값에서 원 데이터를 역산하는 것이 곤란하도록 설계되어 있어 조건을 충족한 nounce의 값을 찾으려면 P2P 네트워크 상에 있는 컴퓨터들이 CPU능력을 소모하여 매우 복잡한 암호화기반 등식을 풀어야만 블록체인 원장에 새로운 데이터를 더할 수 있도록 하는 알고리즘이다. 가장 빨리 등식을 풀어낸 컴퓨터 노드들은 디지털코인을 보상으로 받게 된다. 이러한 작업증명을 통해 가상통화를 수취하는 방식을 흔히 '채굴(mining)'이라 한다(이하 위 논문에서 인용된 그림을 인용한다).



이에 대해 최근에는 지분증명(proof of stake: PoS) 방식이 등장하고 있다. 이는 '자산량(stake)'를 보다 많이 소유한 승인자가 우선적으로 블록을 만들 수 있게 되는 방식이다. 즉 가장 많은 디지털코인을 가진 사람(가장 지분이 큰 사람)이 가상통화 혹은 블록체인 원장을 관리할 수 있게 된다. 작업증명(PoW)에서는 블록 작성에 복잡한 등식을 풀어야 하므로 시간이 걸림과 동시에 전기료와 기자재 취득 비용이 발생하며, 높은 CPU가 있는 제3자에 의해 네트워크가 편취될 우려도 제기되는 반면, 지분증명(PoS)방식의 경우 스스로 자산 가치를 낮추는 일은 없을 것으로 보기 때문에 발행된 전체 자산량에 대한 보유자산비율(즉 지분비율)에 의하여 블록작성의 우선도가 결정되는 방식이다.[18] 최근에는 자

16) 渡邊凉介, 전게서, 37頁。

17) SHA-256 (Secure Hash Algorithm 256-bit)는 암호학적 해쉬함수의 하나로서, 미국 국가안전보장국(NSA)이 설계하여 2001년 미국 국립표준기술연구소 (NIST)가 표준으로 채택했다.

산을 보유하는 자가 이를 이용하지 않고 저장해둘 우려가 있어 블록작성의 우선도를 자산량 및 거래의 크기를 바탕으로 중요도를 산출하여 반영하고자 하는, 이른바 중요도 증명(proof of importance: PoI)도 나오고 있는 등 관련 기술은 나날이 혁신되고 있다.

(2) 작업증명에 관한 나카모토의 구상

이러한 작업증명(PoW)에 대한 나카모토의 구상을 이하 살펴본다:

"이러한 작업증명은 또한 다수결로 의사결정을 할 때 대표자를 선정하는 문제를 해결해 준다. 만약 1 IP주소당 1표라고 한다면(one-IP-address-one-vote) 많은 IP주소를 취득할 수 있는 자는 누구라도 시스템을 전복시킬 수 있다. 작업증명은 원칙적으로 1CPU 당 1표이다. 다수에 의한 의사결정은 가장 많은 작업증명의 노력이 투입된 것을 나타내는, 가장 긴 체인에 의해 대표된다. CPU파워의 과반수가 양심적인 노드에 의해 통제된다면, 가장 양심적인 체인은 다른 어느 체인보다도 빨리 성장할 것이다. 과거의 데이터 블록을 수정하기 위해서는 공격자는 그 블록의 작업증명 뿐 아니라 그 후 이어지는 후속 작업증명도 수정하고 나아가 양심적인 체인에 따라붙고 이를 능가해야 한다. 더 느린 속도의 공격자가 양심적인 체인을 따라잡을 가능성은 후속 블록이 추가될 때마다 지수함수적으로 감소한다는 점을 뒤에서 입증하기로 한다.

가속하는 하드웨어스피트와 장기적으로 변동하는 이익에 대응하기 위해 작업증명 산출의 난이도는 1시간마다 블록 수를 이정한 평균치를 유지하는 것을 목표로 하는 평균이동에 의해 결정된다. 블록산출 속도가 빠를수록 난이도가 증가한다."[19]

5. 네트워크(Network)

나카모토가 생각한 네트워크 실행 순서는 다음과 같다:[20]

1. 새로운 거래는 전체 노드들에게 송신된다.
2. 각 노드가 새로운 거래를 블록에 반영한다.
3. 각 노드가 그 블록에 작업증명을 산출한다.
4. 작업증명을 하는 대로 각 노드는 그것을 전체 노드에게 알려준다.
5. 노드는 블록에 포함된 모든 거래가 유효하고 이전에는 사용되지 않은 경우에만 이를 승인한다.
6. 노드는 승인된 블록의 해쉬를 직전 해위로서 사용하고, 체인의 다음 블록 작성을 개시함으로써 블록 승인을 표시한다.

---

18) 渡邊凉介, 전게서, 37頁。
19) Nakamoto, *supra,* p 3.
20) Nakamoto, *supra,* p 3.

이와 관련하여, 노드는 항상 가장 긴 체인을 정확하다고 판단하고 나아가 여기에 블록을 연장하고자 한다.

그렇다면 만약 두 노드가 동시에 다른 2개의 패턴의 블록을 다음 블록으로서 고지한 경우가 문제될 수 있다. 이 점에 대해 나카모토의 논문에서는, "이 경우 노드에 의해 수신의 순번이 뒤바뀔 가능성이 생기는바, 만약 노드가 최초 수신한 쪽의 블록을 처리하지만 다른 한 쪽의 블록도 보존하고 그 쪽의 체인이 길어질 경우에 대비해 둔다. 다음 작업증명이 발견되고 어느 쪽인지 한 쪽의 체인이 길어진 경우 그 쪽이 옳은 체인이라고 인식하고 다른 쪽 체인에 있던 노드는 보다 긴 체인으로 갈아탄다" 고 설명하고 있다.

그리고 나카모토의 설명에 의하면 새로운 거래의 고지(broadcast)는 반드시 모든 노드에게 이루어지지 않아도 되며, 고지가 많은 노드(*필자 주: 논문에서는 단순히 'many' 라고만 되어 있으나 비교우위의 면에서 더 많다는 의미로 이해된다)에게 수신되는 한 블록에 반영할 수 있다. 블록 고지도 또한 메시지 누락을 참을 수 있다. 노드가 블록을 수신하지 않은 경우, 다음 블록을 수신할 때에 그것을 요구하여 한 개를 놓쳤음을 인식하게 된다고 본다.[21]

6. 인센티브(Incentive)

나카모토가 구상한 설계대로라면 비잔티움장애를 방지하기 위해 합의 알고리즘으로서 작업증명이 필요하게 되고, 작업증명이 채택됨으로 인하여 채굴자들에게는 막대한 계산량과 더불어 컴퓨터 작업으로 인한 전기료,기자재 비용 등이 발생한다. 따라서 이러한 많은 계산량에도 불구하고 필요한 문제를 풀도록 하게 하기 위해서, 다시 말하면 비용의 부담을 상회하는 인센티브를 위해 모종의 이익을 부여할 필요성이 있다.

이에 나카모토 역시 코인이 블록작성자의 것으로 귀속되게 함으로써 채굴의 인센티브를 고취시키고 있다:

> "관례에 의해 블록 내 최초 거래는 새로운 코인을 시작하는 특별한 거래이고, 그 코인은 블록작성자의 것이 된다. 이것은 노드에게 네트워크를 지지하는 인센티브가 됨과 동시에 코인을 발행하는 중앙기관 부재에도 최초 코인을 배포하는 방법으로서 기능한다. 새로운 코인을 일정량 안정적으로 추가해 가는 것은 금광의 노동자가 금을 채굴하여 금의 유동량을 증가시키는 것과 유사하다. 우리의 경우에는 이것이 CPU 시간과 전력이다.
>
> 인센티브는 거래수수료에 의해서도 얻을 수 있다. 만약 어느 거래에서 산출되는 가치가 산입되는 가치보다 적은 경우 그 차이는 거래수수료로서 그 거래를 포함한 블록의 인센티브에 가산된다.(중간 생략)
>
> 인센티브는 노드가 계속 양심적으로 있을 수 있도록 해준다. 만약 탐욕스러운 공격자

21) Nakamoto, *supra,* p 4.

가 양심적인 노드의 합계를 상회하는 CPU파워를 이용할 수 있다면 그는 다른 양심적인 노드로부터 자신이 지급한 금액을 훔쳐서 다시 빼앗든지, 아니면 새로운 코인을 만들든지의 선택을 해야만 할 것이다. 그는 자신의 자산가치와 이를 지탱하는 시스템을 손상하는 것보다는 규칙에 따라 행동하고 다른 모든 노드를 합친 것보다는 많은 새로운 코인을 만드는 것이 자신에게 더 유리하다는 것을 알아야만 한다."[22)]

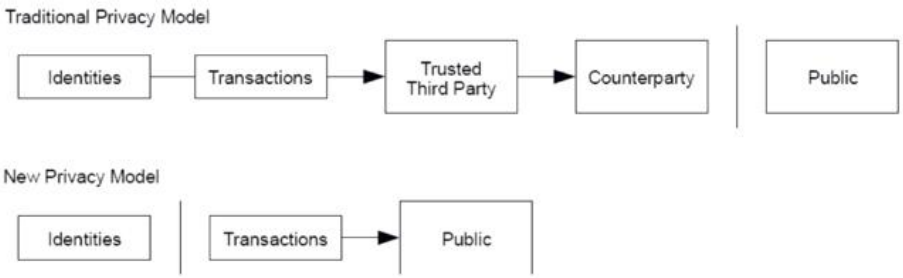
7. 프라이버시(Privacy)

최근의 개인정보보호의 흐름에 비추어 볼 때 비트코인의 거래와 관련해서도 프라이버시의 문제가 매우 중요하다. 거래 관련 모든 데이터를 공개하는 분산원장 시스템을 적용하게 되면 개인정보보호 내지는 침해의 우려가 있기 때문이다.

이와 관련하여 나카모토 사토시는 10번째 항목으로서 프라이버시 보호 문제를 전통적인 뱅킹 시스템과 비교하여 다음과 같이 구상하고 있다(이하 위 논문에서 인용된 그림도 아래에서 함께 인용한다).

"전통적인 은행 모델은 정보에 대한 접근을 관련된 당사자와 신뢰받는 제3자 기관에 한정함으로써 일정한 수준의 프라이버시를 달성하고 있다. 모든 거래를 공개적으로 선언할 필요성이 있기 때문에 이 경우에는 위 방법을 사용할 수 없지만, 정보의 흐름을 다른 곳에서 분석(break)-퍼블릭키를 익명으로 유지-함으로써 프라이버시는 여전히 유지될 수 있다. 대중은 누가 누구에게 보냈는지를 볼 수 있지만, 그 거래와 링크된 정보는 공개되지 않는다. 이는 개별 거래의 시간이나 사이즈, "테이프"는 공개되지만 구체적으로 당사자는 공개되지 않는, 증권거래소에서 제공되는 정보의 수준과 비슷하다.

추가적인 방화벽(firewall)으로서 일반 소유자(common owner)에게 링크되는 것을 방지하기 위해 각 거래마다 새로운 키 페어가 사용되어야만 한다. 복수의 입력(in-put)이 있는 경우 약간의 링크는 여전히 불가피하고, 필연적으로 동일한 소유자에 의한 입력임이 밝혀질 수 밖에 없다. (이 때의) 리스크는 만약 그 키의 소유자가 밝혀진다면 그 링크에 의해 동일한 소유자에게 속하는 다른 거래도 노출될 수 있다는 것이다."



22) Nakamoto, *supra,* p 4.

8. 나카모토 사토시 논문의 결론

그렇다면 나카모토 사토시는 이 논문에서 어떠한 결론을 제시하고 있는가를 살펴본다.

이 논문을 통해 제시하고자 한 것은 바로 개방형, 탈중앙화의 '신용에 의존하지 않는 전자거래 시스템' (a system for electronic transactions without relying on trust)이었다.

위 논문에서는, 전자서명으로 만들어진 코인(coin)이라는 통상의 틀(framework)를 시작하였고, 이는 소유권의 강력한 지배를 받는 것으로서, 이중사용문제를 방지하는 데에 불완전하다고 밝히면서, 그에 대한 해결수단으로서, 작업증명을 사용하여 거래들의 이력을 공개하여 기록하는 P2P(peer-to-peer) 네트워크를 제안하고 있는 것이다. 이러한 네트워크는 정직한 노드가 CPU파워의 과반수를 통제하는 한 공개된 거래이력을 공격자가 변경(변조)하려는 공격자를 컴퓨터적으로 신속하게 무력화할 것으로 보았다.[23] 그 이유로 이 논문에서는 "네크워크는 복잡한 구조가 아니라 단순한 것으로서 견고할 것이며, 모든 노드는 동시에 작동하지만 협조성은 거의 없다"는 점을 들고 있다.[24]

또한 이 논문에서는 "특정 장소에서 메시지가 전송되는 것이 아니고 최선노력원칙하에서 전달되는 것만으로 충분하므로 노드들은 특정될 필요가 없다. 노드들은 그들이 이탈한 동안의 작업증명 체인을 그 동안의 거래 증명으로서 승인함으로써 그 의사에 따라 이탈하거나 접속할 수 있다. 노드들은 블록을 연장함으로서 유효한 블록으로 승인하였음을 표시하고, 이러한 처리를 거부함으로써 무효인 블록은 거절하여 CPU파워를 사용하여 의사를 표명한다(*필자 주: 여기에서 투표한다는 의미의 'vote'를 사용하고 있다). 필요한 규정(rule)과 인센티브는 이러한 합의의 메카니즘으로 실행될 수 있다"고 보아, 기존의 중앙기관에 의한 통제가 아닌 합의의 메카니즘으로 작동하는 시스템을 제안하고 있다.[25]

9. 소결

이 논문 이후 현재까지 다양한 형태의 블록체인 네트워크들이 경쟁 중인바 네트워크 참가자(노드)의 성격에 따라 구분해보면 통상적으로 ① 퍼블릭 블록체인(Public Blockchain), ② 프라이빗 블록체인(Private Blockchain), ③ 하이브리드 또는 컨소시엄 블록체인(Hybrid or Consortium Blockchain) 등이 있다.

이 중 이 논문에서 구상한 것은 이른바 1세대라 할 수 있는 "퍼블릭 블록체인"에 속한다고 할 수 있다. 퍼블릭 블록체인 네트워크에서는 누구든지 허가 없이 블록체인의 데이터를 읽고-쓰고-검증할 수 있는 구조로서 누구나 운영의 주체가 될 수 있고, 참여자가 많을수록 코인을 위변조할 수 없다. 그러나 퍼블릭 블록체인 형태는 개방성이라는 장점이 오히려 악용되어 범죄 혹은 자금세탁과 같은 행위에 이용되기도 하였다. 이에 전세계적으로 이른바 가상자산을 이용한 자금세탁, 테러자금조달에 대한 대응방안이 진지하게 논의되고 있다.[26]

---

23) Nakamoto, *supra,* p 8.
24) Nakamoto, *supra,* p 8.
25) Nakamoto, *supra,* p 8.

이에 대해 2세대라 할 수 있는, “프라이빗 블록체인”이 있다. 현 단계에서 프라이빗 블록체인 기술은 퍼블릭 블록체인이 가진 문제점을 없애고, 블록체인의 장점을 가지고자 하는 2세대 기술로 파악할 수 있다. 개방성으로 인한 리스크를 최소화하기 위해 하나의 중앙기관이 모든권한을 가지게 된다. 그러나 이 경우 그 중앙의 특정 기관이 인증된 기관으로서 서비스를 제공한다면, 직접 거래 증명이 가능하여 채굴자를 둘 필요가 없어 전통적 방식과의 차이점이 없어진다는 지적이 가능하다. 따라서 퍼블릭과 프라이빗의 혼합형태로서 하이브리드 또는 컨소시엄 블록체인이 논의되고 있다.

그러나 기술은 앞으로 계속 발전되고 새로운 기술이 등장할 것이므로 기술의 구체적인 부분에 매몰되기보다는 이러한 것들의 법적 성격을 먼저 규명하고, 관련하여 발생하였거나, 아니면 발생할 수 있는 법적 문제점을 검토하여 법리나 해석론을 제시하는 것이야말로 법학에서 관심을 가져야 할 부분이라 할 수 있다.

III. 시론적 문제제기와 법적 고찰

: Don’t trust, verify[27]

1. 일반적 개념으로서의 정의(定義)

(1) 가상통화/암호화자산

먼저, 그 법적 성질을 규명하는 것이 법학적 관점에서 볼 때 가장 시급한 과제라 할 수 있다. 많은 문제들을 해결하기 위해서도 법적 성질을 검토할 필요가 있다.

우선 비트코인을 포함하여 이러한 성질의 코인들을 통칭하는 용어로서 업계, 학계 등에서는 ‘가상화폐,’ ‘가상통화(virtual-currency),’ ‘암호화폐(cryptocurrency)’ 등이 혼재되어 사용되는 등 그 용어조차도 아직 통일되지 못하였었다. 그러나 대한민국의 화폐단위인 ‘원’으로 표시되는 원화의 발행권은 한국은행만이 가지므로(한국은행법 제47조), 이러한 법정통화체제 하에서 비트코인을 두고 ‘화폐’ 혹은 ‘통화’라고 부르는 것은 적절하지 않다. 교환매개 및 가치척도의 수단으로서의 기능을 수행한다고 보기도 어렵고, 금(gold)과 달리 내재적 가치가 유지되는 것도 아니다. 경제적 역할의 원만한 수행은 안정된 구매력을 전제로 한 일반적 수용성(受容性)에 있다.[28]

다만 2018년 6월 24일부터 29일에 걸쳐 개최된 제29기 제3차 자금세탁방지기구(FATF) 총회에서는 적절한 하나의 용어가 결정될 때까지는 가상통화를 “Virtual Currencies/Crypto-Assets(가상통화/암호화자산)”로 두 용어를 병기하여 쓰기로 결정하였다.[29] 조만

---

26) , “제29기 제3자 자금세탁방지기구(FATF)총회 결과” 2018. 7. 2.자 보도자료 참고. http://www.fsc.go.kr/info/ntc_news_view.jsp?menu=7210100&bbsid=BBS0030&no=32561

27) 블록체인 업계의 격언이라 한다(유신재, “로스차일드 사칭 ”ICO 사기“소동”, 코인데스크 편집장 칼럼, 2018. 10. 25.자. 상세한 내용은 www.coindeskkorea.com)

28) 안법영, “금전사법의 법리에 관한 소고- 권리대상으로서 금전의 탈유체화에 관해서”, 법학논집 제34집, 고려대학교 법과대학 법학연구소, 1998, 190면.

간 권고기준과 가이던스가 개정되면 이 부분 용어는 전세계적으로 통일될 것으로 생각된다.
사견이지만 비트코인을 현재 상황에서 가장 정확히 표현한 것은 '**암호화 자산**' 이라 할 것이다. 물론 '암호' 라는 용어를 사용함으로 인해 암호화 기술로 그 범주가 제한되는 문제점이 있고 가까운 미래에 암호화되지 않은 유사한 존재의 것이 출현하게 되면 이 용어를 더 이상 사용할 수 없다는 단점이 있으나[30] 현재로서는 위 용어가 가장 타당하다고 생각된다.

(2) 지급결제수단인지 여부

비트코인은 2011년 초 실크로드 사건을 통해 음성적인 불법거래의 수단으로 이용되었다는 사실이 밝혀지면서 특히 그 화폐에 갈음한 결제수단으로서의 기능에 관심이 높아졌다. 마치 게임머니처럼 어떤 한정된 영역 내에서는 사적인 교환수단으로서 기능하고 실제 교환가치를 갖는다고도 볼 수 있지만 앞서 본 바와 같이 법정통화제도 하에서는 화폐 내지는 통화로 보기는 어렵고, 현행처럼 공인된 제3자 기관을 통해 발행되고 인증을 받아야만 통화처럼 사용할 수 있는 전자화폐나 선불지급수단과도 구별된다.
우선 지급결제수단으로 인정받기 위해서는 법적 근거가 필요하나, 우리나라에서는 일본과 달리 지급결제수단임을 명시한 법률이 존재하지 않으므로 가상화폐를 지급결제의 수단으로 볼 수도 없다. 일본의 경우 자금결제법상 가상화폐를 "대가의 변제를 위하여 불특정인에 사용할 수 있으며, 또한 불특정인을 상대방으로 구입 및 매각할 수 있는 재산적 가치"로 규정하고 있으나 그렇다고 하여 가상통화를 법정화폐로서 인정한 것은 아니다. 오히려 자금결제법상 규정을 둔 이후 일본 내에서 자금결제법상 요건을 갖추면서 ICO를 행하는 예는 거의 없어보인다는 시장의 평가도 있다. 한편 금융위원회의 '가상화폐 관련 자금세탁방지 가이드라인'에 따라 가상통화를 매개한 거래가 의심거래의 경우에는 각 은행들이 신고의무를 부담하기는 하나, 이는 의심거래를 감독하기 위한 목적에 불과한 것이고 가상통화를 지급결제수단으로 인정한다는 뜻으로는 해석하기 어렵다.
마찬가지로 미국의 경우 재무부 산하의 FinCEN이 가이드라인을 통해 가상통화를 "일부 환경에서만 통화로 사용되고 진정한 통화의 모든 속성을 가지고 있지는 않은 교환수단으로, 특히 가상화폐는 어떤 법정관할지역에서도 법정화폐로 받아 들여지지 않는 것"이라고 정의하면서 가상화폐 중개기관을 자금세탁방지법상 자금서비스업자에 해당하는 것으로 규정하고 있지만 이러한 FinCEN의 가이드라인 역시 자금세탁방지법 적용을 위해 일종의 '자금' 에 해당한다고 규정한 것일 뿐 지급결제수단이라는 의미로는 해석하기 어렵다.

2. 암호화자산을 둘러싼 법적 검토

(1) 재산적 가치 인정

29) , 위 2018. 7. 2.자 보도자료 2면.
30) 배승욱, "가상통화 법제 구축방안에 관한 연구" 한국외국어대학교 대학원 법학박사학위논문, 2018. 2., 9면.

일응 경제적 가치 있는 이익을 누리는 것을 목적으로 하는 권리를 재산권이라 한다면, 오늘날 거래 현실을 종합하면 비트코인의 경제적 가치 내지는 재산적 가치를 부정하기는 어렵다. 인터넷 포털사이트를 통해 검색해보면 금방 암호화자산의 시세를 검색할 수 있으므로 재산적 가치를 부정한다는 것은 너무나 비현실적이다. 이미 일본의 자금결제법에서는 가상화폐를 "대가의 지급을 위하여 사용될 수 있는 것으로서 재산적 가치가 존재하는 것"임을 인정한 바 있고(제2조), 미국의 상품선물거래위원회(CFTC)에서도 일종의 Commodity 즉, 상품에 해당되는 것으로 보아 선물거래를 허용하고 있다고 한다.

특히 한국원화는 비트코인 거래가 이루어지는 통화 중 엔화, 미국 달러, 유로화 다음으로 세계 4위의 규모를 차지하고 있는 실정이다.[31]

암호통화는 별도의 청산 및 결제 절차를 거치지 않고 교환의 매개물로 제한된 범위 내에서 사용된다는 점에서 통화는 아니지만, 경제적으로 금전과 유사하게 볼 수 있는지 문제될 수 있다.

그러나 이러한 암호통화를 금전으로 보기는 어렵다고 생각한다(사견).

우리 민법 학계의 지배적 견해는 금전은 그 소재성에 주안점을 두어 민법상 유체물로서 동산이라고 본다. 다만 다른 일반 유체동산과 달리 '보통 물건이 가지는 개성을 갖고 있지 않고 가치 그 자체' 또는 '보통 물건이 가지는 개성을 가지지 않고 일정액의 가가치를 표상하는 것이므로 다른 동산과 다른 특수성'이 있어 특수한 동산으로 취급하고 있다.[32] 마찬가지로 T머니와 같은 경우에도 유체물로서의 '카드'가 존재하므로 이 카드 자체의 소유권을 인정하면 될 것이다.

따라서 금전의 특성상 특정한 금전을 반환한다는 것은 무의미하므로 타인의 점유에 돌아간 금전에 대해서는 채권적 반환청구권을 인정하는 것으로 족하다는 견해가 제시되고 있다.[33] 이렇듯 금전을 단지 동산으로 분류한 이유는 그것이 그 소재인 금속이나 종이의 물질적인 유체성을 가진다는 속성에 기인한 것이므로 일부 가치적 기능성은 제한된 범위 내에서 유사할 수는 있지만 암호화자산을 금전과 동일시하기는 어렵다. 다만 제한된 범위 내에서 금전대용적 성격을 가지는 점 자체는 부인하기 어렵다고 생각되는바, '금전대용물'로서의 성격을 인정할 수 있다(사견).

(2) 비트코인과 소유권

암호화자산이 재산적 가치를 가진다는 데에 국내에서 크게 이견은 없으므로, 재산적 가치를 전제로 하여 비트코인에 대한 채굴자 내지는 이를 매입한 자가 갖는 권리의 측면을 생각해보자.

---

31) , "가상통화 관련 거래의 회계처리" 월간공인회계사(2018. 7. 30.), 한국회계기준원(>자료실>기고자료), 2018. 8. 31.http://www.kasb.or.kr/fe/bbs/NR_view.do?bbsCd=1041&bbsSeq=24774

32) 안법영, 앞의 논문, 197면.

33) 예컨대 곽윤직, 민법총칙 (박영사, 1989), 312면 등. 이에 대한 유력한 반론으로서, 안법영, 앞의 논문, 200면-206면.

만약 갑이 비트코인을 가지고 있다고 할 때 단순히 블록체인을 통해 구현되는 분산원장에 기록된 전자적 기록(내지 정보)에 불과한 그 자체와 매개하여 어떠한 권리를 갖는 것으로 볼 것인가는 매우 어려운 문제이다.

특히 우리 민사법체계에서 재산권의 종류로서 물권, 채권, 지식재산권 등이 있는데, 암호화 자산에 대한 권리가 이 중 어디에 속하는지에 대해서는 아직 확립된 이론은 없다.

그럼에도 불구하고 우리는 주위에서 혹은 직접 '비트코인을 샀다(투자했다)' 든가, '내 것' 이라는 표현을 듣고, 사용하고 있는데, 이처럼 비트코인에 대해서도 이른바 '소유권' 을 인정할 수 있을까?

소유권은 법령의 제한 내에서 자유롭게 그 소유한 물건을 사용, 수익, 처분할 수 있는 권리로서, 소유권 등 물권은 바로 물건 기타의 객체를 직접 지배해서 배타적으로 이익을 얻는 권리라 할 수 있다. 여기서 소유권 등 물권의 대상은 법적으로 "물건" 일 것을 요구하고 있으며 민법 제99조는 "본법에서 물건이라 함은 유체물 및 전기 기타 관리할 수 있는 자연력을 말한다" 라고 규정하고 있다. 그리고 부동산이라 '토지 및 그 정착물' 을, 그리고 동산은 '부동산 이외의 물건' 을 뜻하는 것으로서 법률개념을 포섭하고 있다.[34] 그리고 '동산' 등의 경우에도 권리의 객체로서 배타적 지배가 가능할 것을 요건으로 하는 특정성의 원칙을 표방하고 있다고 해석되는바, 대부분의 재산법적 권리는 이러한 물권의 객체로 인식하는 데 그 중점이 놓여 있다. 이와 관련하여 우리 민법은 '동산' 의 개념을 유체물로만 한정한 것이 아니라 '관리할 수 있는 자연력' 을 포함하여 정의하고 있다.[35]

여기서 말하는 '유체물' 이란 액체, 기체 및 고체 등 공간의 일부를 점하고 있는 것이며, 채권이나 저작권 등의 권리 기타 자연력(전기, 열, 빛 등)과 같은 무체물에 대비되는 것이다.[36] 그러나 우리 민법은 유체물뿐만 아니라 무체물도 그 배타적 지배와 관리가 가능하다면 '물건' 의 개념에 포함시켜 거래의 실제적 필요에 상응한 입법태도를 취하고 있다.[37]

그렇다면 기존의 관념에 비추어 분석하면, 비트코인이라는 것 자체는 디지털로 암호화된 코드 내지는 데이터정보에 불과하므로, 유체물은 당연히 아니며, 전기와 같이 배타적으로 지배가능한 자연력(에너지)이라고 보기도 어렵기는 하다.

그러나 민법상 원칙적으로 소유권을 포함한 물권의 객체를 유체물 및 기타 관리가능한 자연력으로 한정한 취지에는 바로 소유권은 객체인 물건에 대한 타인의 이용을 배제할 수 있는 권리이므로 배타적인 지배가능성이 요구된다는 점이므로 여기서의 관리할 수 있는 자연력의 범위를 합목적적으로 해석하여 비트코인 등과 같은 데이터정보도 소유권의 객체가 되는 물건의 범위에 속한다고 해석함이 타당하다(사견).

물론 2015년 8월 5일 동경지방재판소는 '권리의 소유권' 을 승인하는 것이 되어 물권과 채권을 준별하는 일본 민법에 반하는 점과 더불어 (원고가 주장하기를, 법적으로 보호할 재산성이 있다면 유체물로 보아야 한다는 점에 대하여) 법적으로 보호할 가치는 유체물이든,

---

34) , 앞의 논문, 198면.

35) 안법영, 앞의 논문, 199면.

36) 鈴木尊明「ビットコインを客体とする所有 の成立が否定された事例」新 · 判例Watch Vol.19(2016. 10.) 59頁。

37) 안법영, 앞의 논문, 198면.

무체물이든 모두 있으므로 일본 민법 제85조에서의 ‘物(물건)’에 해당하는지 여부의 기준이 될 수 없다는 점을 들어 비트코인에 대한 소유권 성립을 부정한 바 있다.[38]

이처럼 동경지방재판소은 배타적 지배가능성을 부정하였는데, 비트코인의 거래과정의 기본 구조에서 그 논거를 찾았다. 즉 비트코인 거래에서는 보내는 사람과 받는 사람 쌍방의 계좌를 암호화하여 거래하며 그 과정에서 네트워크 상의 불특정다수의 참가자(*필자 주: 노드)가 일정한 계산행위를 하고, 그 거래와 계산행위 모두를 기록한 블록체인이 형성되어 인터넷상 공개되므로, 비트코인 거래는 “송부되는 비트코인을 표상하는 전자적 기록의 송부에 의하여 이루어지는 것이 아니라, 그 실현에는 송부하는 당사자들 이외의 관여가 필요하다”는 점에 주목한 것이다. 그러므로 특정한 참가자가 작성, 관리하는 비트코인 계좌에서의 ‘비트코인 잔고’는 블록체인 상 기록된 같은 address(*필자 주: 계좌)와 관계하는 비트코인의 모든 거래를 차감계산한 결과 산출되는 수량이고, 당해 비트코인 address에 잔고에 상당하는 비트코인 자체를 표상하는 전자적 기록은 존재하지 않는다는 점을 지적하고 있다. 그 결과 동경지방재판소는 위에서 살펴본 바와 같은 기본 거래구조를 볼 때 비트코인 계좌의 관리자가 당해 address에서의 당해 잔고물량의 비트코인을 배타적으로 지배하고 있다고 인정할 수 없다고 본 것이다.

물론 이에 대해 일본 내에서도 비판하는 견해가 적지 않았으며, 비트코인의 채굴행위를 통해 비트코인을 취득하므로 이러한 계산행위는 방대한 계산에 의한 지적 영위(營爲)로서 지적재산권(필자 주: 지식재산권) 이 성립한다는 견해도 제기되었다.[39]

그러나 사견으로서, 앞서 본 바와 같이 이러한 가상공간에서의 생산물 역시 민법상 ‘물건’의 개념 속에 포섭할 수 있다고 본다.

우리 민법은 일본 민법과 달리 관리할 수 있는 자연력 즉 무체물에 대해서까지 법률의 규정에서 명시적으로 포섭가능성을 열어두고 있다. 이 때의 ‘관리할 수 있는 자연력’의 예시로는 대체로 전기, 빛, 열 등을 들고 있으나, 역사적으로 볼 때 전기, 빛, 열에 대한 소유권이라는 개념조차 생소한 시절도 과거에 있었다. 따라서 이른바 제4차 산업혁명시대를 살고 있는 우리들에게 이러한 네트워크상 나의 계정에 보관되어 있는 많은 것들(게임머니, 게임 아이템, SNS상 아바타 등)이 실제로는 데이터정보의 형태로만 존재한다고 하더라도 오프라인이 아닌 온라인의 세계에서는 충분히 관리가능하며 또 배타적으로 지배하고 있다고 볼 여지가 있다. 그러므로 인터넷상 게임머니, 혹은 인터넷 게임상 희귀한 아이템 그리고 SNS에서의 아바타 등도 굳이 그 실체를 기술적으로 분석하면 그저 전자적 기록에 불과하겠지만, 이것들 역시 개인의 계좌에 보관하면서 관리가 가능하다면 충분히 배타적으로 지배가능하다고 보아 소유권을 인정할 수 있다고 생각한다(사견).

이 점과 관련해서는 비록 세법상의 판결이기는 하나, ‘게임머니’도 재산적 가치가 있는 모든 유체물과 무체물을 의미하는 구 부가가치세법상의 ‘재화’에 해당한다는 대법원의 판결이 있다.[40]

---

38) 平成27年8月5日　平成26年(ワ)第33320　ビットコイン引渡等請求事件(判例集未登載)。
39) 土屋雅一「ビットコインと税務」税大ジャーナル23号(2014年)　81−82頁。
40) 대법원 2012. 4. 13. 선고 2011두30281 판결.

또한 한국회계기준원은 2018년 2월 비트코인, 이더리움 등 이른바 가상통화가 기업재무제표에서 '유동자산'으로 분류된다고 판단하였다.

즉 주식회사 등 외부감사의 법률('외감법')의 적용을 받는 기업인 가상통화 취급업소인 빗썸[41]이 제기한 회계기준 질의에 대한 회신으로서 회계기준원이 회계처리 관련 공개초안을 발표하면서, 유동자산은 현금성 자산, 금융자산, 매출채권, 기타 자산으로 구성되고, 가상통화는 환급성이 높은 당좌자산 중 기업의 판단에 따라 분류를 지정하되, 기업이 가상통화를 1년 이상 보유하면 기타 자산, 1년 내에 처분할 경우에는 기타 유동자산으로 분류하면 된다는 입장을 취하였다. 다만 가상통화의 가치는 가격변동성이 크기 때문에 취득원가보다는 시장 가치를 반영하게 된다. 그러나 이것 역시 국제회계기준(IFRS)에 따른 것이 아니라, 임시적인 방편에 불과하므로 향후 전개되는 논의에 관심을 가지고 주목할 필요가 있다.

(3) 비트코인과 채권성 여부

만약 위 (2)의 논의와 관련하여, 암호화자산을 민법상 물건으로 보기 어렵다는 입장을 취할 경우, 이것이 디지털로 암호화된 코드에 지나지 않으나, 환금성(換金性)을 가지고, 재산 혹은 재산적 가치를 가지는 이상, 민법 373조(금전으로 가액을 산정할 수 없는 것이라도 채권의 목적으로 할 수 있다)를 근거로 암호화자산을 목적물로 한 작위, 부작위 급무의무로 구성하여 일종의 채권의 목적이 된다는 입장도 있을 수 있다.[42]

채권의 목적이란 '채권자가 채무자에 대하여 일정한 급부행위를 구하는 것'인데, 가액을 산정할 수 없는 급부를 목적으로 하는 채권도 그 효력에 있어서는 보통의 채권과 다를 바가 없고 채무자의 이행이 없으면 채권자는 이행판결을 구할 수 있고 그 판결에 의하여 강제집행을 할 수 있으며, 강제집행과 함께 그것에 갈음하여 손해배상을 청구할 수 있으므로(단 민법 제394조에 의해 손해배상은 금전에 의하는 것이 원칙) 가상화폐를 목적물로 한 작위, 부작위 급부의무로 구성하여 재산권을 가진 채권의 목적이 된다고 본다.

그러나 현실에서 비트코인을 채권집행의 방법으로 다루지 못하는 것은 현행법상 '채권'의 개념 속에 과연 '전자지갑의 주인이 비트코인의 네트워크에 대해 송금지시를 내릴 권리'까지 포섭할 수 있는지 등의 여러 쟁점이 명확하지 않기 때문이다.[43]

(4) 금융투자상품 혹은 증권인지 여부

자본시장과 금융투자업에 관한 법률(이하 "자본시장법")에서는 금융투자상품을 '이익을 얻거나 손실을 회피할 목적으로 현재 또는 장래의 특정(특정) 시점에 금전, 그 밖의 재산적 가치가 있는 것(이하 "금전등"이라 한다)을 지급하기로 약정함으로써 취득하는 권리로서,

41) 이외에도 코빗, 코인원이 외감법의 적용을 받는다. 12월 결산법인일 경우 외감법에 따라 익년 3월말까지 감사보고서를 제출해야 한다.

42) 윤배경, "가상화폐에 대한 민사강제집행", 2018. 4. 26.자 법률신문 제11면.

43) 전승재·권헌영, "비트코인에 대한 민사상 강제집행 방안 – 암호화폐의 제도권 편입 필요성을 중심으로-" 정보법학 제22권 제1호 (2018), 87면.

그 권리를 취득하기 위하여 지급하였거나 지급하여야 할 금전 등의 총액(판매수수료 등 대통령령으로 정하는 금액을 제외한다)이 그 권리로부터 회수하였거나 회수할 수 있는 금전등의 총액(해지수수료 등 대통령령으로 정하는 금액을 포함한다)을 초과하게 될 위험(이하 "투자성"이라 한다)이 있는 것' 을 의미한다(동법 제3조 제1항). 자본시장법상 금융투자상품은 크게 증권과 파생상품으로 구분되며(동법 제3조 제2항), 증권의 경우 채무증권, 지분증권, 수익증권, 투자계약증권, 파생결합증권, 증권예탁증권 등 6가지 유형으로 규정하고 있다(동법 제4조 제2항). 또 우리가 흔히 주식 투자와 유사하게 느끼면서 이른바 '비트코인에 투자한다' 는 식의 표현을 종종 접하게 되는데, 자본시장법상 주식은 증권에 해당하며, 증권이란 '내국인 또는 외국인이 발행한 금융투자상품으로서 투자자가 취득과 동시에 지급한 금전등 외에 어떠한 명목으로든지 추가로 지급의무(투자자가 기초자산에 대한 매매를 성립시킬 수 있는 권리를 행사하게 됨으로써 부담하게 되는 지급의무를 제외한다)를 부담하지 아니하는 것' 을 의미한다(동법 제4조 제1항) 따라서 주식처럼 증권은 발행자(발행회사)를 전제로 하는 반면, 퍼블릭 블록체인을 통해서 채굴되는 비트코인의 경우 특정 발행자가 있는 것이 아니어서 증권이라고 보기는 어렵다고 생각한다.

물론 가상통화 그 자체의 증권성 인정 여부는 ICO(Initial Coin Offering: 최초코인발행)를 통해 발행된 토큰 등을 증권으로 볼 수 있느냐에 대한 논의와는 또 다른 측면이다. ICO는 이른바 IPO(Initial Public Offering: 기업공개)에서 유래한 용어인데,기업공개의 경우 대상이 되는 것이 회사의 주식이고 주식을 중심으로 한 법률관계는 법률적으로도 정비가 되어 있는 반면, ICO의 경우 발행되는 코인, 토큰의 법적 성격이 무엇인지에 대해 법적으로 아직 정비되지 못한 상태이다.[44] ICO에 의해 자금을 조달한 사례로서 텔레그램, 카카오, 라인, 라쿠텐 등의 사례가 있다.[45] 다만 ICO시에는 투자계약증권으로서 증권성을 인정할 여지도 있고 또 실제로 미국에서는 ICO에 대해 증권발행에 따르는 규제를 부과하고 있다(ICO에 관한 깊은 논의는 이 글에서는 생략한다).[46]

그렇다면 파생상품으로 볼 여지는 없는지가 문제될 수 있으나, 가상통화 그 자체로 어떤 기초자산의 가치를 평가하여 장래의 채권계약을 성립시키는 효력을 갖는 계약은 아니므로 자본시장법에서 규정하고 있는 파생상품이라고도 보기 어렵다.

---

44) , "최근 디지털 가상화폐 거래의 법적 쟁점과 운용방안 – 비트코인 거래를 위주로," 증권법연구 제15권 제3호 (2014) 참조.

45) 이근우, "텔레그램, 카카오, 라인, 라쿠텐, 그리고 ICO" 법률신문 2018. 4. 9.자 오피니언 기사
자세한 내용은, https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=141949

46) 금융위원회는 2018년 10월 24일 보도자료를 통해, 일명 "가상통화펀드" 관련 투자자 유의사항을 밝히면서, 최근 일부 업체가 불특정 다수의 투자자로부터 모은 가상통화를 ICO 및 기존 가상통화에 운용하고 만기에 그 수익을 배분하는 형태의 상품을 판매하면서, 여기에 "펀드(일명 가상통화펀드)"라고 지칭하고 있으나 자본시장법에 따른 펀드가 아니며 자본시장법 위반 소지가 있어 투자에 각별히 유의할 것을 명시하고 있다(금융위원회, "일명 "가상통화펀드" 관련 투자자 유의사항" 2018. 10.24. 보도참고자료. 원래 자본시장법상 모든 펀드는 금융감독원에 등록하여야 하고 공모펀드는 증권신고서를 제출하여야 하며, 펀드를 운용하는 자산운용사와 이를 판매하는 펀드판매회사는 요건을 갖추어 금융위원회의 인가를 받아야 하고 투자자 보호를 위해 건전성 규제와 영업행위 규제를 준수하여야 하는 반면, 이러한 가상통화펀드는 집합투자업의 외형구조를 갖추고 펀드라는 명칭을 사용하고 있으나 자본시장법에 따라 설정된 펀드가 아니어서 자본시장법 위반의 소지가 있다. http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=&sword=&r_url=&menu=7210100&no=32742.

IV. 결: 새로운 법적 논의의 시작

이미 현실적으로는 비트코인에 대한 민사상 강제집행을 어떤 방식으로 할 것인지, 형사상 범죄수익으로서 몰수할 수 있는지 여부가 이미 문제되었다.

민사집행법의 편제는 먼저 실현될 권리가 금전인지 여부에 따라 금전집행과 비금전집행으로 분류한다. 금전집행은 집행대상의 종류에 따라 부동산에 대한 집행, 선박 등에 대한 집행, 동산에 대한 집행으로 구분되고, 동산집행은 다시 '유체동산에 대한 금전집행', '채권과 그 밖의 재산권에 대한 금전집행'으로 구분된다. 비금전집행은 물건의 인도를 구하는 청구권의 집행과 작위(대체적, 부대체적 작위), 부작위, 의사표시를 구하는 청구권의 집행으로 나뉜다. 이처럼 집행의 대상이 되는 재산의 종류에 따라 동산집행과 부동산집행으로 나뒤는데, 동산집행에는 민법과 달리 채권과 그 밖의 재산권도 포함된다.

금전집행의 경우 그 강제집행은 동산집행 중 채권과 그 밖의 재산권에 대한 집행으로 분류되는바 금전집행은 ㉠ 압류, ㉡ 현금화, ㉢ 배당의 절차를 거친다. 비금전집행의 경우(예컨대 당사자 사이에 특정일자에 채굴한 비트코인 등 특정 가상통화의 수수가 직접적인 목적일 경우)라면 대상물인 암호화자산은 특정한 동산이나 대체물의 일정한 수량이 아니므로 동산인도청구의 집행(민사집행법 제257조)의 대상이 될 수 없고 상대방의 협력을 요하는 비대체적 작위채권의 집행으로 분류할 가능성이 있는바, 이 경우에는 간접강제의 방식(민사집행법 제261조)을 취하게 된다고 보고 있다.[47]

따라서 민사상 강제집행을 어떠한 방식으로 할 것인지조차 고민스러운 부분이다. 특히 종국적으로는 현금화가 필요한데 속칭 거래소라는 취급업체를 통해 이를 매각할 수 있다고 보기 위해 먼저 이 점에 대한 법적 근거를 둘 필요가 있는바 시급히 법제를 정비할 필요가 있다. 아직 정부 당국에서 가상통화 관련된 법제조차 정비하지 않은 상황이어서 거래소를 통한 매각에 의한 현금화 방식을 허용하기에는 시기상조가 아닐까 싶다.

나아가 형사적으로도 많은 문제를 야기하고 있는데, 특히 비트코인이 범죄수익은닉의 규제 및 처벌 등에 관한 법률에서 규정하고 있는 '재산'에 해당하여 몰수할 수 있는지 여부가 크게 다투어졌고 이 점에 대해, 2018년 대법원은 비트코인도 일종의 무형 재산으로 보아 그 몰수를 허용하였다.[48]

한편 앞서 본 동경지방재판소의 위 판결로 인해 가상통화 전반에 대한 규제가 논란이 되자

---

47) , 앞의 글, 11면. 단 이 때의 문제는 압류명령을 통하여 채무자가 가상화폐 거래에 필요한 지갑 및 키파일(key file) 등에 대한 처분금지까지 가능한지 여부다. 이론적으로, 가상화폐 보유자가 블록체인을 통하여 P2P 방식으로 가상화폐를 제3자에게 이전하는 것을 거래소가 관여할 수 없기 때문이다(거래소 이용약관은 이를 '자율거래'라고 하는데, 가상화폐를 전달하는 과정에서 거래소의 참여 없이 판매자와 구매자가 서로 지정한 방법을 통해 거래하는 것으로 정의하고 있다). 현재로서는 거래소가 압류명령에 의하여 채무자의 가상화폐 거래 정보에 대한 접근이나 처분을 금지, 정지하여야 할 법적 근거는 희박해 보인다. 다만, 거래소가 채무자와 체결한 이용약관에 기하여 채무자에게 개설된 거래계정 전체를 포함한 거래를 정지할 수 있다면 이에 따른 금지명령이 수용될 여지가 있다. …(생략) 대부분의 거래소 이용약관이 거래소의 '운영정책', '관리자의 판단'에 맡기고 있고 그 이유도 타인의 서비스 ID 및 비밀번호 도용, 타인의 명예 훼손, 컴퓨터 바이러스 유통, 정보의 무단 복사 등 공공질서 및 미풍양속의 저해 등으로 제한되어 있다.(윤배경, 앞의 글, 11면 참조).

48) 대법원 2018. 5. 30. 선고 2018도3619 판결.

일본은 매우 신속하게 2016년 5월 25일 자금결제법을 개정하면서 가상통화를 ‘통화’로 자리매김하였고, 새로이 거래소 등록제를 도입하고 고객 자산과 거래소 자산의 분별관리를 의무화하여 더 이상 이 건과 같은 논란이 없도록 하였다.

따라서 정부당국(금융위원회)에서도 이제는 이 문제에 대한 답을 제시할 때가 되었다고 본다. 그렇다면 소유권의 법리를 통해 규율하더라도 전통적 인식체계에 근거한 것이 아니라 과학기술에 기반을 둔 전자화시대에 맞는 법리를 고민하여 개발할 시점이다.

사견으로서 암호화자산에 대한 소유권을 긍정하였으나, 그 요건이 되는 ‘배타적 지배가능성’을 판단하는 기준과 관련해서는 블록체인이라는 P2P 시스템의 특징을 고려하여 보다 정밀하게 재구성할 필요가 있을 것이다. 탈중앙화 내지는 분산형이므로 필연적으로 제3의 관여자의 존재가 있어 배타적인지 여부에 대해 기존의 관점만 고수하면 배타성이 부정될 가능성을 배제하기 어렵고, 또 전자적인 형태에서 그 잔고가 ‘나’만의 계좌에 기록되는 것이 아니므로 종전의 은행 예금과 같은 형태로는 이해하기 어렵다.

어쩌면 기존의 전통적 시스템하에서 우리가 검토했던 배타적 지배가능성의 판단요소를 새로 써야 하는 것은 아닐까 싶다. 법학을 공부하는 우리 모두의 숙제이자 책무로서 그 시대에 맞는 합리적이고도 타당한 법리를 탐구할 필요가 있다. 구체적으로 소유권이 인정된다고 하여 모든 것이 해결되는 것이 아니다. 이 글은 향후 전개될 거대한 법적 담론의 도입부일 뿐, 그 시작에 불과하다.