Special Report

Economy Outlook

2017.9.5

Economist 임동민
3771_9113
dmlim2337@iprovest.com

블록체인, 거인의 어깨 위에 서서

블록체인의 개념과 신뢰확보 메커니즘: 공개분산원장, 작업증명, 암호화폐

블록체인은 '모든 거래자의 거래장부를 공유하고 대조해서 거래를 안전하게 만드는 보안 기술'을 의미. 이전 거래방식은 신뢰확보를 위해 정부, 은행, 중개인 등 제3자의 신뢰부여가 필요했으며 내부조작, 외부해킹, 중간수수료 확대 등의 문제가 발생. 블록체인은 거래기록을 공개분산원장 블록으로 형성 및 연결. 공개장부의 신뢰성의 대조과정을 작업증명(PoW), '채굴'이라고 하며, 이에 대한 보상으로 암호화폐 지급

블록체인의 역사: 1.0 비트코인, 1.5 알트코인, 2.0 이더리움 국면으로 확장

블록체인 1.0은 2008년 10월 사토시 나카모토에 의해 제안된 비트코인에서 시작. 비트코인은 거래체계에 있어 제3자 신뢰를 배제하고, 이중지불 문제를 해결하는 혁신. 이후 컬러드코인, 네임코인, 스마트자산 등 다양한 암호화폐 시도가 이어짐. 블록체인 2.0에서는 비트코인 암호화폐 체계와 스마트계약, DAPP(탈중앙화 앱) 적용 등 확장된 기능을 구현하는 플랫폼, 이더리움 등장. 블록체인 2.0는 ICO(코인공개상장)으로 DAPP이 토큰을 발행, 암호화폐로 크라우딩 펀딩을 받는 산업 생태계 조성

블록체인에 대한 인식변화: 개인, 기업 비즈니스, 중앙정부 관리 효율, 디플레 화폐

비트코인에 대한 초기인식은 실체 없는 가상화폐로 위험성과 투기성이 지적. 그러나 블록체인 기반의 효율성, 안전성, 거래비용 축소로 개인, 기업에게 비즈니스 기회를 제공, 정부는 효율적인 시스템을 주목하기 시작. DAPP, 블록체인 컨소시엄, EEA(Enterprise Ethereum Alliance), 일부 국가 및 중앙은행 블록체인 시스템 도입이 이를 반영. 화폐 발행이 제한되어 생산부가에 대한 구매력 유지도 인식되기 시작

블록체인 암호화폐 시장의 미래: 디지털 시장 및 블록체인 도입과 동반 성장 여력

블록체인 암호화폐 시장은 올해 급속히 성장. 현재 866개의 암호화폐, 233개의 자산베이스 토큰이 발행, 상장되었으며 시가총액은 $1,632억로 증가. 향후 디지털 시장의 지속적인 확대와 P2P 거래, 기업 및 정부의 블록체인 기반의 플랫폼 적용 확대 예상. 블록체인 기반의 플랫폼이 확대되면, 암호화폐의 거래빈도와 규모확장이 요구됨. 따라서 블록체인 암호화폐의 시가총액은 블록체인 기반의 시장확대와 동반

KYOBO 교보증권

목차

프롤로그, 거인의 어깨 위에 서서

왜 블록체인 자료를 쓰게 되었는가?

세상의 변화는 중요하다. 특히 변화의 초기에는 더욱 그러하다. 관심이 없다면 내게 아무 의미가 없다. 그러나 관심은 흥미가 되고, 흥미가 재미가 되면 더 깊이 알 수 있다. 세상의 변화에 관심을 갖는다면 재미와 동시에, 큰 기회를 얻게 될 수도 있다.

블록체인은 2년 전쯤 여의도의 금융 컨퍼런스에서 접했다. 당시 주제는 향후 금융시장의 화두로 '핀테크, 로보어드바이저, 그리고 블록체인'에 대한 논의였다. 핀테크와 로보어드바이저는 들어봤는데, 블록체인은 뭘까? 호기심은 있었는데 알기는 어려웠다.

1년 전쯤부터는 주위에서 블록체인을 얘기하는 사람들이 꽤 늘어났다. 당차게 스타트업을 시작하고, 준비하는 지인들이 블록체인에 대해 말했다. 여의도의 어떤 투자가는 블록체인 기술에 기반한 암호화폐를 사 놓는 것이 좋겠다는 조언도 해 주었다. 뿐만 아니라 경제학을 가르치고 있는 대학원의 교수님으로부터도 블록체인 이야기를 들었다. 이쯤 되면 블록체인을 간과해서는 안 될 것 같다는 생각이 들었다.

올해부터 비트코인, 이더리움 등 암호화폐 가격이 급격하게 뛰기 시작했다. 서점에서는 블록체인 관련 책들이 출간되기 시작했다. 그 때쯤 「블록체인 혁명, 돈 탭스콧 저/을유문화사」를 읽었다. 사실 그 때까지 비트코인이 블록체인 기술에 기반했다는 것을 몰랐으며, 이는 내게는 충격이었다. 새로움을 받아들이는데 이토록 힘들었던 것이다.

지금은 블록체인은 변화의 대세가 되었다. 블록체인에 기반한 암호화폐 시장은 급격히 커지고 있다. 마이크로소프트, JP모건, 캐나다중앙은행이 블록체인을 도입하겠다고 한다. 일본은 암호화폐 지위를 인정하고, 에스토니아는 국가 차원에서 블록체인 기반 체계를 도입하겠다고 한다. 한국도 정부, 금융, 산업에서 블록체인 논의가 활발하다.

한 편, 아직까지도 블록체인에 기반한 비트코인에 대해 의심스러우며 수상한 가상화폐 가치가 급변동이 위험하고, 투기이며 나아가서는 사기라고 보는 시각도 존재한다.

블록체인과 암호화폐에 대해 알기 위해 많은 책들을 읽었고, 많은 자료를 찾아 봤다. (한국은행은 이미 블록체인과 암호화폐에 대해 깊고 풍부한 분석 자료를 다수 발간하고 있다.) 동영상 강의도 보았으며, 실제 블록체인 암호화폐 투자자를 만나 얘기했다.

블록체인과 암호화폐에 대해 아주 조금 알게 된 이후, 지금까지의 경제 및 자본주의 이론은 짧게 되짚어 봤다. 이번 자료는 이러한 과정들에 대한 정리 작업이었다. 그래서 자료의 제목이 '블록체인, 거인의 어깨 위에 서서'이다. 거인들은 나보다 훨씬 이전, 깊은 고민을 했기 때문에, 거인의 어깨 위에서 보면 세상이 더 잘 보인다. 이 자료가 부디 블록체인에 대한 관심, 이해, 합리적인 판단에 도움이 되었으면 하는 바람이다.

우리가 알기 쉽지 않은 네 가지 에피소드

패리사 아흐마디는 아프가니스탄 헤라트, 하티피여자고등학교의 최상위권 학생이다. 아흐마디는 미국의 예술단체, 필름아넥스에서 제공하는 인터넷 및 소셜미디어 교육을 받은 이후, 영화 제작자들에게 콘텐츠 기여 정도에 따라 금전적 보상을 받고 있다. 그러나 아직도 대부분 아프가니스탄 소녀들은 은행 계좌를 갖고 있지 않아, 아버지나 남자 형제들의 은행 계좌로 이체 받아야 한다.

2014년 초, 필름아넥스의 설립자인 프란시스코 룰리는 지불 시스템의 대대적인 변경을 감행한다. 2013년 불현듯 세상에 나타난 디지털 화폐인 비트코인을 이용해 블로거들에게 대금을 지불하기로 한 것이다. 소액자기자본주의(Bootstrap Capitalism) 철학을 믿는 룰리는 비트코인을 이용해 필름아넥스에 유급 콘텐츠 제공자로 등록된 7,000명 이상의 젊은 아프가니스탄 여성들과 그 둘 중 한 명인 아흐마디를 도울 수 있게 되었다. 비트코인은 인터넷 접속이 가능한 누구나 소위 지갑이라고 불리는 디지털 은행 계좌에 저장할 수 있다. 은행에 계좌를 개설하기 위해 직접 갈 필요도 없고, 서류 또한 필요 없고, 남자임을 증명할 필요도 없다.

이 결과 가부장제 사회의 여성이라도 적어도 인터넷에 접속할 수 있는 여성이라면 자신만의 돈을 관리할 수 있게 되었다. 물론 이것이 아흐마디의 모든 것을 다 해결해 주는 만병통치약은 아니지만, 이런 21세기 첨단 기술의 발전이 인류의 상당 부분을 차지하는 그들을 자유롭게 해줄 것임은 틀림 없다. (비트코인 현상, 블록체인 2.0/ The Age of Crypto Currency/마이클 J. 케이시, 폴 비냐 저/미래의 창 서문 中)

아날리 도밍고는 캐나다 토론토에서 25년 간 가사 및 육아 도우미로 일하고 있는 필리핀 여성이다. 그녀는 젊은 나이에 저축 한 푼 없이 캐나다로 이주해 왔고, 정식 교육도 받지 못 했지만, 열심히 일해 자신과 가족의 삶을 건사할 정도로 자수성가할 수 있었다. 그러나 아날리가 토론토에서 번 돈을 마닐라로 송금하는 과정을 보면, 전형적으로 불합리하다.

아날리는 사장이 손수 서명한 수표를 갖고 근처 은행 지점을 찾는 데 15분이 걸렸다. 창구 직원을 대면하기까지는 5분이 더 걸렸다. 아날리는 수표를 입금한 다음, 아날리는 200 캐나다 달러를 인출했다. 그녀는 현금을 손에 쥐고 버스를 타기 위해 한 블록을 걸어갔다. 버스를 타고 그녀의 집의 반대 방향으로 3킬로미터 정도를 더 가서 내린 후 네 블록을 더 걸어간다. 아날리는 비로서 '금융기관'인 아이레미트(iRemit) 창구에 도달했는데, 이 곳은 캐나다 우범 지대로 악명 높은 성 제임스 타운 부근에 있다.

아날리는 서류를 작성하고 열심히 번 돈을 송금했는데, 이러한 일을 수백 번도 넘게 했을 것이다. 필리핀에서는 70세의 어머니가 마찬가지로 힘든 여정을 거쳐 돈을 찾아야 한다. 어머니는 아날리가 송금한 돈을 인출하기 위해 은행을 가기까지 3~4일을 기다려야 한다.

아날리는 200 달러를 송금하기 위해 10 달러의 고정 수수료를 낸다. (캐나다에서 10 달러로 한 끼 식사와 한 번의 버스요금을 해결할 수 있고, 마닐라에서는 일주일 치 장을 볼 수 있다.) 이는 5%에 해당하고, 1~2%의 환전 수수료를 부담해야 한다. 이는 국제적 평균치인 7.68%에 비하면 다소 저렴한 편이다. 아날리의 실제적인 총 비용은 두 시간 일을 하지 못 해 소요된 기회비용 40 달러까지 포함된다. 아날리와 어머니는 둘 다 은행의 고객이면서 이러한 과정을 거쳐야 한다. (블록체인 혁명/Blockchain Revolution/돈 탭스콧, 알렉스 탭스콧 저/을유 문화사 아날리 도밍고의 송금 일화 中)

외륵 플라쩨는 세계 최초로 비트코인으로 결제를 받기 시작한 레스트랑 '룽77'를 운영하고 있다. 2011년 5월부터 식사와 맥주 등 서비스에 비트코인을 받고 있다. 현금 결제는 되지만 신용카드 결제는 받지 않는다. 외륵 플라쩨의 인터뷰 내용이다. "지금까지의 화폐금융 시스템은 중앙은행을 신뢰해야 하는데, 그들이 돈을 제대로 조절하는지, 금리를 제대로 확정하는지를 봐야 하고, 은행을 신뢰해야 한다. 비트코인은 어느 기관을 신뢰할 필요가 없고, 수학만 신뢰하면 된다. 나는 독일 중앙은행이나, 유럽 중앙은행보다 비트코인을 더 신뢰한다." (KBS파노라마 비트코인 가상화폐의 도전 中)

[도표 1] 비트코인 레스토랑 '룽 77'에 걸려 있는 팻말

자료: https://www.youtube.com/watch?v=L-6m-bqqPTo

커피를 한 잔 사보자. 당신은 지금 '그란데' 사이즈 카페라테가 4.3 달러인 뉴욕 스타벅스에 있다. 당신은 아마 그 가격을 보고 잠깐 망설일 수 있지만, 구매하기로 결정한다면, 당신은 캐셔에게 신용카드를 건네는 것을 고민할 리가 없다. 누가 요즘 현금을 가지고 다니는가? 누가 굳이 바닥에 동전을 떨어뜨릴 지도 모르는 위험을 감수하려고 하는가? 누가 굳이 귀찮게 ATM에서 현금을 뽑아 오고 싶어 하는가? 그리고 라테 가격이 좀 마음에 들지 안 들더라도 현금을 낸다 해서 달라질 것은 없다. 제일 중요한 것은 현대의 편리한 신용 카드 결제 시스템은 그 이용료가 무료라는 것이다. 실체는 어떨지 몰라도 적어도 겉으로는 그렇게 보인다.

이제 그 캐셔가 신용카드를 긁으면 어떤 일들이 생기는지 면밀히 살펴보자. 카드를 긁으면, 마그네틱 선에서는 카드 번호, 유효 기간, 청구서가 날아올 주소의 우편번호, 그리고 CVC 번호들이 저장되어 있다. 이러한 개인 정보들이 최선단프로세서(FEP, front-end processor) 회사로 보내진다. 최선단프로세서 회사들의 역할은 결제된 신용카드 계좌에 청구액을 지불할 충분한 돈이 있는 지 최대한 빨리 확인하는 것이며, 정말 그 신용카드가 당신의 카드인지, 당신의 계좌가 맞는지를 확인하는 작업은 나중에 하게 됨). 이후 카드에 담긴 정보를 관련된 마스터카드, 비자, 아메리칸익스프레스 등 카드사의 네트워크망(card association)으로 전송되며, 당신의 카드가 어떤 은행에서 발급되었는지 확인한다. 당신의 개인 정보는 다수 데이터베이스에 흔적을 남긴 후, 이제 각 계좌를 관리하는 발행은행(issuing bank)별 별도의 지불 프로세서(payment processor)로 이동한다. 은행의 정보 유효성 확인 및 신용 확인 절차가 끝나면 그 신호는 다시 반대 방향으로 보내진다. 비로소 스타벅스 캐셔는 확인 메시지가 카드 리더기 화면에 뜬 것을 확인하고, 이 메시지를 '공인된' 것으로 인식한다. 이 과정은 수 초 안에 진행된다.

당신은 이제 카페라테 컵을 들고 나가지만 지불 시스템은 아직 많이 남았다. 한 가지 예를 들면 스타벅스는 아직 커피 값을 받지 못 했다. 스타벅스는 하루를 마감하는 일일 정산 후, 영수증 더미를 인수은행에 전송한다. 인수은행은 상점에 그 영수증에 적힌 액수를 지급하고, 지연 연준(Federal Reserve) 은행의 AHC(automatic clearinghouse)나 세계 18대 상업은행들의 청산지불망(clearing house payments Co.) 등 전자청산결제 네트워크를 이용해 발행은행에게 그 액수만큼 상환을 요청한다. 이제 당신의 은행은 그 라테를 산 사람이 정말 당신이 맞는지 확인하기 위해 당신의 거래 내역을 살펴 보면서 특이점이 없는 지 살핀다. 은행은 이 모든 사실을 확인한 후, ACH 네트워크에 청산결제 지시를 내리고, 당신의 신용카드 계좌의 대변에 이 사실을 기입한다. 그 이후 이 돈은 스타벅스 인수은행으로 흘러가고, 스타벅스 계좌의 차변에 이 사실을 기입한다. 이 프로세스가 완성되는 데에는 일반적으로 3영업일이 소요된다.

이 거래에서 소비자와 스타벅스를 제외한 7개의 기관이 이 거래에 참여한다. 이들은 직불카드인지 신용카드인지에 따라, 각 매출액의 1~3% 비용을 자신의 수수료를 요구하고, 이를 전체 거래 비용에 합산하며, 은행과 각 중개기관이 이 수수료를 가져간다.

이러한 수수료는 상점(스타벅스)가 낸다. 만일 사기 거래가 발견되면 인수은행이 지불 거절을 하며, 해당 상점은 돈과 상품을 모두 잃게 된다. 사기범을 잡는 것은 쉬운 일이 아니며, 사기와 관련해 다른 수수료도 부과될 수 있다. 이런 과정이 국경을 넘는다면 추가적으로 8%의 수수료가 추가된다.

지금까지는 미시적 측면을 살펴봤다. 이번엔 우리 사회 경제 전체에 어떤 영향을 미치는지에 대한 거시적 측면을 살펴보자. 비자와 마스터카드가 2013년에 처리한 신용카드 및 직불 결제액은 약 11조 달러에 이른다. 비자와 마스터카드는 전 세계 카드업계 매출액의 약 87%를 차지한다. 여기에 약 2% 정도 수수료가 부과되었다고 본다면 전 세계 비자와 마스터카드 가맹상점들의 연간 신용카드 결제 수수료는 약 2,500억 달러에 이른다. 전자 상거래 거래대금은 매년 10%씩 증가하고 있다. 부정거래에서 촉발되는 비용까지 더해서 생각해 본다면, 글로벌 지불 시스템에서 카드 결제 수수료가 '톱니바퀴에 낀 모래'처럼 성장, 효율성 그리고 발전의 장애물로 작용할 수도 있다.

물론 전 세계 수십만 명의 사람들이 이 시스템에 관련된 업무를 하며 은행, 지불 프로세스 및 신용 관련 회사에 고용되어 있다. 또한 세계 경제는 여전히 독립된 제3자를 거치지 않고는 디지털 방식으로 돈을 송금하는 것이 불가능한 시스템에 의존해 있다. 믿을만한 중개인은 우리가 가치를 교환할 때, 의존하고 있는 '중개기관 신뢰(institution trust)'를 창출해 왔다. 만약 신뢰할 수 있는 중개기관 없이 거래를 수행할 수 있는 방법을 찾아내면, 많은 사람들이 일자리를 잃을 수 있다.

그러나 뒤집어 생각해 보면, 시스템을 없앰으로써 사회 모든 구성원들에게 부과되었던 비용이 제거될 수도 있다. 다시 말해, 누군가에게로 재화나 서비스가 이전될 때 수수료를 부과하던 중개기관이라는 존재가 사라지면서, 이 일을 수행하던 사람들에게 돌아가던 사람들에게 돌아가던 수수료가 제거되고, 그 돈이 앞으로는 새로운 사업, 새로운 상품, 그리고 새로운 일자리를 만들어내는 데 쓰일 수도 있다. (비트코인 현상, 블록체인 2.0/ The Age of Crypto Currency/마이클 J. 케이시, 폴 비냐 저/미래의 창 변동성과 신뢰의 문제 中)

아흐마디는 아프가니스탄의 소녀, 도밍고는 캐나다에 거주하는 필리핀계 이주노동자, 프라쩨는 유럽의 상인이다. 이들은 기존의 세계에서 모두 불편함과 불확실성을 느끼고 있다. 이는 여자는 은행계좌를 만들 수 없는 아프가니스탄, 캐나다에서 필리핀으로 송금해야 하는 처지, 화폐제도가 불안한 유럽의 상인에만 국한된 문제일까? 먼 미래에 나의 후손들은 혹시 이런 불확실성에 직면하지는 않을까? 스타벅스는 아니더라도 거의 매일 체크카드나 신용카드를 쓰는 나는 시나브로 많은 비용 부담을 내는 것은 아닐까? 기존 체체에서 소외되지 않거나, 비효율을 접하지 않는 수 있는 개인은 없다.

블록체인의 비전: 분산의 안정, 분권의 신뢰, 공정한 보상

돈 탭스콧이 꿈꾸는 블록체인 혁명

「블록체인 혁명」의 저자 돈 탭스콧 (탭스콧그룹 CEO, 토론토대학교 로트만경영대학원 초빙교수)는 번영된 세계로 향하기 위해(Transformation for a prosperous world), 부를 재분배하기보다는(Rather than re-distributing wealth), 부를 원천적으로 배분하기 위해 (could be pre-distribute wealth), 애초에 부가 창출되는 방법을 변화시켜, 부를 창출을 민주화하고(could be democratize the way that wealth gets created in the first place), 경제 활동에 더 많은 사람들을 참여시키고(engaging more people in the economy), 공정한 보상을 받을(receive fair compensation) 방법이 블록체인 기술이라고 말한다.

탭스콧이 제시하는 블록체인으로 구현 가능한 번영은 다음의 다섯 가지 형태이다.

1) 영구적 기록으로 권리를 보호할 수 있다. 토지 소유권은 장기적인 가치창출의 근간이다. 그런데 온두라스와 같은 국가에서는 토지 소유권 조작이 빈번하다. 블록체인 상에 토지 소유권을 기록하면 이는 영구적이며 불가역적으로 재산권을 보호할 수 있다.

2) 공유경제를 진정으로 실현할 수 있다. 인터넷을 기반으로 성장한 에어비엔비, 우버와 같은 거대기업이 출현했다. 공유경제는 가치낭비를 막는다는 점에서 큰 혁신이다. 그러나 이들 기업들은 가치가 공유가 아닌 유통의 독점으로 오히려 거래자간이 누려야 할 가치를 과도하게 징수한다. 블록체인으로 거래자산 가치를 더 높일 수 있다.

3) 송금 바가지를 종결시킨다. 웨스턴 유니온과 같은 거대 중개자들은 외환거래에 있어 10~20%의 수수료를 받는다. 또한 시간도 지체된다. 이는 거래자들의 번영의 기회를 앗아가는 것과 같다. 블록체인을 도입한 아브라 은행을 활용하면 수수료는 2%에 불과하고, 불과 몇 분이면 송금이 완료된다. 대부분의 금융거래에 적용될 수 있다.

4) 정보와 사생활에 대한 보호와 보상이 있을 수 있다. 개인의 생성하는 정보의 수혜를 거대 중개인인 소셜미디어 기업이 편취하거나, 혹은 사생활이 제재 없이 퍼지게 될 위험이 있다. 블록체인 체계는 개인의 정보에 대해 열람, 배포 등에 대한 계약을 전개할 수 있다. 예를 들어 수익화된 개인정보를 지정하거나, 사생활의 배포 등에 자동적으로 제재할 시스템을 갖출 수 있다.

5) 지적재산권을 보호할 수 있다. 지적재산권은 인터넷 세계에서 오히려 더욱 보호되지 못 한 케이스이다. 왜냐하면 불법 복제와 송신이 자행되고, 이를 감독하기 어렵기 때문이다. 만약 이들이 지적재산권을 거래 중개인에 등록하면 보상체계가 왜곡된다. 미셀리움은 블록체인 상에 음원의 권리를 등록해 컨텐츠를 보호할 수 있다.

[도표 2] 돈 탭스콧이 설명하는 블록체인 활용으로 인해 구현할 수 있는 번영

블록체인을 통해 할 수 있는 것들		거대 중개인	문제점	해결을 통한 번영
영구적 기록으로 권리를 보호	Protecting rights through immutable records	온두라스 정부	토지 소유권에 대한 조작	토지 소유권을 영구적으로 기록해 재산권을 보호
공유경제를 진정으로 실현	Creating a true sharing economy	에어비엔비, 우버 등	이들 기업들은 가치의 공유가 아닌 유통의 독점으로 혼자만 번영	예) 비-에어비앤비, 블록체인 상에서 지불, 후기를 통해 평가
송금 바가지 종결	Ending the remittance rip-off	웨스턴 유니온	10% 가량 수수료, 5 시간 정도 걸림, 송금 확정까지 4~7 일 소요	아브라 은행, 수수료 2%, 몇 분이면 송금 완료
정보와 사생활의 보호와 보상	Enable citizens to own and monetize data, and privacy	소셜 미디어 기업	개인이 생성하는 정보의 수혜를 소셜 미디어 업체가 독점, 프라이버시가 보호되지 않음	블록체인 상 기록된 정보가 활용될 때, 개인에게 수익화 및 디지털 거래로 프라이버시 보호
지적 재산권에 대한 보호	Ensuring compensation for the creators of value	왜곡된 유통보상 체계	인터넷으로 인해 지적 재산권 체계가 오히려 무너짐	미셀리움, 블록체인 상에 음원의 권리를 등록해 컨텐츠를 보호

자료: https://www.youtube.com/watch?v=9vyn5sV37o

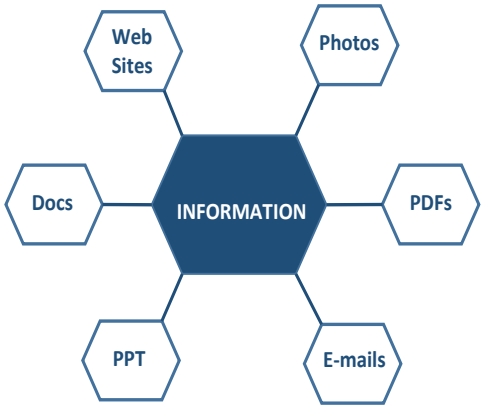
개인 대 개인의 신뢰 프로토콜을 통해 정보 네트워크를 가치 네트워크로 전환

탭스톳은 향후 몇 십 년에 가장 큰 영향을 끼칠 기술로 블록체인을 제시한다. 그는 블록체인 기술이 인터넷의 차세대 모습이며, 인프라 기업과 사회, 그리고 개개인 모두에게 큰 가능성을 보장한다고 한다. 블록체인을 자세히 알기 전에 블록체인으로 이룰 수 있는 것이 무엇인지에 대해 돈 탭스콧의 안목을 미리 보자.

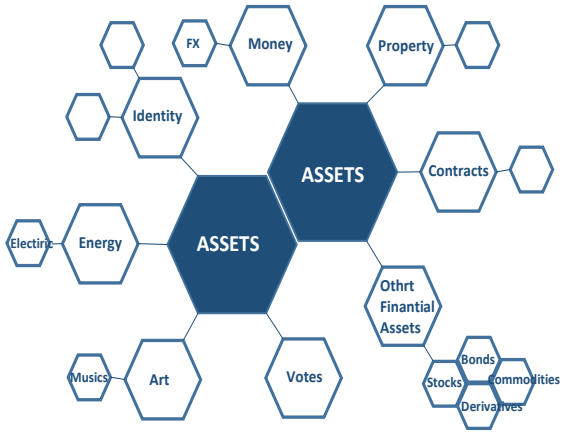
인터넷은 정보망으로 이메일, 서류, 사진 등을 거래비용 없이 보낼 수 있다. 이는 인터넷 이전의 세계보다 분명히 큰 진전이었다.

그러나 인터넷 정보에서 정보전달은 기본적으로 원본을 복사한 파일로 보내는 것이다. 따라서 구매력이나 가치가 녹아 있는 자산을 보낼 수는 없다는 한계가 있었다. 화폐와 주식, 채권 등 금융자산, 부동산 실물자산, 그림 및 음악 등 재산권 보장이 필요한 컨텐츠, 지적재산권, 개인정보, 투표, 계약 등의 신뢰가 필요한 자산을 인터넷 상에서 복사본을 보낼 수 없다. 가치의 정보를 복사하는 순간 이는 신뢰를 잃게 되기 때문이다. (디지털 거래의 관점에서는 이를 이중지불의 문제가 존재한다고 한다)

[도표 3] 정보의 인터넷, 복사된 파일 형태로 연결



[도표 4] 가치의 인터넷, 이중지불의 문제가 존재



자료: https://www.youtube.com/watch?v=9vyn5sV37o

인터넷 상에서 가치가 내재된 거래를 할 때, 결국 신뢰 확보를 위해서 거대 중개자에게 의지하게 된다. 직접 만나서 물물교환을 할 때는 제3자 신뢰가 필요 없다. 약속과 인도의 시차가 있는 거래에서는 거래 상대방이 약속을 어기거나 원본이 아닌 복사본을 보낼 위험과 불확실성을 피하기 위해서 신뢰 있는 제3자 중개에 의지하게 된다.

[도표 5] 이중지불 방지와 신뢰확보를 위해 거대 중개자에 의지

자료: https://www.youtube.com/watch?v=9vyn5sV37o

가치거래의 신뢰확보를 위한 제3자는 예를 들어 정부, 은행, 소셜미디어, 신용카드, 부동산 등 많은 기관이 있다. 이들은 진위판별, 신분확인, 청산, 결제, 기록 등의 임무를 담당하면서 가치거래의 신뢰를 확보해 준다. 모두가 신뢰해야 하기 때문에 평판이 높아야 하며 대개 거대 중개자의 위치를 차지하게 된다.

그러나 거대 중개자들은 통한 거래 체계는 문제점을 낳고 있다. 관리의 집중화로 인해 오히려 해킹 위험에 노출되고, 본의 아니게 경제인구를 배제시킨다. 또한 많은 거래에 대한 신뢰를 보증해야 하므로 거래확정이 지연된다. 신뢰보증의 분업체계로 인해 수수료를 발생시킨다. 도덕적으로 발생해선 안 되지만 내부적인 정보, 가치의 조작도 감행할 수 있다. 무엇보다도 인터넷 정보화 시대의 풍요와 부를 불균형하게 획득시키고 있다는 점이다. 중앙집권은 신뢰를 부여하기 좋지만 느리다. 효율화된 중앙집권일지라도 독점은 불균형과 더 나아가 비효율을 낳는다. 최악의 경우 중앙집권은 타락하고 부패할 수 있다.

[도표 6] 거대 중개자들의 의한 거래 체계에 따른 문제점

문제점	현상
관리의 집중화	해킹에 노출
경제인구를 배제시킴	은행계좌가 없는 많은 세계인
거래확정의 지연	송금 체계 수일이 걸림
높은 비용	송금 수수료 10~20%
디지털 시대의 풍요를 불균형하게 획득	부의 창출과 동시에 불균형 확대

자료: https://www.youtube.com/watch?v=9vyn5sV37o

블록체인 작동원리와 신뢰확보 메커니즘: 공공분산원장과 채굴

블록체인 키워드, '공공거래장부', '암호화폐', 'P2P네트워크', '검증', '보안기술'

최근 블록체인 혁신, 혹은 돈 탭스콧 교수가 주장하듯 블록체인 혁명이라는 용어가 많이 들린다. 사실 우리에게는 블록체인이라는 기술 이전에 비트코인 등 암호화 화폐(Crypto Currency) 등이 투기적인 요소가 많다는 등의 부정적 흐름이 익숙하다. 때문에 블록체인 기반 기술이라는 본질에 대한 이해가 부족한 실정으로 보인다.

블록체인이란 무엇일까? 위키디피아에서는 '공공거래 장부이며 가상화폐로 거래할 때 발생할 수 있는 해킹을 막는 기술'이라고 정의되어 있다. 조금 더 공신력 있는 기관의 정의로써 한국은행에서 발표된「분산원장 기술과 디지털통화의 현황 및 시사점」자료에서는 분산원장기술을 정의하고 있다. 분산원장기술은 '거래정보를 기록한 원장을 정기관의 중앙서버가 아닌 P2P 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하는 기술'이라고 설명되어 있다. 상세하지만 왠지 와 닿지는 않는다.

블록체인 관련 서적에서 정의를 찾아 봤다. 비트코인과 블록체인 역사에 대해 가장 쉽게 읽힌「비트코인 현상, 블록체인 2.0」에서는 '비트코인 중추신경계 역할을 하는 매우 중요한 원장 시스템, 본질적으로는 기술이지만, 돈과 커뮤니티를 둘러싼 개인들이 그룹의 이익을 행동할 수 있도록 하는 규칙」이라고 쓰여 있다. 비트코인 체계를 가장 건조하게 설명한「비트코인, 블록체인과 금융의 혁신」에서는 '거래가 담겨 있는 블록이 그 이전 블록과 연결되어 있는 형태의 정돈된 목록'이라고 쓰여 있다.

블록체인 작동원리를 설명한 유투브 TMook 강좌에서 블록체인은 '모든 거래자의 전체 거래장부를 공유하고 대조해서 거래를 안전하게 만드는 보안 기술을 의미한다.' 라고 설명한다. 이 모든 정의들을 종합해 볼 때, 반복되고 강조되는 단어는 '공공거래장부', '가상화폐(비트코인)', '개인간 거래', '검증', '보안기술'이다. 블록체인에 대해 이러한 배경 지식을 갖고 블록체인의 작동원리와 효과에 대해 본다면 보다 이해가 된다.

[도표 7] 블록체인 및 분산원장 기술에 대한 정의

주체	정의
위키피디아	공공거래 장부이며 가상화폐로 거래할 때 발생할 수 있는 해킹을 막는 기술
「The Age of Cryptocurrency」, 마이클 J. 케이시, 폴 비냐	비트코인에서 중추신경계 역할을 하는 매우 중요한 원장 시스템. 본질적으로는 기술이지만, 돈과 커뮤니티를 둘러싼 개인들이 그룹의 이익을 행동할 수 있도록 하는 규칙
「Mastering Bitcoin: Unlocking Digital Cryptocurrencies」, 안드레아스 M. 안토노폴리스	거래가 담겨 있는 블록이 그 이전 블록과 연결되어 있는 형태의 정돈된 목록
「분산원장 기술과 디지털통화의 현황 및 시사점」, 한국은행 지급결제조사자료(김동섭,2016년 1 월)	분산원장 기술은 거래정보를 기록한 원장을 특정기관의 중앙서버가 아닌 P2P 네트워크(클라이언트나 서버의 개념 없이 동등한 참가자들이 클라이언트와 서버의 역할을 동시에 수행하며 데이터나 주변장치 등을 공유하는 방식으로 주로 음악, 영화 등의 파일을 공유하는 서비스 등에 활용)에 분산하여 참가자가 공동으로 기록하고 관리하는 기술을 의미

자료: 교보증권 리서치센터 정리

블록체인의 작동 원리, 데이터를 모아 검증 뒤, 신뢰가 부여된 공개분산 원장에 연결

은행을 통한 기존의 거래방식에서는 예금, 대출 및 송금 등에 필요한 내용을 작성한다. 이후에 또 다른 새로운 거래를 할 경우 이전의 내용을 확인이 필요하다. 이 때 작성되는 거래내용은 은행(담당기관)만 기록하고 있다. 은행만이 거래내용을 기록, 저장하고 있기 때문에 만약 이전 거래내용에 대한 확인이 필요한 경우 은행에서만 할 수 있다.

블록체인을 통한 거래방식은 모든 거래기록을 공유한다는 점에서 달라진다. 블록체인 방식에서는 거래의 데이터 정보를 블록에 담고, 이 블록이 이전의 블록의 내용과 일치할 경우 모든 거래기록이 담긴 블록의 연결에 추가적으로 연결되게 된다. 블록체인은 거래기록의 모음인 블록인 특정기관의 중앙서버에 기록되지 않고, 암호화된 기록의 형태로 모든 거래자가 보유한다. 새로운 거래는 공개장부 내용 확인 후 확정된다.

[도표 8] 기존 거래방식의 체계

[도표 9] 블록체인 거래방식의 체계

자료: 유투브 TMook (Take easy story and think) 강좌

거래가 이뤄질 때는 거래자들의 장부가 조작, 변경, 해킹되고 있지 않은지에 대한 신뢰가 필요하다. 기존거래방식은 정부, 은행 등 중개자에 의한 중앙집권적 신뢰를 부여받으나, 블록체인 거래방식은 참여자 모두가 거래장부를 보유하고, 확인, 대조한다는 점에서 공개분산형 신뢰를 부여 받는다. 이에 따라 블록체인의 거래방식은 기존 거래 방식에 비해 거래내역 위조, 해킹이 더욱 어려워진다는 장점이 있다. 왜냐하면 블록체인의 거래장부를 위조, 해킹하기 위해서는 네트워크에 참여하는 거래자들의 과반수 이상을 속여야 하는데, 이는 물리적으로 어렵기 때문이다.

[도표 10] 기존 거래방식과 블록체인 거래방식의 비교

구분	특징	신뢰부여 형태
기존거래방식	최소한만 저장, 최소한 인원만 접근. 비밀은 지켜져야 하며 담당기관만이 장부를 보유, 위조 및 해킹 우려	중앙집권적 신뢰
블록체인의 거래방식	공공거래장부. 비밀은 없으며 거래내역 위조 및 해킹이 어려움	공개분산형 신뢰

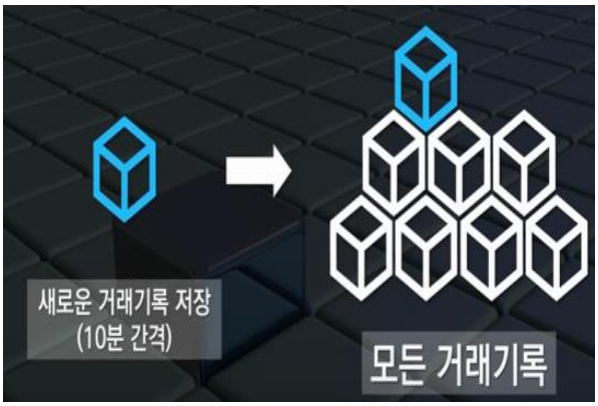
자료: 유투브 TMook (Take easy story and think) 강좌

해시는 암호화 기술로, 블록을 연결하고 위조와 해킹을 차단

새로운 거래는 블록으로 모아진 후, 이전의 모든 거래내용과 비교하게 되는데, 이를 내용대조(Proof of Work)라고 하며, 과반수 이상의 동의를 받으면 블록체인에 연결된다.

[도표 11] 개별 거래의 블록형성 과정

[도표 12] 블록체인 형성 과정



자료: 유투브 TMook (Take easy story and think) 강좌

블록체인을 가능하게 만드는 기술은 해시(hash)다. 해시는 블록을 연결하는 체인의 역할을 하며, 거래내용의 데이터를 암호화하는 과정이다.

해시의 특징은 원문의 길이에 관계 없이 일정한 길이의 값으로 변경된다. 이로 인해 원문 내용보다 적은 데이터 양으로 보관이 가능하다. 또한 원문 내용이 조금만 달라도 해시 값은 완전히 달라진다. 이로 인해 해시 값을 통해 원문 내용을 유추할 수 없다는 특징이 된다. 그리고 이러한 해시의 특징으로 인해 이전 거래내용과 대조해 블록을 연결하고 조작이나 해킹을 어렵게 하는 효과를 나타낸다.

[도표 13] 블록체인 기술에서 해시(Hash)의 역할

정의	블록을 연결하는 체인의 역할을 하며, 거래내용을 암호화하는 과정 예) 비트코인 최초블록 해시 ⊙⊙⊙⊙⊙⊙⊙⊙⊙⊙19d6689c⊙85ae165831e934fffG3ae46aLabcl72b3f1bσ⊙a8ce26f → The Times 03/Jan/2009 Chancellor on brink of second bailout for banks
특징	문장 길이에 관계 없이 일정한 길이의 값으로 변경 원본이 같으면 같은 해시 값이 나오나, 문장 일부라도 다르면 완전히 다른 해시 값이 나옴 해시 값 조합을 통해 원문을 유추할 수 없음 해시 값이 같으면 원본내용을 확인하지 않고도 원본내용이 같음을 신뢰할 수 있음 적은 데이터 양으로 원본내용 모두 완전히 같음을 비교 가능 해시의 특징을 통해 공공거래 장부의 위조를 막음

자료: 유투브 TMook (Take easy story and think) 강좌

거래내역(비트코인의 경우 10분 동안)의 블록의 원문 데이터는 해시 값으로 변경된다. 모든 블록은 직전 블록과 해당 블록의 해시 값을 포함하며, 직전 블록과 해당 블록의 해시 값이 일치할 경우 블록 체인으로 연결된다.

만약 누군가가 거래내용을 위조나 해킹을 하기 위해서는 원본을 바꾼 이후, 블록체인 네트워크에 참여하는 참가자들의 블록보다 빠른 배포가 필요하다. 이는 결국 컴퓨터의 연산력에 의해 좌우된다. 즉 위조나 해킹을 하는 컴퓨터의 연산력이 블록체인 네트워크의 과반수 이상의 연산력보다 높아야 위조나 해킹이 성공할 수 있다. 현재 블록체인 네트워크의 절반의 연산력은 슈퍼 컴퓨터 1~500위 합계의 연산력을 상회한다. 결국 블록체인 상에서 위조 및 해킹의 성공 가능성은 희박하게 된다.

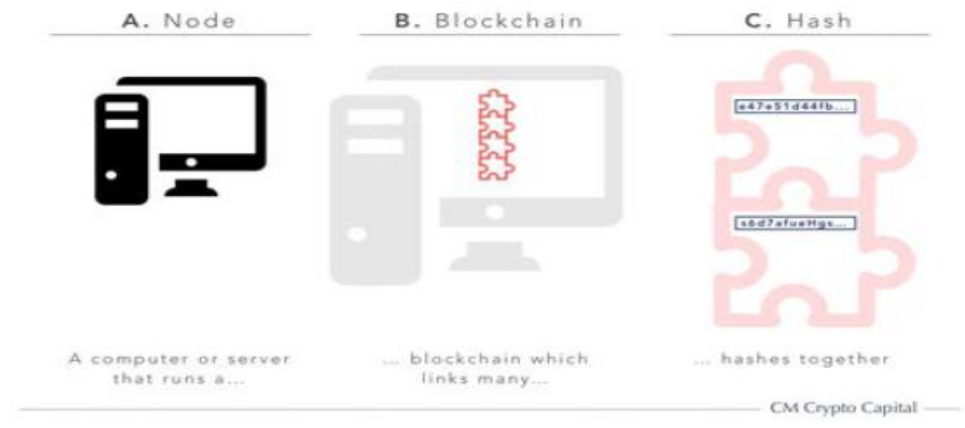
[도표 14] 블록형성은 직전과 해당 블록의 해시 값을 포함

[도표 15] 블록체인에서 위조 및 해킹의 성공 가능성은 희박

자료: 유투브 TMook (Take easy story and think) 강좌

도표24는 블록체인의 주요 개념을 설명한다. 노드는 블록체인 상 분산화된 서버의 기능을 한다. 즉 블록체인을 저장하는 역할을 한다. 블록체인은 검증되고 공인된 블록의 연결이며, 해시는 원문이 암호화로 변경되어 블록을 연결해지는 역할을 한다.

[도표 16] 노드, 블록체인, 해시의 개념도



자료: CM Crypto Capital

채굴(Mining)은 작업증명(PoW)에 대한 화폐보상을 받음, 블록체인의 인센티브로 작용

블록체인 거래체계가 유지되기 위해서는 작업증명(Proof of Work)이 요구된다. 기존 전자거래 체제에서는 이중지불이 가장 큰 문제였다. 즉 거래 시에 자신이 보유한 전자화폐를 한번이 아닌 다수 보낼 위험이 있다는 것이다. 이에 대한 검증이 필요했다.

블록체인 거래체계에서는 작업증명(Proof of Work)를 통해 검증함으로써 이중지불 문제를 해결했다. 그러나 이러한 작업증명은 어떠한 인센티브로 수행하게 될까?

블록체인 체계에서 작업증명을 수행자를 채굴자(Miner), 행위를 채굴(Mining)이라고 한다. 채굴자들은 거래내역을 모아 블록을 생성한다. 이 과정에서 해시 값으로 원본 데이터를 수정해 블록을 생성한다. (이 때 컴퓨터의 연산력이 요구된다) 채굴자들은 블록을 봉인해 해당 작업증명을 네트워크로 전송하고, 다른 채굴자들은 블록의 적합성을 검증한다. 최초로 검증된 블록을 생성한 채굴자는 이에 대한 보상으로 블록에 포함된 거래 수수료와 새로 생성된 암호화 화폐를 보상으로 받게 된다. 결국 채굴은 작업증명에 대한 인센티브를 받게 되고 이에 따라 블록체인 체제가 유지된다.

블록체인은 거래체제는 신뢰성에 대한 네 가지 혁신을 확보

이와 같은 방법으로 정리된 블록체인 거래 체계는 1) 원장 무결성 확보, 2) 참여자간 합의, 3) 화폐발행, 4) 거래장부 동기화로 신뢰성에 대한 혁신을 확보하게 된다.

[도표 17] 분산원장 기술의 신뢰 (Trust) 확보의 혁신적인 측면

신뢰 확보 혁신성	내용
원장 무결성 확보 정책	모든 참여자(node/peer)가 같은 원장을 보관 새로운 거래마다 똑같이 업데이트를 실행 기존의 결제기록에 새로운 결제기록이 추가 블록으로 묶이고 나면 되돌릴 수 없도록 비가역적으로 운영
참여자간 합의 정책	참여자들이 상호 간 거래내역을 전송하기 위해 보증수단 필요 가치 전송을 요청한 당사자를 제외한 불특정 다수가 거래 검증 다수의 승인결과를 시스템 내에서 종합해 정당한 거래임을 입증 이 때 검증권한을 가진 참여자가 다수가 되면 거래 정당성 인정 이것이 검증된 분산장부에 기록되면 거래가 완결
화폐 발행 정책	분산원장 가상통화 시스템은 화폐 발행 (누가, 얼마나, 어떻게 등) 체계 정립 요구 비트코인은 참여자들이 합의된 문제를 풀고 이를 증명하면 발행된 화폐를 소유, 허가 이 방식은 컴퓨팅 파워가 높은 시스템을 보유한 참가가, 즉 소수가 코인을 독점할 수 있다는 단점이 있음 리플코인 등 몇몇 가상화폐는 미리 참여자에게 정해진 양의 화폐를 배분하기도 함
거래장부 동기화 정책	탈중앙 분산장부 시스템의 정상적인 작동을 위해서는, 검증권한을 가진 참여자들이 거래를 요청한 주체의 최근 거래내역 및 일련의 정보를 동일하게 보유해야 함 그러나 여러 이유로 시스템들이 형태가 다른 장부를 가지고 있을 수 있음 이를 분기(Fork)되었다고 하는데, 이때 각 참여자들은 블록(노드)가 많이 형성된 가지가 많은 것을 진본으로 간주

자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」

블록체인 1.0, 비트코인의 시작

비트코인의 시작, 사토시 나카모토(Satoshi Nakamoto)의 백서

2008년 10월 31일 뉴욕 시간 오후 2시 10분, 암호학 전문가 및 아마추어 등 관련자 수백 명이 사토시 나카모토라는 이에게서 이메일 한 통을 받았다.

그는 "저는 신뢰할 만한 제3자 중개인이 전혀 필요 없는, 완전히 당사자간 1:1로 운영되는 새로운 전자통화 시스템을 연구해오고 있습니다."라는 간결하고도 담담한 문구를 적었다. 그는 그 문구와 함께 9쪽짜리 보고서를 다운받을 수 있는 링크를 보냈으며, 그 보고서가 업로드되어 있는 웹사이트는 두 달 전쯤 개설된 것으로 확인됐다. 그는 그 통화시스템을 '비트코인'이라 부르고 있었다. (비트코인 현상, 블록체인 2.0/마이클 J. 케이시, 폴 비냐 저/미래의 창) 이것이 비트코인의 시작이다.

사토시 나카모토의 비트코인 백서의 초록은 다음과 같이 비트코인의 토대와 기본 원칙을 설명한다. (비즈니스 블록체인/윌리엄 무가야 저/한빛미디어)

▶순수 P2P 버전의 전자화폐로 금융기관의 개입 없이 당사자 간에 온라인 대금 결제가 가능

▶이중지불(컴퓨터 파일을 쉽게 복제할 수 있는 것과 같이, 디지털화폐를 복제해 사용할 때 발생하는 문제)을 저지할 믿을 수 있는 제3자는 필요하지 않음

▶P2P 네트워크로 이중지불 문제에 대한 해결책을 제시

▶네트워크는 타임스탬핑 기능을 통해 거래들을 기록. 거래들은 해시 값(데이터를 특정 규칙을 통해 기존보다 짧은 길이로 변환해 위변조 여부를 파악하는 용도로 사용)을 기반으로 한 작업증명(POW : 작업을 증명한다는 뜻이 아닌 작업을 활용한 증명)이 연쇄적인 체인 형상으로 기록. 이 기록은 작업증명을 새로 수행하지 않는 한 변경을 가할 수 없음

▶최장 길이의 체인은 발생한 사건들의 순서를 증명하는 동시에 그 사건들이 최대 규모의 컴퓨팅 파워 풀을 통해 입증되었음을 나타냄. 다수의 컴퓨팅 파워가 네트워크에 대한 공격의도가 없는 노드들에 의해 제어되는 한 이 노드들은 길이기 가장 긴 체인을 생성하여 공격자들을 물리칠 것

▶네트워크는 최소한의 구조를 갖춰야 함. 각 노드에서 발생되는 메시지는 네트워크 안에서 최대한 공유. 노드들은 네트워크에서 자유롭게 참여하고 떠나기를 반복할 수 있으며, 부재중에 발생한 일에 대한 증거로 최장길이를 유지하는 작업증명 체인을 채택

사토시 나카모토가 제시하는 비트코인의 토대와 기본원칙은 1) P2P 전거거래 및 상호작용, 2) 금융기관의 필요성 상실, 3) 암호학적 증명으로 중앙의 신용기관 대체, 4) 중앙기관 개입 없이 네트워크 자체가 신뢰인증 해결로 요약된다. 다음은 사토시 나카모토의 백서(White Paper) 초록과 거래내용들의 블록체인 형성과정 및 신뢰 형성 과정을 설명한 도식이다. 앞서 살펴본 블록체인 작동원리를 보면 이해가 갈 것이다.

[도표 18] 비트코인 백서 초록

Bitcoin : A Peer-to-Peer Electronic Cash System (비트코인 : 개인간 전자화폐 시스템)

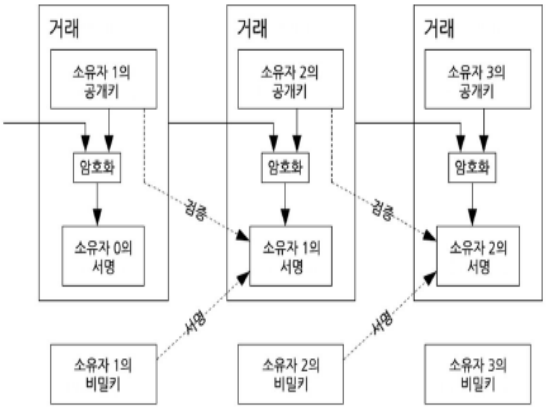
Satoshi Nakamoto (사토시 나카모토)
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financail institution. Digital signitures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

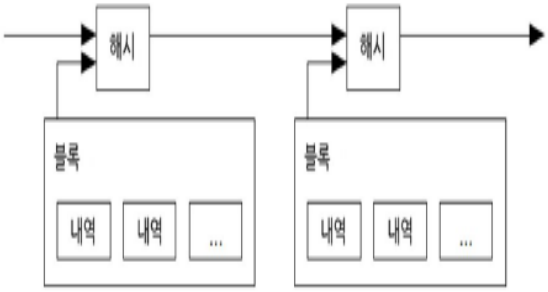
초록. 순 개인과 개인과의 전자화폐는 한 집단에서 다른 곳으로 금융기관을 거치치 않고 직접 온라인 지불을 가능하게 할 것이다. 디지털 서명 기술이 일부 해결해주지만, 믿을 수 있는 제 3 자가 이중지불을 방지해야 한다면 그 주요한 장점은 사라지게 된다. 우리는 이 논문에서 P2P 네트워크를 이용한 이중지불 문제의 해결 방법을 제안하고자 한다. 계속 진행되고 있는 암호화 기반 작업증명 과정의 연쇄 상에서 네트워크 시간 및 거래를 암호화하여 기록을 생성하게 되면 작업증명 과정을 되풀이하지 않는 한 바꿀 수 없게 된다. 가장 긴 체인은 각 사건 순서를 입증해 주기도 하며, 가장 많은 컴퓨팅 파워가 입증됐다는 뜻이기도 하다. 노드들에 의해 제어되는 컴퓨터 전력의 과반수가 협력하여 네트워크를 공격하지 않는 한, 그들은 가장 긴 체인을 생성하며 네트워크 공격자를 능가하게 될 것이다. 이러한 네트워크는 최소한의 구조를 필요로 한다. 각 노드들은 자발적으로 그 네트워크를 떠나거나 다시 합류할 수 있고, 어떤 일이 벌어졌는지에 대한 입증으로 가장 긴 작업증명 체인을 받아들이는 노드들의 메시지가 최대한 공유된다.

자료: 「Bitcoin: A Peer-to-Peer Electronic Cash System」

[도표 19] 거래자간 서명과 검증으로 거래기록이 불록화

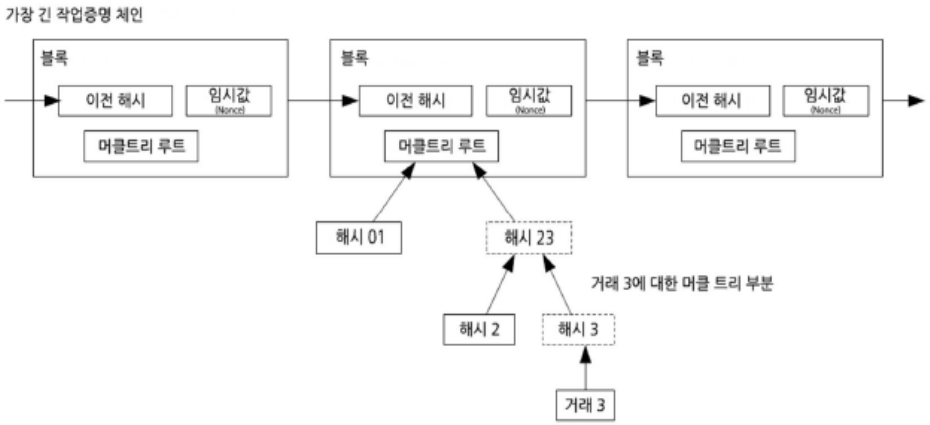


[도표 20] 타임스탬프 서버 체인 형성 과정



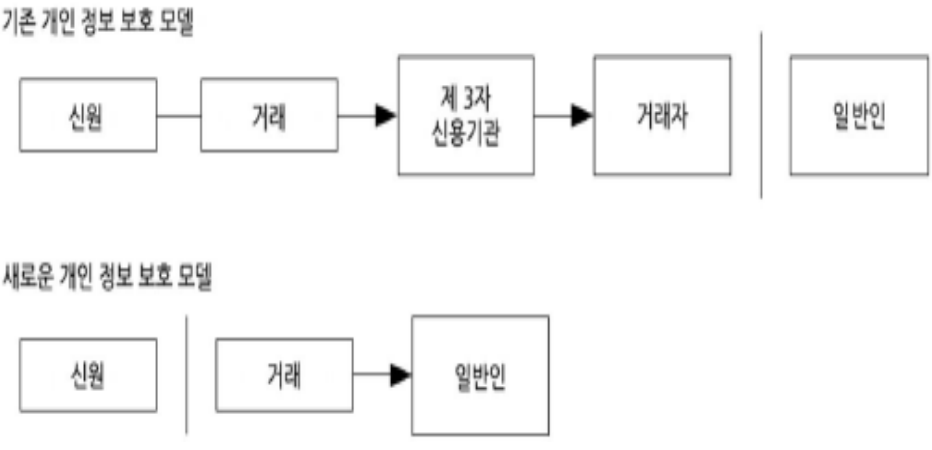
자료: 「Bitcoin: A Peer-to-Peer Electronic Cash System」

[도표 21] 지불 입증 간소화 과정



자료: 「Bitcoin: A Peer-to-Peer Electronic Cash System」

[도표 22] 기존 거래와 비트코인 거래에서 개인정보 보호 체계 비교



자료: 「Bitcoin: A Peer-to-Peer Electronic Cash System」

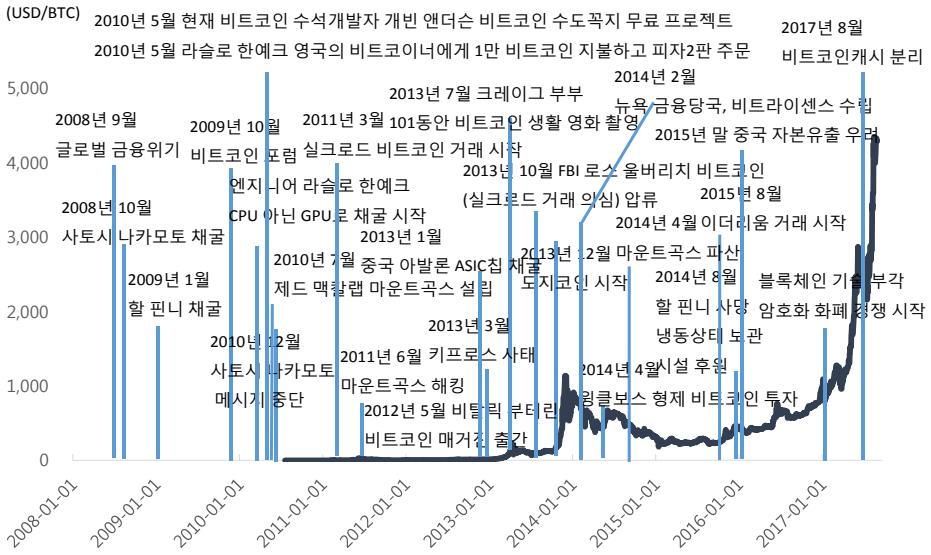
다섯 국면으로 구분한 비트코인의 역사

2008년 10월 사토시 나카모토에 의해 소개된 비트코인은 공식적으로 (거래소 상) 2010년 7월 $0.08에 시작되어 2017년 8월 현재 $4,288.70로 올랐다. 약 7년 간 무려 536만 % 올랐다. 이러한 비트코인의 법정화폐 표시 가격상승을 볼 때 투기와 사기를 떠올리는 것도 무리는 아니다. 그러나 비트코인의 스토리를 함께 정리해 보면, 화폐가 발행되고, 교환되기 시작하고, 거래체계를 갖추어 가는 과정을 이해할 수 있다.

1국면: 2008년 9월 리만 브러더스 파산 이후 직후 10월 사토시 나카모토는 비트코인을 공개했다. 이후 사토시는 자신이 만든 비트코인 소프트웨어를 깔고 첫 번째 블록(Genesis block)을 만들고 채굴을 시작했다. 2009년 1월, PGP(Pretty Good Privacy)라는 주식회사 CEO였던 할 핀니가 사토시의 아이디어에 반응하면서 두 번째 채굴자로 나섰다. 할 핀니는 암호화 분야의 선구자로 이더리움의 창시자 비탈릭 부테린의 백서에 소개되는 인물이다. 할 핀니는 2014년 8월, 죽기 전 냉동인간을 선택한다.

2국면: 2009년 10월 비트코인 포럼이 만들어지면서 개발자들과 채굴자들이 등장한다. 라슬로 한예크라는 엔지니어는 CPU보다 GPU 채굴효율이 더 좋음을 알아 채굴자로 나선다. 2010년 5월에는 비트코인 수석개발자인 개빈 앤더슨이 '비트코인 수도꼭지'라는 프로젝트로 비트코인을 무료로 나눠주는 행사를 벌인다. 같은 달 라슬로 한예크는 유명한 일화인 1만 비트코인으로 피자 2판을 주문하기도 했다. 이는 처음으로 비트코인이 재화와 교환된 사례이다. 2010년 7월에는 최초의 거래소인 마운트곡스가 설립되었다. 2010년 12월에는 사토시 나카모토의 공개 메시지가 중단되었다.

[도표 23] 비트코인 가격과 이벤트 정리



자료: Coinmarketcap, 「비트코인 현상, 블록체인 2.0」

마운트곡스 설립 이후 드디어 비트코인의 달러표시 가격이 형성되었는데, 1 비트코인은 $1 이하였다. 2011년 3월에는 실크로드에서 마약이 비트코인으로 거래되기 시작했으며, 2011년 6월 마운트곡스에서 해킹이 발생되었다. 2012년 5월에는 훗날 이더리움의 창시자인 비탈릭 부테린이 '비트코인 매거진'을 출간했다.

3국면: 2013년 1월부터는 중국의 채굴자들이 '아발론'이라는 기업을 세워 ASIC(주문형 반도체)칩으로 채굴하기 시작했다. 2013년 3월에는 키프로스 재정위기가 발생했다. 키프로스 은행 구제금융에 있어 예금자들에 대한 손실부담 및 자본유출 중단이 결정되자, 비트코인 수요가 크게 올라 가격이 급등했다. 2013년 7월에는 크레이그 부부가 101일 동안 비트코인으로 생활한 영화를 찍었다. 비트코인의 국경간 이동과 교환의 매개 기능이 알려지면서 비트코인 가격이 상승했다. 2013년 10월에는 FBI가 실크로드에서 마약 거래 혐의로 로스 울버리치를 체포했으며, 그의 PC에 있던 비트코인을 압류했다. (FBI는 이런 방식으로 상당량의 비트코인을 보유하고 있을 것으로 추정된다.) 2013년 12월에는 최초의 비트코인 거래소인 마운트곡스가 파산하면서 과열양상을 보인 비트코인 시장이 냉각되기 시작한다. 2014년 2월에는 뉴욕의 금융당국이 비트코인 라이선스를 추진했으며, 같은 해 4월에는 윙클보스 형제가 비트코인이 투자했다는 발표했다. 그 이후 비트코인은 한 동안 관심에서 멀어져 간 듯 했다.

4국면: 러시아 출신의 캐나다 프로그래머이자 '비트코인 매거진' 2013년 말, 「A Next-Generation Smart Contract and Decentralized Application Platform(차세대 스마트 컨트랙트와 탈중앙화된 어플리케이션 플랫폼)」이라는 제목의 백서를 발표하고, 블록체인 기반의 암호화 화폐이자 플랫폼인 '이더리움'을 공개했다. (이더리움에 대해서는 차후 자세히 설명한다.) 2015년 8월 이더리움이 암호화 화폐 거래소에서 달러화 표시 가격이 결정되기 시작한다. 이더리움이 블록체인 기반으로 통화체계 뿐만 아니라, 스마트 계약, 분권화 앱 등의 확장에 대한 기대로 부상하기 시작했다. 이 때부터 암호화 화폐에 대한 관심이 더욱 높아지기 시작했으며, 비트코인 가격은 멈추지 않는 상승세를 보인다. 2015~2016년에는 중국의 자본유출 위험이 크게 확대되면서 비트코인이 위안화 표시자산의 대안 및 투기의 대상이 되었다는 시각도 있다.

4국면: 이더리움 등 암호화 화폐 등이 부상하면서 비트코인 한계점이 인식되었다. 비트코인은 통화거래체계에 머물러 있고, 블록이 10분당 형성되어 거래처리 능력이 제한적인 점 등 한계점이 있다. 세그윗(Segwit/Seperated witness: 블록 용량의 약 절반을 차지하는 디지털 서명(거래인증 데이터)를 분리, 보관하는 방식으로 블록크기 증가 없이 1.7~2배 처리량 증대 가능)이 논의되었으나, 중국 채굴자 Bitmain 연합은 이를 반대했다. 세그윗은 연기되고 Bitmain 연합은 비트코인 캐시(BCH)를 도입하는 1차 하드 포크(Fork: 소프트웨어에서 버전 업그레이드를 의미, 소프트 포크는 채굴자가 업그레이드, 유저는 하지 않아도 됨, 블록체인 유지. 하드 포크는 채굴자, 유저 모두 업그레이드, 블록페인 분리) 현실화되었다. 비트코인은 합의불발 우려로 급락했으나, 1차 하드 포크 이후 비트코인 캐시 가격이 급등, 비트코인은 거래능력 증대 기대로 상승하고 있다.

5국면 (2차 하드포크와 미래): 비트코인 생태계는 개발자, 소유자, 채굴자로 구성되며 서로 다른 니즈를 가진다. 특히 비트코인 처리용량 확대와 관련해 개발자와 채굴자의 의견이 대립되고 있다. 비트코인 처리지연이 확대됨에 따라 2017년 5월 소유자와 다수의 채굴자는 우선 세그윗을 하고, 2X(블록크기 2배 확대)에 합의했으나, 중국 Bitmain 연합과 개발자는 이에 반대했으며, 일단 8월 1일 Bitmain 연합의 비트코인 캐시 도입으로 1차 하드 포크 결정 이후 비트코인은 2017년 11월 2차 하드 포크를 앞두고 있다.

[도표 24] 비트코인 생태계 진영 별 역할과 주요 니즈

구성원	역할	주요 니즈
개발자	비트코인 프로그램(코어, 지급 등) 개발	탈중앙화, 네트워크상 자유/익명성
소유자	시장수요의 근간, 가격 형성(가치 창출)	자산가치 상승, 결제/송금 기능
채굴자	신규통화의 공급, 거래 검증(신뢰 창출)	채굴경쟁 승리(통화획득), 거래수수료 극대화

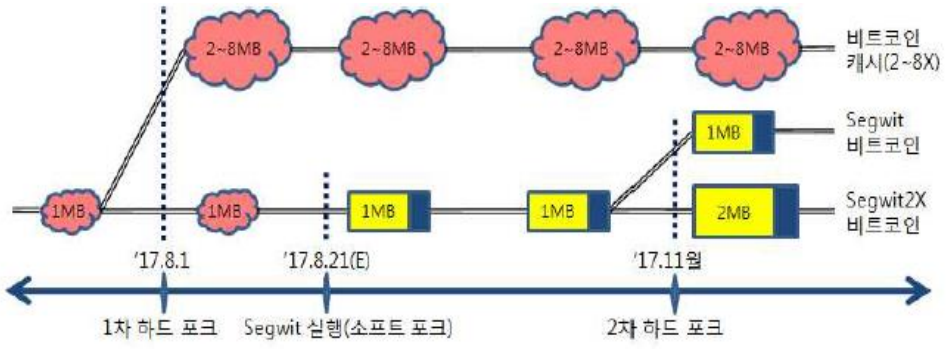
[도표 25] 비트코인 처리용량 확대(Scaling) 주요 내용

구분	개발자 입장	채굴자 입장
세그윗 (Segwit)	탈중앙화 제고(채굴 집중화 완화), 블록구조 변경으로 보안 강화, 확장성 개선	기존 블록구조에 최적화된 전용(ASIC) 채굴기 효율 감소
블록크기 확대 (2X)	채굴집중화 가중(고성능 저장, 네트워크 장비 필요, 블록 전파속도 감소)	전용 채굴기 유효, 고가의 장비유지가 가능한 기업형 채굴자의 경쟁력 상승

자료: 산업은행 「비트코인 진화와 생태계 내전」 주: 세그윗을 통한 블록체인 변경은 다른 블록체인과 연계, 신기술인 스마트계약 도입 등 기술적인 확장성에 유리

2차 하드포크의 쟁점은 세그윗 만을 주장한 개발자들이 2X(블록크기 2배 확대)에 반대하는 것이다. 만약 소유자와 다수의 채굴자가 합의한 Segwit2X 비트코인 도입에 반대할 경우, 현재 비트코인은 개발자 진영의 Segwit 비트코인과, Segwit2X로 분리될 수 있고, 결국 비트코인은 Segwit, Segwit2X, 비트코인캐시 등 세 가지로 분리될 수 있으며, 각기 비트코인의 가치망(Value network)에 대한 신뢰와 가격변화에 대한 불확실성이 존재한다.

[도표 26] 2017 년 8 월 이후 비트코인 포크 일정



자료: 산업은행 「비트코인 진화와 생태계 내전」 주: 소프트 포크(Soft Fork)란 체인 분리가 일어나지 않는 블록(지갑, 채굴 소프트웨어) 업그레이드로 포크 이전과 호환성이 유지. 하드 포크(Hard Fork)란 체인 분리가 일어나는 블록(지갑, 채굴 소프트웨어) 업그레이드로 포크 이전과 호환성이 단절

Appendix # 1. 비트코인 관련 용어 해설

[도표 27] 주요 비트코인 관련 용어 해설

명칭	영문	내용
주소	address	비트코인의 주소형태는 1DSrfJdB2AnWaFNgSv3MZC2m74996JafV 와 같은 형식. 1(숫자)로 시작하는 여러 개의 문자와 숫자의 조합으로 이루어져 있음. 상대방에게 이메일을 보내기 위해 이메일 주소를 물어보는 것처럼 상대방에게 비트코인 주소로 비트코인을 보내 달라고 요청할 수 있음
QR 코드	QR code	비트코인 주소를 인코딩해 형상화한 것 (일종의 바코드)
비트코인 개선 제안	Bitcoin Improvement Proposals	비트코인 커뮤니티 회원들이 비트코인을 개선하기 위해 내놓은 일련의 제안. 예를 들면 BIP0021 은 비트코인의 인터넷식별자(URI) 체제를 개선하기 위한 제안
비트코인	bitcoin	화폐 단위(코인), 해당 네트워크 및 소프트웨어의 이름
블록	block	거래의 집합으로 타임스탬프와 이전 블록의 지문이 표시. 불록 헤더를 요약해 작업증명(proof of work)을 만들고 이를 통해 거래가 유효화. 유효화된 블록들은 네트워크의 동의를 얻은 후 주 불록체인에 추가
블록체인	blockchain	유효화된 블록의 집합으로 각 블록체인은 이전에 생성된 블록체인과 연결되어 최초블록(genesis block)까지 이어짐
승인	confirmation	거래가 블록 내에 들어가면 한 건의 승인이 발생. 동일한 블록체인 상에서 또 다른 블록이 채굴되자마자 해당 거래는 두 건의 승인을 보유하게 되며, 이 과정이 반복. 최소 여섯 건의 승인이 있어야 거래가 철회될 수 없다고 판단
난이도	difficulty	작업증명을 하기 위해서 얼마나 많은 계산이 필요한지를 제어하는, 전 네트워크의 설정값
난이도 목표값	difficulty target	해당 네트워크 내에 있는 계산력으로 약 10 분마다 블록을 찾을 수 있는 난이도를 말함
난이도 재설정	difficulty retargeting	2,016 개의 블록에서 한 번 발생하며 이전 2,016 개의 블록의 해싱파워를 고려해 네트워크상에서 난이도를 다시 계산
수수료	fees	비트코인 송신자는 요구받은 거래에 대해 해당 네트워크 수수료를 포함시킴. 대부분의 경우 거래 한 건당 최소 0.5mBTC 의 수수료가 듬
해시	hash	2 진수 입력에 대한 디지털 지문
최초블록	genesis block	블록체인에서 첫 블록으로, 암호화 화폐를 시작하는 데 사용
채굴자	miner	새로운 블록에서 유효한 작업인증을 찾기 위해 해상을 반복하는 네트워크 노드를 말함
네트워크	network	거래와 블록을 네트워크상에 있는 모든 비트코인 노드에세 전파하는 P2P 기반 네트워크를 말함
작업증명	Proof of Work	블록을 찾기 위해 다량의 계산을 요구하는 데이터. 비트코인에서 채굴자들은 전 네트워크에 걸쳐 설정되어 있는 목표값, 즉 난이도 목표값을 충족하는 SHA256 알고리즘에 대한 수치적 솔루션을 찾아내야 함
보상	reward	작업증명 솔루션을 발견한 채굴자에게 네트워크가 보상의 개념으로 새 블록 각각에 포함시켜 놓은 금액. 현재 한 블록당 25BTC
비밀키(개인키)	secret key(private key)	해당 주소로 전송된 비트코인을 사용할 수 있게 해 주는 비밀번호. 비밀키는 5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh 의 형태를 가짐
거래	transaction	간단하게 설명하면, 어떤 한 주소에서 다른 주소로 비트코인이 이동하는 것을 말함. 좀 더 자세히 설명하면 거래란 송금을 의미하는 서명된 데이터 구조. 거래는 비트코인 네트워크를 통해 전송되며, 채굴자들이 수집하고 블록에 포함시켜서 블록체인 내 영구적으로 존재하게 만듬
지갑	wallet	비트코인 주소와 비밀키가 담겨 있는 소프트웨어. 비트코인을 전송하고 수취하고 보관하는데 이용

자료: 비트코인, 블록체인과 금융의 혁신 / 안드레아스 M. 안토노풀로스

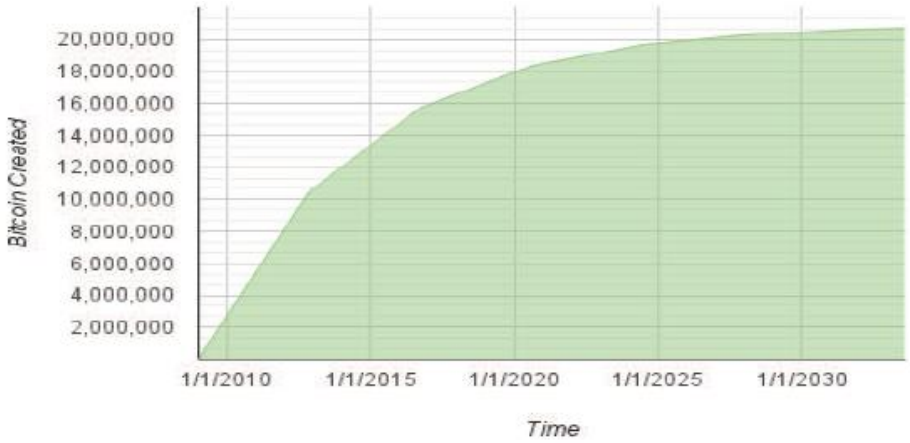
Appendix # 2. 비트코인의 거래 절차

[도표 28] 비트코인 거래 절차의 도식화

자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」 2016년 공동연구 결과보고서

Appendix # 3. 비트코인 통화 공급량

[도표 29] 비트코인 통화 공급량, 2040 년까지 2,100 만 비트코인이 발행



자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」 2016년 공동연구 결과보고서

Appendix # 4. 워렌 버핏과 마크 안데르센 간 논쟁

비트코인에 대한 워렌 버핏의 의견, "수표는 돈을 전달하는 도구이다. 그렇다고 해서 '수표 그 자체'에 투자가치가 있다고 할 순 없다. 비트코인도 마찬가지이다. 비트코인은 돈을 전달하는 새롭고 편리한 수단일 뿐, '비트코인 그 자체'에 투자가치가 있는 것은 아니다."

벤처 투자자 마크 안데르센의 반론, "(워렌 버핏의 의견은) 테크놀로지가 뭔지 잘 모르는 사람들이 기술에 대해 폄하할 때, 상투적으로 하는 방식이다. 이 기술이 난리 법석을 칠 만큼 미치도록 유용하거나 가치 있진 않을 것이라고 하는 것이다. 비트코인의 본질적인 가치는 가치교환 인프라의 기능적 가치에서 창출된다. 비트코인은 화폐 경제에 어느 정도 포함될 텐데, 현재(2014년) 유통량과 유통속도를 감안하면, 비트코인의 Marketcap 규모는 충분히 높아야 한다."

[도표 30] 비트코인에 대해 상반된 시각을 보인 워렌 버핏과 안데르센 호로비츠

자료: CNBC 보도 내용

블록체인 1.5, 알트코인 전국시대

블록체인 기술로 구현할 수 있는 네 가지 카테고리 기술

비트코인은 화폐분야에서 담보나 내재적 가치를 갖지 않는 가운데, 중앙통제 기관 없는 거래가 가능함을 보였다. 이더리움의 창시자 비탈릭 부테린은 이와 함께 분산합의 수단으로서 블록체인으로 구현할 수 있는 일들에 중요성을 더욱 높게 평가했다.

2009년 비트코인이 나오고 어느 정도 성공을 거둔 이후, 블록체인 기술이 접목되어 1) 암호화통화 기술, 2) 자산등기 기술, 3) 플랫폼 기술, 4) 분권화된 자율 조직 및 애플리케이션들이 다양하게 나온다. 이른 바 블록체인의 춘추전국시대가 시작된다. (차후 내용은「공동연구, 분산원장 기술의 현황 및 주요 이슈」, 한국은행과「비트코인, 블록체인과 금융의 혁신」안드레아스 M. 안토노폴로스, 위키디피아 참조)

[도표 31] 2009 년 비트코인 구현 이후 다양하게 전개된 블록체인 기술

자료: 한국은행 「공동연구, 분산원장 기술의 현황 및 주요 이슈」

자산등기기술 (Asset Registry Technology)

자산등기기술은 블록체인을 활용해 자산을 등록하는데 사용하며 매스터코인, 컬러드코인, 네임코인, 카운터파티 등이 있다. 분산원장 상의 작은 거래기록을 통해 어떤 자산(주식, 자동차, 건물, 토지, 도메인 등)의 존재에 대한 증거를 남기면 중앙기관(대부분 정부)에서 관리하는 등기소에 등록할 필요 없이 특정한 자산에 대한 소유권을 증명할 수 있다. 공공원장에 존재하는 개인키의 소유자가 그 특정한 자산의 소유자가 되는 것이다. 자산등록기술은 규제와 감사비용을 줄일 수 있다. 현재 자산등록은 새롭게 네트워크를 구성하지 않고 기존 분산원장에 비트코인 블록체인을 사용해 추가 데이터를 포함해 단순 인지하는 데 그치고 있다. 때문에 비트코인 블록체인 이외 매스터코인이나, 컬러드코인의 가치가 보호되지 않을 수 있으며 확장성에 한계가 있다.

암호화 통화기술 (Crypto-currencies)

초기 분산원장 기술은 비트코인(Bitcoin)을 필두로 라이트코인(LiteCoin), 피어코인(PeerCoin), 도기코인(DogeCoin) 등 암호화통화의 가치보존과 유통을 위해 설계되었다. 암호화통화는 제3자 없이 신뢰할 수 없는 다수의 참가자가 네트워크에서 신뢰할 수 있도록 수학적 알고리즘에 의해 설계되었다. 이는 임의조작이 불가능하고, 이중지불 문제를 해결해 지급결제 수단으로서 법정화폐처럼 안전하게 유통시킬 수 있다. 법정화폐와 다른 점은 법적인 지위를 갖지 않고, 규제와 감독의 대상이 아니라는 점이다. 이는 장점이자 단점이 될 수 있다. 암호화통화의 시장규모는 미미했지만 최근 빠르게 확대되고 있다. 비트코인 등은 초당 처리할 수 있는 거래건수의 확장이 제한되는 등 기술적 한계가 있다. 다만 이에 대한 개발자, 채굴자 및 소유자들이 변화에 합의한다면 개선될 여지가 있어 귀추가 주목된다.

비트코인(BitCoin/BTC, XBT)은 디플레이션을 위한 고정발행통화라는 특성을 부여해 주는 통화적 변수를 몇 개 갖고 있다. 비트코인은 2,100만 비트코인으로(2,100조 사토시)으로 그 발행량이 한정되어 있으며 기하학적으로 발행률이 감소된다. 또한 10분 단위로 블록이 생성되는 '핵심적인 특징'을 갖고 있고, 이를 통해 거래승인 및 통화생성 속도를 관리할 수 있다. 많은 알트코인(비트코인의 소스코드로부터 파생되었으나 각기 다른 블록체인을 사용한다. 비트코인은 통화수단, 알트코인 용도는 다르다.)

라이트코인(LiteCoin/LTC)은 2011년 초기에 출시된 알트코인이며, 비트코인 다음으로 성공한 화폐다. 라이트코인은 작업증명 알고리즘으로 스크립트를 사용(비트코인은 SHA-256 기반)하고, 통화적 변수에 대한 값들이 비트코인보다 빠르고 작다. 블록생성 시간은 2분 30초, 총 발행량은 2140년까지 8,400백만 코인, 합의 알고리즘은 스크립트 작업증명이며 시가총액은 2017년 8월 현재 $33억 6천만으로 5위를 차지하고 있다.

피어코인(PeerCoin/PPC)은 2012년 8월 도입되었으며 작업증명 알고리즘과 지분증명 알고리즘을 함께 사용하여 새로운 통화를 발행하는 첫 번째 알트코인이다. 블록생성 시간은 10분, 총 발행량은 무제한이며, 합의 알고리즘은 작업증명을 사용하다가 나중에는 지분증명과 혼합하게 된다. 시가총액은 2017년 8월 현재 $4천 6백만으로 90위를 차지하고 있다.

도기코인(DogeCoin)은 라이트코인의 분기를 기반으로 2013년 12월 출시되었다. 도기코인이 주목을 받은 이유는 코인의 발행속도가 빠르고 통화 한도치가 매우 높다는 것이다. 총 발행량이 높은 것은 소비와 팁 문화를 장려하기 위해서다. 도기코인은 장난삼아 시작되었다가 유명해진 코인으로 널리 알려져 있다. 2014년 급속하게 쇠퇴하기 전까지 규모가 크고 활동이 많은 커뮤니티 내에서 인기를 끌었다. 블록생성 시간은 60초, 총 발행량은 2015년까지 1,000억 코인, 합의 알고리즘은 스크립트 작업증명, 시가총액은 2017년 8월 현재 $1억 9천만으로 40위를 차지하고 있다.

자산중심기술 (Asset Centered Technology)

자산중심기술은 자산 존재의 디지털 표현과 관리에 초점을 맞춘 기술이다. 자산등록 기술과 유사하지만 퍼블릭 원장에 데이터를 추가하는 방식이 아닌 고유한 기술과 프라이빗 네트워크나 컨소시엄 네트워크를 구현해 자산의 거래나 이동을 용이하게 하는 기술을 개발한다. 예를 들어 리플, 스텔라, 하이퍼렛저 등의 서비스는 각각 자산(통화, 금속, 주식, 채권 등) 존재의 디지털 표현과 관리에 집중한다.

이 네트워크에서의 신뢰는 비트코인 식의 블록체인을 통한 검증이 아닌, 참여자들이 직접 제공해 만들어진다. 이런 방식이 성공하기 위해서는 참여자들이 '미화', '위안화', '금', '비트코인' 등의 데이터 자산을 네트워크에 출고하겠다는 약속이 있어야 가능하다. 또한 참여자들 중 몇몇은 이러한 자산을 다른 자산으로 바꿀 수 있도록 하는 책임이 있다. 즉, 현실세계와 가상세계를 연결하는 게이트웨이 역할을 해야 한다. 어떤 자산을 다른 자산으로 바꾸기 위해 시장조성자(Market Maker) 기능이 필요한데, 이는 궁극적으로 탈중앙화되지 못 해 블록체인 철학에서 벗어나 있다는 비판을 받기도 한다.

리플(Ripple/XRP)은 금융기관을 대상으로 하고 국경 간 지급을 용이하게 하는 블록체인 기반 솔루션을 제공하기 위해 고안된 프로젝트이다. 리플은 프로젝트를 실현하기 위해 규제기관 및 중앙은행과 협력하고 있다. 국경 간 송금 시에 게이트웨이 중개를 통해 거래를 완성하지만, 신용을 제공하지 않는다. 리플의 합의 메커니즘은 채굴 작업 없이 이뤄지며, 노드가 8개에 불과하다. 리플의 토큰인 XRP 발행량은 1,000억이나 전적으로 리플 운영사의 소관이다. 리플은 중앙집권적에 머물러 있다는 비판을 받는다. 시가총액은 2017년 8월 현재 $75억 7천만으로 4위를 차지하고 있다.

스텔라(Stellar Lumens/XLM)는 2014년 리플의 포크(분기)로 시작되었다. 2017년 8월 현재 시가총액은 $2억 3천만으로 34위를 차지하고 있다.

하이퍼렛저(Hyperledger/XRP)는 비즈니스 운영을 위한 블록체인 플랫폼을 개발하기 위해 만들어진 리눅스 재단 중심의 오픈소스 프로젝트이다. 오픈소스 방식으로 플랫폼 기술개발을 추진하되 회원을 중심으로 운영되는 각종 위원회를 통해 프로젝트 운영 정책과 블록체인 기술발전 방향을 논의하고 수립한다. 현재 IBM, Accenture, Digital Asset Holdings 등의 IT 기업과 JP Morgan, Moscow Exchange, 미국 예탁결제기구인 DTCC 등 글로벌 금융기관이 참여하며 활동하고 있다.

플랫폼 기술 (Platform Technology)

블록체인에 있어 플랫폼 기술은 암호와통화 기술을 플랫폼화해 다른 분야에 적용하는 방법을 모색하는 기술이다. 분산 네트워크 상에서 완벽한 애플리케이션의 개발과 실행을 위한 플랫폼 개발이 주된 목표다. 주요 암호화 화폐로는 이더리움이 있다. 이더리움에 대해서는 다음 장에서 자세히 설명한다.

탈중앙애플리케이션 (DApp/Decentralized Applications)과 탈중앙자율조직 (DAO/Decentralized Autonomous Organization)

이더리움과 같은 플랫폼 기술은 무한확장이 가능한 프로그래밍 수준에까지 활용될 수 있도록 프로그래밍이 가능하다. 따라서 이를 이용한 스마트 계약이 최대한도로 사용될 경우 계약에 의해 실행되는 비즈니스 모델이 탄생할 수 있다. 이 프로그래밍 기능을 이용해 애플리케이션을 개발하는 것을 DApp라고 부르고, 현재 수백개의 DApp이 개발되어 사용되고 있다.

스마트계약에 의한 애플리케이션은 기업운영의 형태까지도 띌 수 있는데, 이를 탈중앙자율조직(DAO)이라고 부른다. 이는 법적으로 이전에는 존재하지 않았던 새로운 사업모델의 형태로 이것이 유한책임을 갖는지, 무한책임을 갖는지조차 불분명하다.

탈중앙자율조직의 첫 번째 사례는 더다오라는 그룹으로 투자자가 직접 운영하는 크라우딩 펀딩을 통한 벤처캐피털 펀드를 지향하고 2016년 5월 펀드모집을 했다. 더다오(TheDAO)는 이더리움 블록체인을 이용한 다수의 계약을 통해 존재하는 조직이라는 점에서 어느 국가에도 속해 있는 사업조직이었다. 더다오는 "프로젝트에 펀드를 나눠주는 허브 역할'을 하려고 했다. 즉, 더다오는 토큰을 투자자들에게 판매하고 거기서 만들어진 펀드를 투표를 통해 벤처투자를 하려고 했다. 더다오는 완벽하게 투명할 수 있도록 펀드매니저와 펀드디렉터를 없애고 투자자가 직접 벤처투자에 관여하도록 한 것이다. 더다오는 모든 것이 투명할 뿐만 아니라 모든 것이 프로그램 코드에 의해 운영되도록 했다. 누구나 자세한 내용을 들여다 볼 수 있게 했으나, 2016년 6월 운영이 종료되었다. 다오 토큰의 환급 과정에서 해킹이 발생했고, 이더리움과 이더리움 클래식이 하드 포크된다.

블록체인 2.0, 블록체인의 '안드로이드' 이더리움

이더리움 창시자, 비탈릭 부테린 "우리는 가상화폐계의 안드로이드가 되길 원한다."

이제 이더리움에 대해 알아보자. 이더리움을 창시한 비탈릭 부테린은 현재 23세의 청년이다. (MS의 빌 게이츠, 애플의 스티브 잡스, 페이스북의 마크 주커버그도 IT 창업 시 모두 청년이었다.) 그는 러시아계 캐나다인으로 경제에 관심이 많은 프로그래머였다고 한다. 비탈릭은 비트코인 진영에서 일하고 있었고 2014년 테크놀로지 부분에서 노벨상으로 불리는 월드 테크놀로지 어워드 IT 소프트웨어 부분에서 마크 주커버그를 제치고 수상해서 유명하다. 지금은 물론 이더리움의 리더로서 더욱 유명하다.

[도표 32] 이더리움의 창시자 비탈릭 부테린 소개

이름	비탈릭 부테린 (Vitalik Buterin)
출생 국적 학력	1994 년 1 월 31 일(23 세) 러시아, 캐나다 워털루 대학교 1 학년 중퇴
수상	2012 년 국제올림피아드 정보부문 동메달 2014 년 월드 테크놀로지 어워드 IT 소프트웨어 수상 (경쟁후보 페이스북 창업자 마크 주커버그)
경력	비트코인 관련 블로그를 위한 기사집필 2011 년 <비트코인 매거진> 초대 창간 논문심사 학술지 <레저> 편집국 2013 년 이더리움 백서 발표 2014 년 이더리움 재단 클라우드 펀딩으로 설립
웹사이트	https://about.me/vitalik_buterin

자료: 위키디피아

비탈릭 부테린은 비트코인의 분권화된 신뢰 프로토콜에 매료되어 비트코인에 대한 글을 썼고 비트코인 진영에서 일하기도 했다. 그러나 비트코인의 핵심 프로토콜은 소프트웨어 개발자가 '강력하면서 사용자 친화적인 API (Application Programming Interface)를 만들기에 너무 까다롭다고 생각했다. 프로그래밍 언어로 작성된 모든 종류의 응용 프로그램을 지원하는 완전히 독립적인 프로토콜과 블록체인을 구축하는 경우를 개발자들은 튜링 완전성(Turing Complete)이라고 말한다.

어떠한 종류의 분산된 서비스(통화거래 시스템, 스마트계약, 주주명부 등록, 의결권 시스템, DApps, DACs, DAOs 등)도 지원할 수 있고, 개발자들이 시장이 필요하다고 생각하고 인터페이스를 구성할 수 있게 한다면 그가 생각해낸 솔루션은 모든 형태의 계약과 분산된 애플리케이션을 설치할 수 있는 개방형 플랫폼으로 기능하는 완벽하게 재설계된 대용도의 분산형 블록체인이었고, 그는 이것을 이더리움이라고 불렀다. 비탈릭 부테린은 "우리는 가상화폐계의 안드로이드가 되기를 희망한다."며 이더리움 프로젝트에 착수했다. (비트코인 현상, 블록체인 2.0/마이클 J. 케이시, 폴 비냐 저/미래의 창)

이더리움은 비트코인의 한계를 극복하면서 블록체인 기능을 향상

비탈릭 부테린에 의해 만들어진 이더리움에 대해 가장 잘 이해하는 방법은 비트코인과의 비교다. 비트코인은 암호화 화폐 체계인데 반해 이더리움은 암호화 화폐 체계에 스마트 계약 기능이 더해진 것이다. 프로그램 언어는 비트코인은 스크립트, 이더리움은 튜링완전 언어이다. 블록체인 체계의 핵심은 합의 메커니즘은 비트코인은 작업증명이며, 블록체인은 작업증명에서 자산증명으로 전환의 목표를 갖고 있다. 블록생성 시간은 비트코인 10분에 비해 이더리움은 15초로 빠르며 이에 따라 초당 거래개수의 차이가 있다. 비트코인 발행량은 2040년까지 2,100만 비트로 한정된 반면, 이더리움은 매년 1,800만 이더가 발행된다. 이더리움은 Dapp과 Smart Contract 기능이 더해졌다.

[도표 33] 비트코인과 이더리움의 비교

	비트코인 (Bitcoin)	이더리움 (Ethereum)
핵심 개념	암호화 화폐	암호화 화폐+스마트 계약
설립자	사토시 나카모토 (Satoshi Nakamoto)	비탈릭 부테린 (Vitalik Buterin)
출시 년도	2009 년 1 월	2014 년 7 월
언어	스크립트 언어*	튜링 완전한 언어 (Solidity, Serpent, LLL)**
합의 메커니즘	작업증명 (PoW : Proof of Work : 채굴 노드)	현재 : GPU 채굴 기반 작업증명, 목표 : 자산증명 (PoS : Proof of Stake : 이더리움을 보유한 노드만 노드로 인정)
블록생성 시간	약 10 분	약 15 초 (PoS 로 전환되면 3~4 초 가량으로 낮아짐, Dapp 실행속도 향상)
초당 거래건수	2.7 건	15 건
노드 수	6,181 (변동함)	22,008 (변동함)
최대 발행	2040 년 2100 만개로 제한	매년 1,800 만 이더리움 발행, 최초발행 프리세일 코인의 25%이며 전체 통화량 대비 발행량은 매년 하락. 이더리움 소유자의 죽음 및 손실 분을 감안하면 1 억 개 정도로 평형상태를 이룰 것으로 예상
추가 기능		Dapp(Decentralized Application/분권화 애플리케이션), Smart Contract(지능형 계약)

자료: 교보증권 리서치센터 정리 주: * 스크립트 언어: 컴파일하지 않고, 작성해서 바로 실행할 수 있는 언어로 개발자가 지정한 몇몇 행동만을 프로그램화할 수 있음. ** 튜링 완전한 언어: 모든 수학문제를 풀 수 있는 일반적인 알고리즘을 만들어낼 수 있는 언어로 개발자가 원하는 모든 행동을 프로그램화할 수 있음

이더리움은 비탈릭 부테린이 비트코인의 한계 1) 스크립트 언어의 단점, 2) 비효율적, 중앙 집권화될 수 있는 합의 메커니즘, 3) 늦은 거래처리속도, 4) 의사결정 구조의 불안정성을 인식하고 이를 개선하는 방향으로 구현되었다. 비탈릭 부테린이 이러한 비전을 갖고 백서를 발표했을 때, 많은 암호학 전문가와 엔지니어들이 공감했다고 한다.

[도표 34] 비탈릭 부테린에 의해 지적된 비트코인의 한계

비트코인의 문제점	지적 및 내용
비트코인 스크립트 언어의 단점	비탈릭 부테린에 의해 주로 지적
튜링 불완전성 (Turing-incomplentness)	언어가 단순해서 화폐 거래정보만 처리 가능
Value-blindness	가치의 분리가 불가능
Lack of state	상태, 조건 및 계약의 저장이 불가능
작업증명 방식의 합의 메커니즘	비트코인 상에서 문제가 발견
지나치게 큰 에너지 소모	고도화 채굴장비 합의 메커니즘 비효율
채굴자들의 중앙화	거버넌스 문제점 발생
늦은 거래처리속도	10 분당 1MB 밖에 처리가 안 됨, 확장성 문제
의사결정 구조	UAHF, 세그윗, 하드포크 등 의사결정 구조 문제

자료: http://www.youtobe.com/watch?v=uUC3hELa-Oo

[도표 35] 이더리움 백서 결론 및 요약

A Next-Generation Smart Contract and Decentralized Application Platform
(차세대 스마트 컨트랙트와 탈중앙화된 어플리케이션 플랫폼)

Ethereum (이더리움)

Writtren by Vitalik Buterin (비탈릭 부테린)

Satosh Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultanneously has no baking or "intrinsic value" and no centralized issuer or controller. However, another, arguably more important, part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcion.

Commonly cited alternative applications if blockchain technology include using on-blockchain digital assets to represent custom currencies and financail instruments ("colored coins"), the ownership of an underlying physical device ("smart property"), non-fungibla assets such as being directly controlled by a piece of code implementing arbitrary rules ("smart contracts") or even blockchain-based "decentralized autonomous organizations" (DAOs).

What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitary state transition fuctions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

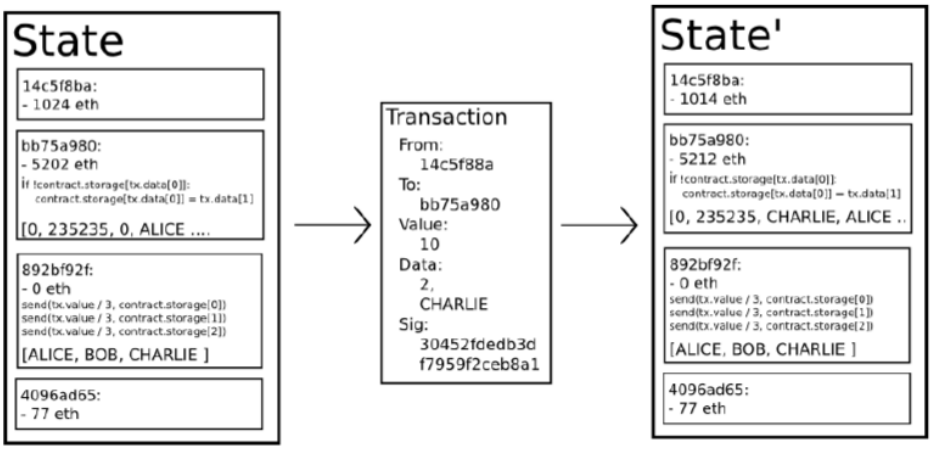
사토시 나카모토에 의해 2009 년 개발된 비트코인은 종종 화폐와 통화분야에서 매우 근본적인 혁신으로 묘사되어 왔는데, 이것은 비트코인이 어떤 담보나 내재적인 가치를 가지지 않으며, 중앙화된 발행기관이나 통제기관도 없는 디지털 자산의 첫 번째 사례였기 때문이다. 하지만 비트코인 실험의 더욱 중요한 측면은 비트코인을 떠받치고 있는 분산 합의 수단으로서의 블록체인 기술이며, 이에 대한 관심이 급격하게 늘어나고 있다.

블록체인 기술을 이용한 대안적 어플리케이션들에는 다음과 같은 것들이 자주 거론되고 있다. 사용자 정의 화폐와 금융상품을 블록체인 위에 표현하는 컬러드 코인("colerd coins"), 물리적 대상의 소유권을 표현하는 스마트 자산("smart property"), 도메인 이름과 같은 비동질적 자산을 기록하는 네임코인("namecoin"), 임의적인 계약규칙을 구현한 코드에 의해 디지털 자산을 관리하는 좀 더 복잡한 형태의 스마트 컨트랙트("smart contracts"), 더 나아가 블록체인을 기반으로 한 탈중앙화된 자율 조직("decentalized autonomous organization", DAOs) 등이다.

이더리움이 제공하려는 것은 완벽한 튜링완전(turing-complete) 프로그래밍 언어가 심어진 블록체인이다. 이 프로그래밍 언어는, 코딩된 규칙에 따라 '어떤 상태"를 다르게 변화시키는 기능(arbitary state transition functions)이 포함된 "계약(contracts)"을 유저들이 작성할 수 있게 함으로써 앞서 설명한 시스템들을 구현 가능하게 할 뿐만 아니라 우리가 아직 상상하지 못 한 다른 많은 어플리케이션들도 매우 쉽게 만들 수 있도록 도와줄 것이다.

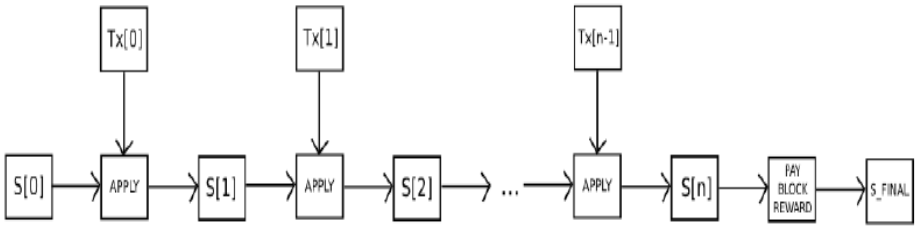
자료: 「A Next-Generation Smart Contract and Decentralized Application Platform」

[도표 36] 이더리움 상태 변환 함수



자료: 「A Next-Generation Smart Contract and Decentralized Application Platform」

[도표 37] 이더리움 블록체인과 채굴 과정



자료: 「A Next-Generation Smart Contract and Decentralized Application Platform」

이더리움의 기능, 비트코인을 뛰어 넘어 블록체인 상 할 수 있는 모든 기반을 제공

이더리움은 스마트 계약을 실행시키고 분산화된 애플리케이션을 지원할 수 있다. 이더리움을 지원하는 튜링완전 언어는 계약조건을 넣고, 이 조건이 충족되면 자동적으로 실행시킬 수 있다. 예를 들어 자동차를 할부로 샀을 때, 연체가 되었을 경우 시동이 안 걸리게 할 수 있는 프로그래밍 등이다. 분산화된 애플리케이션이란 중앙 서버 없이 이더리움 블록체인 지원을 받아 비즈니스 및 거래활동이 구현되는 것이다. 기업가와 개발자가 진입장벽이나 거래 및 고정비용 없는 스타트 업 기회를 확보한다.

[도표 38] 이더리움의 구성 및 기능

특징	내용
이더리움	블록체인 기반의 분산 컴퓨팅(distributed computing) 플랫폼 튜링 완전한 프로그래밍 언어를 내장하고 있어 스마트 계약과 분산 애플리케이션을 구현할 수 있음 예) A 가 B 에게 5BTC 를 보냄(비트코인) vs 2017 년 7 월 이전에 B 의 잔고가 10ETH 이하인 경우에만 A 가 B 에게 5ETH 를 보냄(이더리움) 2013 년 말, 비탈릭 부테린에 의해 처음 제안되었으며 2014 년 7 월 크라우드 세일을 진행한 후 7 월 말 초기버전인 Frontier 를 출시
스마트 계약	온라인 상에서 특정계약 조건을 실행 스마트 계약이 코드로서 블록체인 위에 기록되기 때문에 누구도 처음에 명시된 조건 이외의 경우 계약조건을 바꿀 수 없음 특정 조건을 만족시키는 경우에는 계약의 내용이 1) 자동적으로, 2) 무조건 실행
분산 어플리케이션	중앙중개 기관 없이 다양한 종류의 서비스를 사용자들에게 제공하는 어플리케이션 금융, 신원관리, SNS, 의료, 예술, 정부행정 등 다양한 분야에 걸쳐 중앙중개 기관을 통한 서비스 제공 대신 탈중앙화된 분산 어플리케이션을 통해 보다 효율적이고 안전한 서비스 제공 기존 어플리케이션의 백엔드 코드가 중앙서버에서 실행된다면 분산 어플리케이션의 백엔드 코드가 분산화된 P2P 네트워크에서 실행
이더리움 가상머신	모든 참가자(node)들의 컴퓨터에서 동일한 연산을 수행하며 이를 통해 동일한 상태(state)에 합의 전세계 모든 참가자가 동일한 하나의 컴퓨터를 돌리는 것과 같기 때문에 "세계 컴퓨터(world computer)"라 불리기도 함 각각의 노드는 이더리움 가상머신(EVM)을 통해 동일한 연산을 수행. 이더리움 가상머신은 스마트 계약이 실행될 수 있는 런타임 환경을 제공

자료: http://www.youtobe.com/watch?v=uUC3hELa-Oo

이더리움은 블록체인을 하나의 데이터베이스로 보고, 모든 자산을 올릴 수 있고, 각 자산이 구동하거나 거래되는 방식까지 직접 프로그래밍할 수 있는 하나의 '개방 플랫폼(Open Platform)으로 설계되었다. 블록체인 관련 업계나 인물들의 경우 이더리움의 이러한 다양한 가치창출 확장성으로 인해 '블록체인 2.0'이라고 표현하고 있다.

우리는 다음 장에서 Dapp(Decentralized Application)과 ICO(Initial Coin Offering)에 대해서 살펴볼 것이다. 이는 블록체인 상에서 (특히 이더리움 기반의) 비즈니스가 구현되고 이에 따라 가치가 창출되고, 암호화 화폐가 회전하면서 새로운 형태의 산업 생태계가 조성되고, 디지털 경제에서 부의 창출, 이전, 분배되는 새로운 현상이 될 것이다.

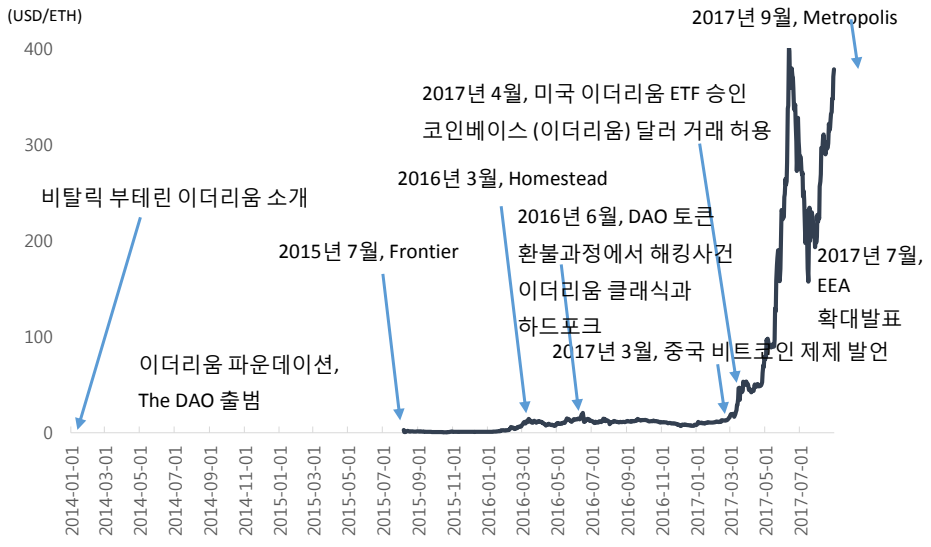
이더리움의 역사, 역시 다섯 국면으로 구분될 것

비탈릭 부테린이 비트코인 혁신을 목표로 백서를 발표하고, 2015년 7월 이더 프리세일로 이더리움이 나온 이후 현재까지 이더리움은 3 단계로 구분된다.

Frontier (2015년 7월~2016년 3월): 이더리움의 기초 형태로 이더 채굴, 교환이 시작되고 이더리움 블록체인 상에서 Dapp을 업로드 및 테스트할 수 있는 시기로 당시 이더리움 가격은 $0.5~2 사이에서 형성되었다.

Homestead (2016년 3월~2017년 9월): 이더리움 블록체인이 안정적인 단계이며, 이더리움이 주요 프로젝트들이 구현되는 시기이다. 이 기간 동안에는 The DAO가 해산 시 토큰이 환불되는 과정에서 해킹이 발생되어 이더리움이 도난되는 사고가 발생한다. 이때 이더리움이 본래의 이더리움과 하드 포크된다. 도난된 이더리움은 이더리움 클래식으로 분기된다. 2017년 3월 중국이 비트코인 제제발언, 4월 미국이 이더리움 ETF 승인 및 달러거래 허용으로 이더리움 가격은 $10대에서 2017년 6월 12일 $401.5까지 급등한다. 6~7월 암호화 화폐의 동반 급락세를 보였다. 2017년 7월 EEA(Enterprise Ethereum Alliance)가 확대 발표되면서 이더리움 가격은 전고점을 회복 중이다.

[도표 39] 이더리움 가격과 이벤트 정리



자료: Coinmarketcap, 교보증권 리서치센터

Metropolis (2017년 9월~): 이더리움 블록체인 기술의 대중화 단계로 2017년 9월에 시작해 약 1~2년 정도의 시간이 소요될 것으로 예상되고 있다. 메트로폴리스 단계에서는 이더리움을 활용한 대중적 Dapp을 지원할 수 있도록 다양한 기능이 포함된다. 또한 채굴방식에 있어 작업증명(PoW)와 자산증명(PoS)가 병행된다.

Serenity: 이더리움의 마지막 단계로 네트워크 신뢰를 위한 채굴과정이 에너지 낭비가 심한 작업증명(PoW)을 자산증명(PoS)으로 완전히 전환한다. 작업증명(PoW)은 많은 컴퓨팅 파워를 필요로 하기 때문에 과도한 전력과 계산력이 필요하다. 자산증명(PoS)의 채굴방식에서는 거래소에 이더를 보관 중인 일반 거래자들도 채굴 수수료를 뺀 일정 이자를 이자(배당으로) 지급받을 수 있게 된다.

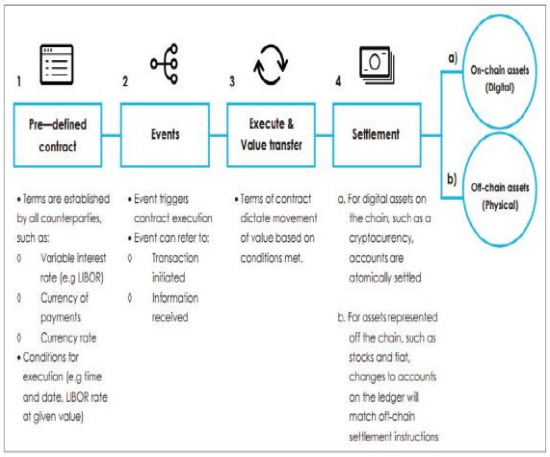
Serenity 이후: 이더리움 블록체인이 완전히 안전성을 자리잡은 이후, 기술 업데이트 및 거버넌스 유지를 위한 합의 기능을 한 이더리움 파운데이션은 해산한다. 이더리움 블록체인은 현재 인터넷의 월드 와이드 웹(World Wide Web)처럼 월드 와이드 네트워크(World Wide Network)로 작용하며 일반인들이 아무런 의식 없이 사용하게 된다.

[도표 40] 이더리움의 발전 단계, 현재는 Homestead 단계, 9 월 곧 Metropolis 진입

단계	명칭	상황
1 단계	Frontier (2015 년 7 월)	이더리움의 가장 기초적인 형태로서 커멘드 라인 인터페이스를 통해 이더 계약을 업로드하고 실행시킬 수 있음. 채굴자들은 채굴을 시작. 거래소에서 이더 거래 가능. 분산 어플리케이션(dapp)을 테스트할 수 있고 이더를 구입하여 자신의 소프트웨어를 이더리움에 업로드 가능
2 단계	Homestead (2016 년 3 월)	프론티어의 가장 광범위한 테스트가 끝나고 코어 개발자들이 안정적이고 안전하다고 판단될 때 시작. 홈스테드 단계의 이더리움은 "안전하다"고 판단될 수 있음. 2 단계까지는 이더리움의 베타(beta) 버전으로서 이더리움의 주요 프로젝트들이 처음 개발 및 구현
3 단계	Metropolis (2017 년 9 월)	기술을 모르는 일반일들도 사용할 수 있는 공식 인터페이스가 출시. Mist 및 분산 어플리케이션 스토어 출시. 이더리움 네트워크 위에서 다양한 프로그램들이 제대로 작동하게 되며 강력한 생태계를 갖춰가기 시작
4 단계	Serenity	이더리움의 마지막 단계로서 에너지 낭비가 심한 작업증명을 자산증명으로 전환. 네트워크의 확장성(scalability)이 개선되어 처리속도가 빠르고 효율적이 되며 초보자들도 사용하기 쉬운 단계. 채굴을 없애더라도 안정적인 네트워크 확보

자료: http://www.youtobe.com/watch?v=uUC3hELa-Oo

[도표 41] 스마트 계약의 구조



자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」 2016년 공동연구

[도표 42] EEA 초기 참여 기업, 현재에는 참여 더욱 확대

자료: EEA (Enterprise Ethereum Alliance)

블록체인에 의한 새로운 부의 창출: ICO와 DAPP

복싱 챔피언 메이웨더, 블록체인 ICO 홍보, '토큰판매', '자금모집'

복싱 챔피언 플로이드 메이웨더 주니어는 지난 달 자신의 인스타그램을 통해 ICO를 홍보해 큰 파장을 일으켰다. 그런 그가 트위터에 두 번째로 자신의 ICO에 대해 홍보했다. 블록체인 기반 Contents 시장을 개발 중인 후비 네트워크에 대한 메이워더의 홍보는 메이웨더가 이번 주 코너 맥그리거와의 복싱 경기 몇 일 전에 이루어졌다.

메시지에서 그는 자신을 "플로이드 크립토"라 자칭하며 #크립토미디어그룹이란 해시태그를 사용해 지속적인 홍보 노력을 기울였다. 메이웨더의 대변인은 이메일을 통한 의견요청에 즉시 응답하지 않고 있는 상황이다. 코인데스크에 보고된 바와 같이 이번 일을 메이웨더의 암호화폐 시장에 대한 첫 번째 진출시도가 아니다. 7월 말 경, 메이웨더는 인스타그램을 통해 스톡스 토큰판매에 대한 홍보를 했으며 스톡스는 토큰 판매로 3,000만 달러 이상을 모금했다. (날짜 2017년 8월 23일, 출처 Finextra, 옮긴이 제5기 핀테크지원센터 Univ. Fintecher 유진환 기자)

메이웨더는 블록체인 기반의 스톡스와 후비 네트워크 ICO에 대해 홍보했다고 한다. 메이웨더가 홍보한 블록체인 기반의 '스톡스', '후비 네트워크', '그리고 'ICO'는 무엇일까?

[도표 43] 플로이드 메이워더, 트위터에 두 번째 ICO 홍보하다

자료: 핀테크 지원센터 기사

IPO (Initial Public Offering)과 ICO (Initial Coin Offering)

ICO는 Initial Coin Offering의 약자로 '코인공개상장'으로 해석된다. ICO을 이해하기 전에 이미 우리에게 익숙한 개념인 IPO부터 되짚어 보자.

IPO는 Initial Public Offering의 약자로 '주식공개상장'으로 해석된다. IPO는 기업이 최초로 외부투자자에게 주식을 공개 매각하기 위해 증권거래소에 처음 상장하는 것을 말한다. ICO는 블록체인 기반에서 기업, 또는 개인이 최초로 외부투자자에게 자신이 발행한 코인을 공개 매각하는 과정이다. 이 때 투자자는 ICO 발행 코인을 받는 대신 비트코인, 혹은 이더리움과 같은 암호화폐를 지불하게 된다.

ICO와 IPO를 비교하면, 공통점은 비즈니스 기회를 공개하고, 투자자금을 유치한다는 점이다. ICO에서는 코인(암호화폐)를 발행하고, IPO는 주식을 발행하며, ICO는 비트코인, 이더리움 등 역시 암호화폐로 코인공개에 참여하고, IPO는 법정화폐로 주식공개에 참여하게 된다. 비즈니스에 대한 수익배분 기회를 공유하게 되는 구조는 유사하다.

ICO와 IPO의 근본적인 차이는 바로 블록체인과 암호화폐의 거래 체계 그 자체다. IPO는 거래 중개인이 연결된다. 따라서 아무리 좋은 기업공개가 있다고 하더라도 실제적으로 참여가능여부가 제한된다. 또한 중개인이 받는 수수료도 존재한다. 블록체인 상에서 ICO는 중개인 없이 코인 발행자와 투자자가 직접 연결되는 크라우드 펀딩 시스템이다. 따라서 블록체인 상에서 ICO 리스트를 보고 누구나 소액으로 참여할 수 있다.

ICO의 개념을 이해하기 위해서 IPO와 비교했지만, ICO는 비즈니스의 초기 국면인 스타트업의 자본구성과 유사한 절차로 보여진다. 스타트업 초기 당장 수익을 내기는 쉽지 않으므로, 투자비용은 대출보다는 자본이 안전하다. 기업이 수익을 내고 성장해 나가면서 대출을 쓰고 더욱 확장해서 일정 궤도에 오르면 IPO에 나서는 것이 일반적이다. ICO는 자체 코인 발행 후 공개매각하기 때문에 부채가 없는 상태에서 진행된다. 물론 ICO와 스타트업 자금모집에 있어서도 결국 블록체인 유무의 근본적 차이가 있다.

[도표 44] ICO 와 IPO 및 Start Up 자본구성의 비교

	ICO	IPO	Start Up
발행주체	블록체인, 암호화폐 체계의 기업가	현재 기업가	현재 기업가
투자자	블록체인, 암호화폐 체계의 투자자, 크라우딩	사모 및 공모	사모 및 크라우딩
중개인	없음	있음	있음
비즈니스	블록체인, 암호화폐 기반의 서비스 및 기술	재화, 서비스 및 기술	재화, 서비스 및 기술
발행	각자 코인	주식	주식
투자자금	암호화 화폐	법정 화폐	법정 화폐
재무상태	100% 자본	자본+부채	주로 자본
수익배분	비즈니스 가치에 따른 토큰가치 상승, 배당	주가상승, 이자, 배당	주가상승, 이자, 배당
수익배분 신뢰	대체로 백서(White Paper)에 기술	경영활동 및 주주총회 확정	경영활동 및 주주총회 확정

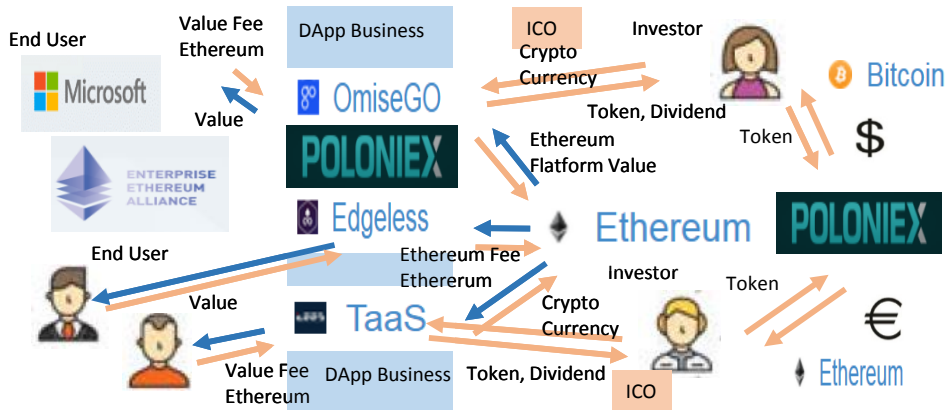
자료: 교보증권 리서치센터

ICO는 블록체인 상에서 비즈니스 기회와 암호화폐 유통 기능을 제공

블록체인 암호화폐 체계에서 ICO는 비즈니스 창출, 가치와 암호화폐 유통, 그리고 법정화폐로의 순환을 이끈다는 측면에서 아주 중요하다.

블록체인 세계에서 경제주체는 사용자, 기업가, 투자자이며 현재 실물경제와 비교하면 중개인이 없을 뿐 같다. 기업가와 개발자는 ICO를 통해 가치를 창출하며 투자자도 이에 참여한다. 이때 화폐거래는 암호화 화폐를 통해 이뤄진다. 또한 사용자는 블록체인 서비스를 제공받고 암호화폐를 지불한다. 특히 이더리움은 블록체인에서 다양한 비즈니스 기회를 주며, 이더리움 블록체인을 기반으로 비즈니스를 운영하는 기업은 이더리움 사용료를 내게 된다. 기업은 가치를 창출하고 이더리움을 받는 대신, 자신의 토큰을 갖고 있는 투자자와 이더리움 전체를 소유한 개인에게 사용료를 낸다. 이더리움 순환체계를 만들게 되며, 암호화폐 거래소를 통해 법정화폐 교환도 이뤄진다.

[도표 45] 블록체인 암호화폐와 ICO 발행토큰이 유통되는 과정



자료: 교보증권 리서치센터

ICO는 리턴, 리스크 큰 투자. 블록체인 체계, 사업 전망 및 개발자 신뢰도 필요

ICO는 블록체인 암호화폐 체계에서 100% 자기자본으로 비즈니스가 시행된다. 당연히 담보가치가 없으며, 비즈니스가 무산되면 해당 토큰의 가치는 급격히 하락하게 될 것이다. 블록체인 체계에서 좋은 비즈니스를 하고 성공을 거둔다면 그 가치가 토큰 보유자에게 그 가치가 돌아가지면, 신뢰되지 않고, 실패한다면 리스크도 크다. 특히 제3자 중개인이 없는 만큼 비즈니스 공개와 토큰발행의 진입장벽이 낮으므로 그만큼 사기도 많을 수 있다. ICO 투자에 있어서는 블록체인 체계를 잘 이해하고 ICO 백서 내용에 담긴 비즈니스 계획 및 전망, 토큰발행 및 배당계획과 개발자에 대한 신뢰도 필요하다.

[도표 46] Block Chain Crypto Currency

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$80,046,216,774	$4840.15	16,537,962 BTC	$2,507,220,000	2.82%	
2	Ethereum	$36,513,911,888	$386.90	94,374,360 ETH	$860,628,000	0.96%	
3	Bitcoin Cash	$10,288,819,557	$621.47	16,555,538 BCH	$384,878,000	5.64%	
4	Ripple	$9,570,009,433	$0.249584	38,343,841,883 XRP *	$365,545,000	0.21%	
5	Litecoin	$4,530,285,628	$85.90	52,738,757 LTC	$1,513,610,000	20.84%	
6	NEM	$2,958,885,000	$0.328765	8,999,999,999 XEM *	$12,298,300	-2.75%	
7	Dash	$2,927,789,685	$388.94	7,527,593 DASH	$53,315,100	2.51%	
8	IOTA	$2,199,864,802	$0.791452	2,779,530,283 MIOTA *	$27,611,500	-6.92%	
9	Monero	$2,151,003,968	$143.19	15,022,026 XMR	$161,735,000	1.76%	
10	Ethereum Classic	$2,040,913,924	$21.46	95,105,381 ETC	$740,713,000	32.67%	

자료: Coinmarketcap 주: 2017년 9월 2일 기준

[도표 47] Block Chain Asset (Decentralized Application)

#	Name	Platform	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	OmiseGO	Ethereum	$1,174,877,843	$11.95	98,312,024	$91,545,000	0.05%	2.05%	45.68%
2	Qtum	Ethereum	$1,036,683,100	$17.57	59,000,000	$65,800,600	0.33%	1.53%	32.70%
3	TenX	Ethereum	$418,555,231	$4.00	104,661,310	$19,356,900	-0.73%	-5.73%	14.51%
4	EOS	Ethereum	$414,831,873	$1.29	320,908,402	$26,261,100	1.06%	0.58%	-6.38%
5	Tether	Omni	$320,891,295	$1.00	319,498,283	$193,309,000	-0.17%	0.09%	0.17%
6	MaidSafeCoin	Omni	$313,249,086	$0.692183	452,552,412	$3,272,230	-0.07%	3.64%	28.37%
7	Augur	Ethereum	$308,463,100	$28.04	11,000,000	$3,360,890	-0.61%	6.59%	8.84%
8	Golem	Ethereum	$305,203,765	$0.366377	833,032,000	$3,772,110	3.31%	9.53%	23.38%
9	Iconomi	Ethereum	$302,760,997	$3.03	99,900,350	$3,761,070	-1.77%	20.26%	12.72%
10	Basic Attenti...	Ethereum	$285,102,000	$0.285102	1,000,000,000	$9,225,020	0.98%	2.33%	34.29%
11	Metal	Ethereum	$247,066,234	$12.80	19,300,994	$11,472,900	1.81%	31.61%	32.18%
12	Binance Coin	Ethereum	$217,734,000	$2.18	100,000,000	$18,432,000	-1.17%	-1.75%	-12.92%
13	Gnosis	Ethereum	$203,537,276	$184.26	1,104,590	$1,095,210	-0.29%	3.86%	16.16%
14	DigixDAO	Ethereum	$192,611,200	$96.31	2,000,000	$861,532	-0.63%	-2.25%	0.19%
15	0x	Ethereum	$186,572,500	$0.373145	500,000,000	$9,169,330	0.17%	3.79%	4.10%
16	Populous	Ethereum	$170,734,796	$4.14	41,252,246	$1,279,090	-13.54%	11.49%	-0.99%
17	Civic	Ethereum	$166,399,400	$0.489410	340,000,000	$4,961,240	0.62%	-8.67%	-2.91%
18	Status	Ethereum	$164,511,343	$0.047403	3,470,483,788	$7,384,140	-1.00%	-2.96%	-6.91%
19	Veritaseum	Ethereum	$161,252,156	$80.18	2,011,134	$973,754	4.83%	-13.10%	-31.97%
20	MCAP	Ethereum	$149,244,526	$1.66	89,866,280	$951,675	1.47%	9.39%	-0.35%

자료: Coinmarketcap 주: 2017년 9월 2일 기준

블록체인 암호화폐의 화폐적 시각

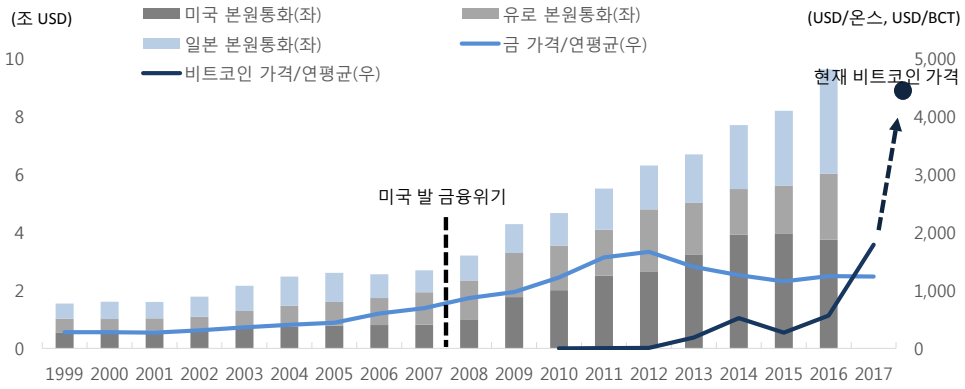
화폐가치 하락, 더 구체적으로 말하면 화폐의 구매력 하락의 문제

블록체인을 구현한 비트코인은 사토시 나카모토에 의해 2008년 10월에 세상에 공개되었고 2010년부터 거래되기 시작했다. 이는 2008년 9월 글로벌 금융위기 이후다.

글로벌 금융위기, 경기침체 이후 미국, 유럽, 일본 등 선진국 중앙은행은 제로금리, 마이너스 수신금리, 수 차례의 걸친 양적 완화를 전개하고 있다. 이에 따라 각국 본원통화는 급격히 늘었고, 금리도 장기간 낮은 탓에 달러를 비롯한 법정화폐의 구매력을 하락하고 있다. 인플레이션은 발생하고 있지 않지만 자산버블이 발생하고 있고, 이것이 과잉 유동성이 유입된 결과인 것을 부정할 이는 없을 것이다. 이러한 부정적 현상에도 불구하고 과잉부채 상태에 있어 팽창된 통화팽창이 빨리 거둬지기도 어렵다.

법정화폐의 구매력 하락은 1) 기존 자산버블과 함께 2) 금 등 안전자산의 재인식, 그리고, 3) 비트코인 등 암호화폐의 부상을 야기하고 있는 것으로 보인다.

[도표 48] 2008~2009 년 미국 발 금융위기 이후 본원통화 급증, 이후 금과 비트코인의 순차적 상승



자료: Bloomberg, 교보증권 리서치센터 주: 각국 본원통화는 연평균 환율을 적용해 미국 달러로 환산

미국, 유로, 일본의 본원통화 합계와 금, 그리고 비트코인 가격을 보면 법정화폐의 구매력 하락에 따른 금 등 안전자산의 부상과 순차적인 암호화폐의 부상 현상을 볼 수 있다. 2008년 글로벌 금융위기 후 금 가격이 오르기 시작해고, 유로 재정위기로 인해 ECB가 양적 완화에 나서는 시점에 온스당 $1,800을 상회할 정도로 올랐다.

비트코인은 2010년 7월 $0.06로 거래되기 시작했고, 2013~2014년 급격히 올라 $800 이상으로 올랐다. 이 시기부터 금 가격은 장기적인 조정국면으로 진입하기 시작해 화폐가치가 보전되는 자산으로서 금의 위치를 서서히 비트코인이 차지하기 시작한 현상으로 볼 수 있다. 2014~2015년은 미국 경제가 비교적 안정되어 테이퍼링 등이 논의되면서 달러화가 일시 강세를 보였지만, 2016~2017년 비트코인은 다시 급등했다.

법정화폐 유통속도 하락, 신흥국은 과잉 레버리지로 역시 유통속도 하락

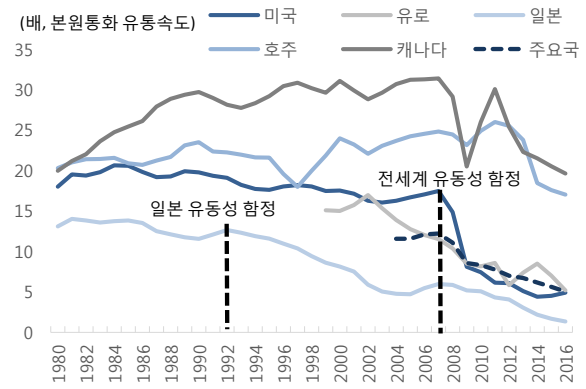
글로벌 경제는 유동성 함정에 빠져 있다고 한다. 유동성 함정이란 금리가 너무 낮아서 채권보다 현금이 오히려 선호되는 현상을 의미한다. 이는 경제활동에 있어 부가가치를 창출할 수 있는 대출이 약화되고 유동성이 잠기게 되는 상태를 의미하며 오래가면 불황으로 빠진다. 유동성 함정을 가장 잘 설명하는 지표는 화폐 유통속도다,

화폐 유통속도는 현금이 선호되면 떨어진다. (현금이 선호되는 데도 구매력이 떨어지면 정말 문제인데, 지금이 그렇다.) 미국, 유럽, 일본은 금융위기 이후 지난 10년간 엄청난 유동성을 풀었으므로 본원통화 유통속도가 역사적 최저치로 하락해 있다. 미국은 4.9배, 유로 5.2배, 일본 1.4배로 1992년 일본 장기불황 시기 때보다 현저히 낮다.

본원통화, 시중은행 예금 합계인 M1의 화폐 유통속도가 하락하는 것도 마찬가지다. 미국, 유로의 M1 유통속도는 각각 5.7배, 1.6배로 낮다. 일본은 M1을 통계를 내 놓지 않아 M2 유통속도를 보면 0.57배로 GDP의 175%에 달할 정도의 과잉 유동성이다. 그나마 미국의 M1 유통속도가 높지만 이는 경제활동이 활력적이기보다는 예금 자체가 적고, 금융위기 이후 은행들이 초과지준을 쌓는 등 레버리지를 늘리지 않은 결과다.

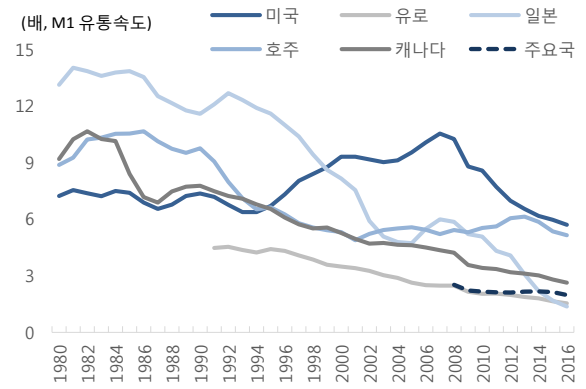
미국, 유로, 일본의 상황과 달리 캐나다, 호주 등은 양적 완화를 시행하지 않았다. 따라서 캐나다, 호주의 본원통화 유통속도는 각각 17.1배, 19.7배를 나타내고 있다. 역사적으로 볼 때 높지는 않지만 낮은 수치라고는 볼 수 없다. 다만 호주와 캐나다의 M1 유통속도는 5.2배, 2.6배로 역시 역사적으로 낮은 수준으로 하락하고 있다. 호주와 캐나다 입장에서는 미국, 유럽, 일본의 통화팽창 정책이 짜증이 날 만 하다. 자기들은 나름대로 통화관리를 잘 하고 있지만, B3의 통화팽창으로 자국 자산버블이 발생하고 있기 때문이다. 호주, 캐나다, 독일, 스위스 및 북유럽 국가들이 암호화폐 도입에 긍정적인 면을 보고 있는 점도 이해가 간다. 어쨌든 화폐유통속도 하락은 공통적인 현상이다.

[도표 49] 주요 선진국 본원통화 유통속도 하락



자료: Bloomberg, 교보증권 리서치센터 주: 화폐유통속도=명목GDP/통화량

[도표 50] 주요 선진국 M1 유통속도 하락

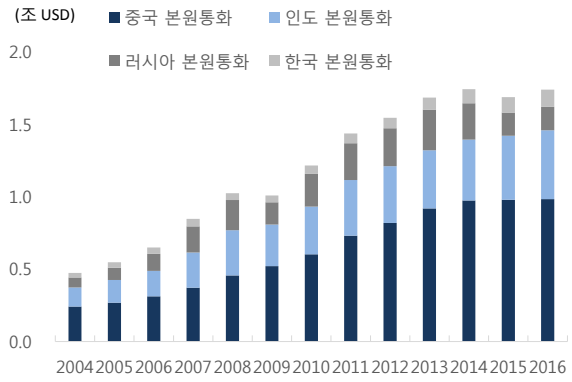


자료: Bloomberg, 교보증권 리서치센터 주: 일본은 M2

중국, 러시아, 인도, 한국 등 신흥국의 상황은 어떨까? 이들 신흥국의 상황은 대체로 호주, 캐나다와 비슷하다. 본원통화는 크게 증가하기 않았지만, M1 및 M2, 특히 중국의 경우가 크게 증가했다. 반면 금융위기 이후 잠재성장률이 하락하고 실질성장률도 하락하면서 본원통화 및 M2, M2 등 화폐유통속도는 역시 하락하고 있다.

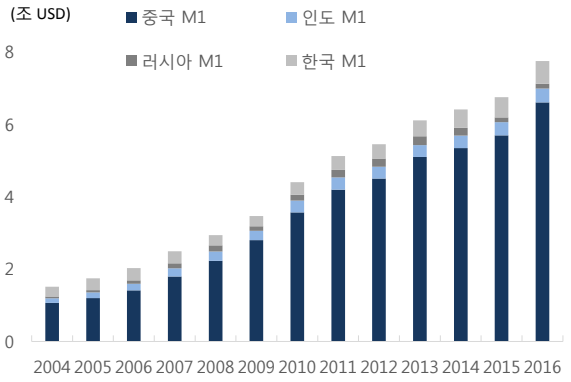
그럼에도 불구하고 화폐의 실질구매력은 하락, 자산버블은 발생하고 있다. 또한 신흥국간 경제성장에 밑거름이 되는 교역에 있어 글로벌 기축통화인 달러화에 대한 거래비용이 증가하고 있다. 상황이 좋을 때는 거래비용이 문제가 되지 않지만 지금처럼 상황이 좋지 않을 때는 거래비용은 큰 성장에 큰 장애물이다. 이들에게 달러화는 그야말로 계륵이다. 달러화는 장기적으로 가치가 하락할 통화이지만, 기축통화기 때문에 없으면 거래할 수가 없다. 특히나 기업, 개인에게 달러화로 거래하는 것은 엄청난 거래비용을 수반한다. 가난하면 더 심하다. 달러화 자체가 거래의 장애요인이다.

[도표 51] 주요 신흥국 본원통화는 점진적으로 증가



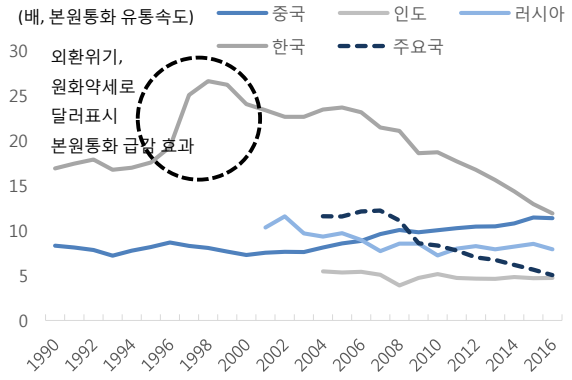
자료: Bloomberg, 교보증권 리서치센터

[도표 52] 그러나 신흥국 M1, M2 등은 확장적으로 증가



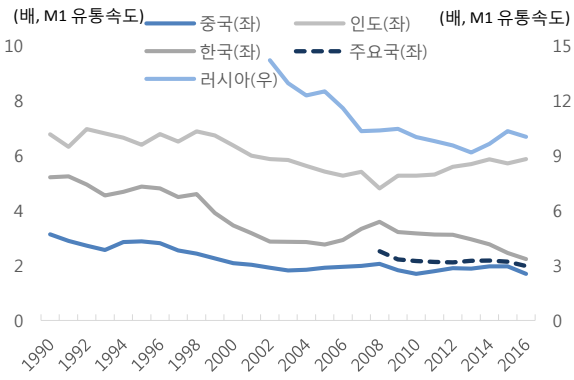
자료: Bloomberg, 교보증권 리서치센터

[도표 53] 주요 신흥국은 경제악화로 본원통화 유통속도 하락



자료: Bloomberg, 교보증권 리서치센터

[도표 54] M1 유통속도 하락, 이는 과잉부채와 자산버블을 의미



자료: Bloomberg, 교보증권 리서치센터

블록체인 암호화폐 및 토큰 시장, 디지털 거래 늘어날 시 상승여력 보유

현재 블록체인 암호화폐 시가총액은 $1,600억을 넘고 있다. 비트코인이 처음 거래된 시기가 2010년이었으므로 7년간 빠른 속도로 확대되었다. 가격 뿐만 아니라 다양한 화폐와 자산(비즈니스) 베이스 토큰이 발행되고 있다. (866개의 암호화폐, 233개의 자산 베이스 토큰이 상장되어 전세계 5,421개 거래소에서 거래되고 있다.) 시가총액 비중으로 비트코인 46.2%, 이더리움 19.9%, 비트코인캐시 5.8%, 리플 5.3%를 차지하고 있다.

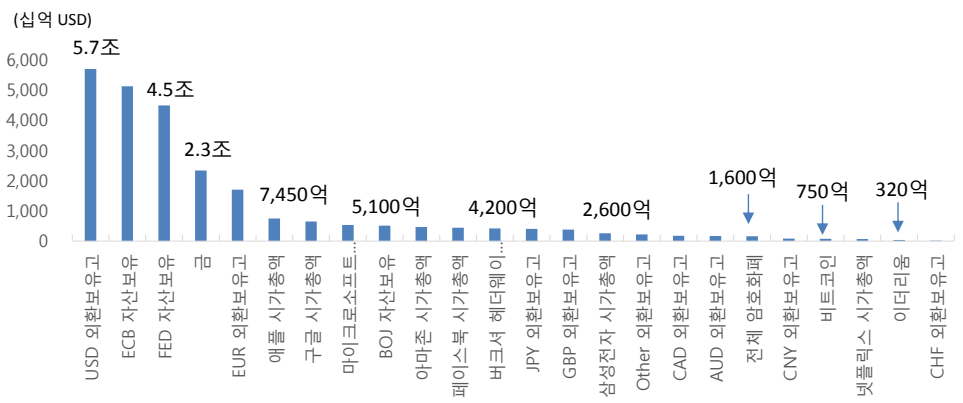
[도표 55] 블록체인 암호화폐 시장은$1,600 억 규모, 866 개의 암호화폐, 233 개의 자산, 5,421 개의 거래소가 존재

866 Currencies	233 Assets	5,421 Markets					
Name	Symbol	MarketCap	Price	Circulating Supply	Volume (24h)	Marketcap Share	Volume Share
Bitcoin	BTC	74,589,069,559	4,509.59	16,540,100	2,697,580,000	46.2	32.1
Ethereum	ETH	32,048,108,895	339.51	94,393,794	1,428,850,000	19.9	17.0
Bitcoin Cash	BCH	9,396,069,079	567.49	16,557,213	316,957,000	5.8	3.8
Ripple	XRP	8,535,224,172	0.222597	38,343,841,883	322,699,000	5.3	3.8
Litecoin	LTC	3,999,424,145	75.81	52,754,082	1,326,960,000	2.5	15.8
NEM	XEM	2,638,755,000	0.293195	8,999,999,999	9,600,250	1.6	0.1
Dash	DASH	2596168423	344.79	7,529,622	53,814,100	1.6	0.6
IOTA	MIOTA	1865148206	0.67103	2,779,530,283	39,987,500	1.2	0.5
Monero	XMR	1,858,297,598	123.67	15,026,868	127,482,000	1.2	1.5
Ethereum Classaic	ETC	1,816,998,555	19.1	95,138,286	648,175,000	1.1	7.7
Total		161,432,339,117			8,394,539,363	100	100

자료: Coinmarketcap, 9월 3일 기준

지금까지 암호화폐는 실제 교환의 매개보다는 주로 자산가치 저장 수단으로 시장이 형성되었다. 암호화폐 체계에 부정적 시각을 갖는다면 이는 물론 투기이며, 더 나아가서는 사기로 볼 수도 있다. 그러나 이제 블록체인 2.0 단계에 진입하면서 실제로 암호화폐 체계의 비즈니스 기회가 창출되고, 실제 암호화폐 거래가 늘어나게 된다면 암호화폐의 시가총액은 자연스럽게 증가하게 될 것이다. 전세계 화폐시장의 규모 및 IT 혁신기업에 비해 암호화폐 시장은 여전히 작다. 암호화폐체계를 옹호한 안데르센 호로비츠의 의견처럼 화폐기능을 감당하기 위해서는 어느 정도 시가총액 형성이 중요하다.

[도표 56] 주요 통화와 혁신적 IT 기업들, 그리고 암호화폐 시가총액



자료: Bloomberg, Coinmarketcap, 9월 3일 기준

비트코인이 금 시장을 대체한다면?

(단순 추론에 의한 시나리오이므로 투자선택 및 결정의 근거로 사용되어서는 안 됨)

과연 비트코인 가격은 언제, 얼마까지 오를까? 여기에 대한 정확한 답을 누구도 할 수는 없을 것이다. 다만 올해 들어 비트코인 가격이 급격히 상승하기 시작하면서 하나, 둘 가격전망을 내놓기 시작했다. 대체로 비트코인 기술에 대해 긍정적으로 평가하면서 가격상승세가 이어질 것이라는 관측을 내 놓고 있다. 단기(올해)로는 대체로 $5,000~7,500, 장기로는 $50,000과 $100,000(중국 채굴왕 우지한)이 있다. 골드만삭스의 셰바 자파리는 $4,827까지 상승 이후 $2,221까지 하락할 것이라는 비관적 전망을 했다.

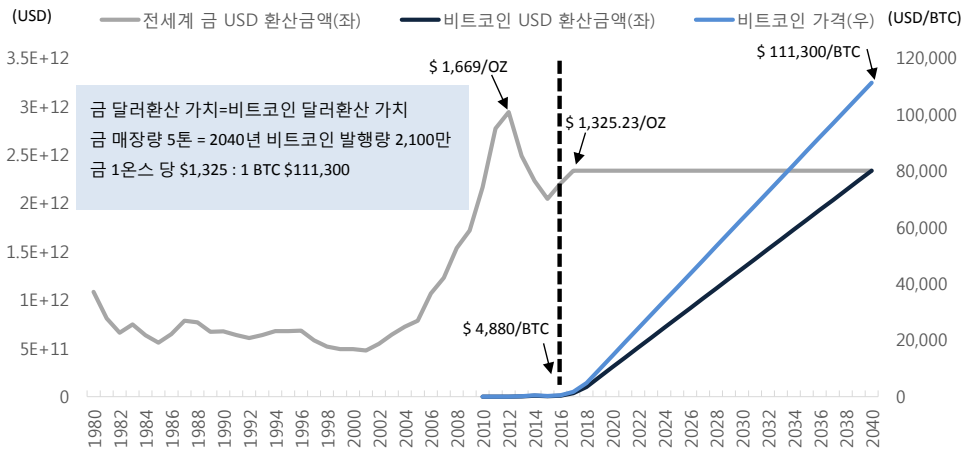
[도표 57] 비트코인 분석가, 투자자 및 채굴자들의 비트코인 가격 전망

인물	소속	단기	장기	발언 및 전망 내용
맥스 카이저	미국 재무분석가	$5,000		비트코인 도입국가 확대와 기관투자가 수요 증가
톰 리				비트코인은 금과 매우 유사한 특징을 지닌 매력적인 대체 통화
안드레아스 안토노폴로스	비트코인 기술자			비트코인에 대한 시장에 대한 확신 강함, 거래확대로 점차 자산시장 수요 확대
셰바 자파리	골드만 삭스 / Technical Strategist	$4,827	$2,221	
아더 헤이즈	비트메인 CEO	$5,000		비트코인 세그윗 구현 호재
로니 모아스	독립 애널리스트	$7,500	$50,000	스마트폰 보급과 함께 암호화폐 채택 늘어나고, 자산배분에도 포함될 것
우지한	비트메인		$100,000	비트코인 가격은 5 년 내 $100,000 될 것

자료: 교보증권 리서치센터 정리

중국 비트메인의 채굴왕 우지한의 장기 가격 $100,000의 근거는 무엇일까? 궁금해 진다. 우리는 전세계 금 매장량의 현재 달러환산 가치와 2040년 비트코인 채굴 종료 이후 달러환산 가치가 같아진다면 1 비트코인은 $111,300에 이른다는 추론을 해 봤다. 물론 비트코인이 금 역할 대체에 대한 동의가 필요하다. 만약 비트코인이 금 시장의 절반을 차지한다면 $55,650이 될 것이다. 이렇게 보면 비트코인 상승여력은 아직 크다.

[도표 58] 전세계 금 매장량의 현재 달러환산 가치와 2040 년 비트코인 달러환산 가치가 같다면



자료: Bloomberg, 교보증권 리서치센터

법정 화폐론자들의 문제제기를 극복해 나가야 한다.

물론 비트코인, 이더리움 등 암호화폐가 법정화폐를 대체할 수 있는 지에 대한 판단은 불확실하다. 기존 법정 화폐를 지지하는 진영에서는 당연히 암호화폐 체계의 문제점을 지적하고, 규제의 필요성을 제기할 것이기 때문이다. 이에 대해 암호화폐 진영에서는 암호화폐의 적절한 분배와 보상, 네트워크의 신뢰성, 화폐유통 체계 등에 대한 개발과 노력이 요구될 것이다. 부디 건전한 토론으로 법정 화폐와 암호 화폐 체계가 각각 자신을 혁신하고 공존하며 전세계 부의 새로운 창출과 분배 과정이 진행되었으면 하는 바람이다.

[도표 59] 비트코인의 화폐로서의 문제점과 극복 방안

기능	법정화폐론자 입장 (David Yermack, Is bitcoin a real currency? An economic appraisal, 2014 년 4 월)	비트코인에 대한 Open Mind 혹은 법정화폐 시스템에 대한 문제
교환의 매개 (medium of exchange)	비트코인은 거래목적보다는 주로 투기목적으로 보유 새로운 비트코인 획득의 어려움, 상품의 구입을 위해서는 반드시 비트코인을 보유해야 하는 점 등이 비트코인 사용에 장애요인으로 작용 반면, 전통적인 통화는 신용카드나 판매신용 등 소비자신용을 사용하여 구입 가능	누가 판단? 화폐주조차익은 화폐 시스템 초기 언제, 어디서든 발생
가치척도 (unit of account)	비트코인이 가치척도 수단으로 사용되어지는 증거는 거의 없음 비트코인 가치의 매우 ① 높은 변동성, ② 불확실한 시장가치, ③ 높은 가격에 따른 가격비교 곤란 등이 비트코인이 가치척도로 사용되기 어렵게 함 ① 미 달러화 대비 비트코인의 일일변동성은 높으며, 이에 따라 업체들은 매우 빈번하게 표시가격을 수정해야 함 ② 재정거래로 일물일가 법칙이 성립하는 기존 통화와 달리 비트코인은 거래소간 가격이 다르게 형성 ③ 비트코인 한 단위의 가치가 너무 높아 가격이 소수점 이하 5 자리 이상으로 표시	네트워크의 기술 및 거래자들의 신뢰만 있으면 극복 가능 재정거래는 이론 상에서나 가능, 실제 외환시장에서는 수요/공급 환경의 차이 발생하며, 화폐 암시장도 엄연히 존재 1/100 센티비트코인, 1/1000 밀리비트코인, 1/1000000 마이크로비트코인, 1/100000000 사토시
가치저장 (store of value)	기존 통화에 비해 매우 높은 가치 변동성을 감안할 때 가치저장 수단으로 기능하기 어려움 디지털통화의 환율은 다른 통화와 상관계수가 사실상 '0'인 것으로 나타남에 따라 디지털통화는 환변동 위험을 헤지하기도 어려움	비트코인 체계는 이론 상, 실물경제 및 온라인 거래의 확장성 비교할 때, 공급이 제한되어 있어 장기적으로는 오히려 가치가 안정, 혹은 상승할 수 있음 (금과 유사한 성격)
화폐시장의 경제 안정화 효과	화폐 총 공급량이 고정되어 있어 디지털통화 경제는 수요변동에 따라 통화공급을 조절할 수 없게 되어 가격과 실물경제에 심각한 변동성을 초래할 수 있음 경제성장에도 통화공급이 증가하지 못 하여 디플레이션을 초래하고 소비와 투자를 위축시키는 문제가 있음	화폐유통속도가 충분히 빠르면 통화부족 문제는 발생하지 않음

자료: 한국은행 교보증권 리서치센터

블록체인과 암호화폐에 대한 인식의 변화

4차 산업혁명과 블록체인

정재승 박사는 tvN 알쓸신잡에서 제 4차 산업 혁명에 대해서 혁신적으로 설명해 주었다. 제 4차 산업 혁명의 근본적인 아이디어는 '현실세계의 모든 것들이 온라인의 비트 세상으로 옮겨간다.'는 것이다. 인간이나 사물의 이동, 거래 등을 포함한 모든 정보가 인터넷을 통해서 정보화되고, 이를 인공지능이나 로봇이 빠르고, 저비용으로 활용해 생산할 수 있게 된다.

[도표 60] 3 차 산업혁명까지의 정리와 다가올 3 차 산업혁명의 개념

자료: tvN 알쓸신잡 9회

그러나 제 4차 산업 혁명에서 노동의 가치는 하락하는 문제가 있다. 더욱이 새로운 부를 창출하는 인공지능, 로봇을 포함한 새로운 기술은 생산력을 크게 증가시키지만 소비하지는 못 한다. 이에 따라 생산성 향상이 인간의 소득으로 이어지지 않고, 소비력이 떨어지는 결과로 이어지고 결국 자본주의 시스템이 유지되지 못 하게 된다.

정재승 박사는 이러한 제 4차 산업혁명의 결과, 자본주의 자체적으로 기본소득제를 진지하게 논의되고 있다는 흥미로운 현상을 설명했다. '더 이상 일하지 않는 자는 먹지도 말라, 노동만이 가치로운 것이라는 생각을 한 발짝 버리고, 기계가 생산한 것을 인간에게 분배해서 소비로라도 자본주의에 기여하라는 점에서 기본소득제가 논의되고 있다.'고 설명했다. 자본주의의 최전선에 있는 '다보스 포럼'에서 최근 기본소득제 및 자본주의 수정에 대해서 논의하고 있는 부분과 일맥상통하고 있다.

블록체인 기술은 정재승 박사가 얘기한 4차 산업혁명의 논점과 연결된다. 실제세계의 많은 정보들이 온라인에 기록되어 누구나 그 정보를 활용해 부가가치를 창출할 수 있는 토대가 되기 때문이다. 블록체인은 이러한 아이디어들이 이더리움 등의 블록체인 플랫폼을 통해 비즈니스화되고, 암호화폐 거래를 통해 비용과 보상을 효율적으로 처리할 수 있게 되기 때문이다.

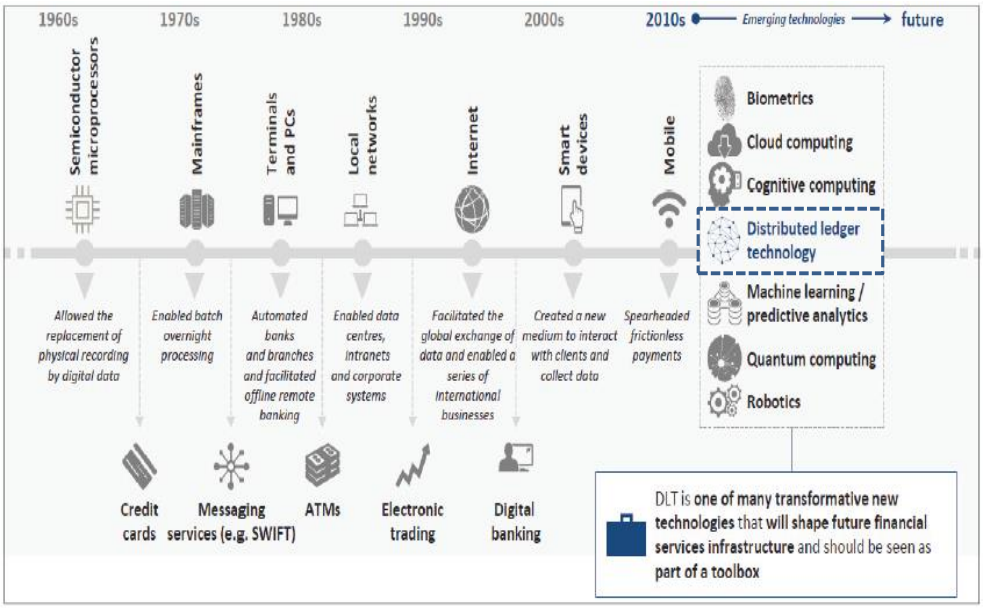
블록체인 기술을 활용하고자 하는 노력은 다양하게 진행되고 있다. 무디스에 따르면 블록체인 기술은 금융, 기업, 정부, 산업연계에 있어서 다양하게 전개될 수 있다. 특히 IT기술과 금융이 접목된 핀테크 분야에서 중앙관리 체계에 의한 거래비용 및 시간 등을 블록체인 기술로 효율화시킨다면 역사적으로 가장 느린 진전을 보인 금융역할의 확대시킬 수 있다. 기존 고객들의 거래비용을 축소하고, 제3세계 진출이 용이해진다.

[도표 61] 블록체인 기술의 활용 분류

금융	기업	정부	산업 연계
국제송금	공급사슬관리	기록관리	재무관리 및 회계
자본시장	헬스케어	신원관리	주주투표
무역금융	부동산	투표	기록관리
규제준수 및 감사	미디어	세금	사이버보안
자금세탁방지 및 고객알기제도	에너지	정부 및 비영리기구 투명성	빅데이터
보험		입법, 준수, 규제 감시	데이터저장
P2P 거래			사물인터넷

자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」 2016년 공동연구, Moody's Investor Service, Credit Strategy-Blockchain Technology: Robust, Cost-effective Application Key to Unlocking Blockchain's Potential Credit Bebefit, 2016년 7월

[도표 62] 기술혁신과 금융서비스의 진화



자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」 2016년 공동연구, World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future Service Series, 2016년 8월

블록체인에 대한 기업의 대처, 적극 도입

블록체인 기술은 IT 시스템에서 응용기술 개발, 인프라 장비조달, 중간구조 개발비용을 절감할 수 있다. 기업경영에 있어 회계감사, 서류관리, 노동비용을 절감할 수 있다. 향후 IT 시스템과 기업경영에 있어 블록체인의 의한 대규모 아웃소싱이 진행될 것이다.

[도표 63] 블록체인 도입에 따른 비용 절감

구분	절감 요인	개요
IT 시스템	응용기술 개발비용 절감	· 클라우드 기반의 비공개 분산원장 환경으로 이전함으로써 비용 감소 · 백업 비용과 위기대응 비용의 감소 가능
	인프라 장비조달 비용 절감	· 위기대응과 관련한 계획, 설계, 테스트의 개인적 비용 감소 · 오픈소스로 자원의 자급자족인 경우 비용 절감 가능
	중간구조(middle structure) 개발비용 절감	· 분산원장의 개발설계가 현존 DB를 수용하는 구조일 경우 비용 감소 · 운영관리 측면의 비용 절감 가능
기업 경영	회계감사 비용 절감	· 지급보증서나 거래기록의 관리 비용 절감 · 거래 투명성과 사기의 어려움으로 인한 제3자의 회계감사 비용 감소
	종이서류 관리비용 절감	· 종이서류로 진행되는 작업의 감소로 인한 비용 절감 · 메일을 이용한 아날로그식 인증 비용의 감소
	노동비용 절감	· 원스톱 디지털 작업에 따른 노동비용 절감 · 스마트계약의 실행에 따른 운영인력 비용 절감

자료: 한국은행「분산원장 기술의 현황 및 주요 이슈」2016년 공동연구, Nomura Research Institute, Survey on Blockchain Technologies and Related Services, FY2015 Report, 2016년 3월

기업들은 컨소시엄을 구성해 블록체인 기술을 도입할 시도를 하고 있다. 대표적인 블록체인 컨소시엄으로는 미국 주도의 R3, HyperLedger, 일본의 SBI, 중국의 ChinaLeger가 있다. 또한 이더리움 중심으로 결성된 EEA (Enterprise Ethereum Alliance)가 있다. 결국 블록체인 기술이 서로 접목될 때는 공개 블록체인의 중요성이 커질 것이다.

[도표 64] 주요 글로벌 분산원장 기술 컨소시엄

컨소시엄	참가기관	주요 특징
R3	미국 IT 기업 R3 사 설립 골드만삭스, UBS 등 60 여개 대형 금융기관 국내 5 개 은행 (국민, 신한, 하나, 기업, 우리)	금융기관 계약 기록관리 시스템(Corda) 개발
HyperLedger	리눅스 재단이 관리 금융기관 및 비금융 IT 기업 등 100 여개 기업 국내기업 (한국 예탁결제원, 코인플러그, 삼성 SDS)	오픈 소스 범산업용 블록체인 플랫폼을 연구 개발
SBI 핀테크 컨소시엄	일본 SBI 금융그룹 주도 리플, 코인플러그 등 참여	
차이나레저	중국 완샹 블록체인 랩 주도 중국 11 개 대형 금융기관 참여	R3 와 이더리움 재단 자문

자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」

블록체인에 대한 정부의 입장, 의심에서 도입으로 변화되고 있음

블록체인에 대한 정부의 입장은 어떨까? 비트코인이 주도한 블록체인 1.0과 현재 플랫폼 기반으로 쓰임새가 확장된 블록체인 2.0에 진입한 시점과 양상이 달라지고 있다.

초기 비트코인은 탈 중앙화와 기존 화폐체계에 대한 위협으로 느껴져 정부나 중앙은행 입장에서는 위험스러운 존재였으며, 자연스러운 규제 방향으로 나타났다. 특히 마약, 탈세, 불법해외 자금 송금 등 불법적 행위에 사용하기 용이했던 것도 사실이다.

[도표 65] 비트코인에 대한 국가별 규제 도입

구분	규제
미국	FinCen (2013 년) : 거래소 등에 자금세탁방지규제 적용 국세청 (2014 년) : 디지털통화에 재산세 부과 선물거래위원회 (2015 년) : 비트코인 파생상품 감독 시행 뉴욕주 (2015 년) : 비트라이센트 도입
EU	은행감독청 (2013 년) : 디지털통화 소비자 주의 경고 유럽위원회 (2016 년) : 거래소 등에 자금세탁방지규제 적용
일본	금융청 (2016 년) : 거래소 등에 규제를 적용하고 비트코인 매매시 소비세 비적용 검토

자료: 한국은행 「분산원장 기술과 디지털통화의 현황 및 시사점」

정부 입장에서는 비트코인이 자금세탁, 탈세 등에 사용되지 않도록 규제하기 시작했다. 중앙은행이나 통화당국의 입장에서는 투기적인 요소와 투자자 보호에 대해서 경고했다. 또한 비트코인이라는 정체 불명의 화폐가 각국의 법정화폐를 대체할 것을 차단하기 위해 거래수단으로 차단하는 규제도 했다. 정부의 곱지 않은 시선과 함께 많은 사람들 역시 비트코인의 거래체계의 혁신보다는 수상한 화폐로 인식하였다.

[도표 66] 각국의 비트코인 거래 금지 내역

국가	기관	주요 내용
중국	인민은행	금융기관에 비트코인 관련 거래 금지 경고 (2013 년 12 월) 동 조치를 지급결제 서비스업체로 확대 (2014 년 1 월)
태국	태국은행	비트코인 관련 인허가 거부하면서 비트코인 매입, 판매, 사용 등이 불법이라고 회신
인도네시아	인도네시아 중앙은행	비트코인은 인도네시아 실정법을 다수 위반하고 있다고 발표
러시아	대검찰청	비트코인은 러시아에서 금지된 대체화폐에 해당한다고 발표
	중앙은행	비트코인 관련 서비스는 의심스러운 거래(dubious tranction)에 해당한다고 발표

자료: 한국은행 「분산원장 기술과 디지털통화의 현황 및 시사점」

정부나 중앙은행이 비트코인에 대한 경계했지만, 사실 제대로 규제할 방법은 없었다. 비트코인의 거래체계에 대한 법 체계가 없기 때문이다. 실제로 비트코인으로 부동산 거래를 한 후 신고했지만, 미비한 법 체계로 관련 세금을 걷지 못 했다는 일화도 있다. 즉, 정부나 중앙은행의 규제는 그저 경고와 주의 정도에 불과한 것이었다.

비트코인이 나온 이후 유럽 재정위기, 선진국들의 양적 완화 등 비트코인의 우호적인 사건들이 발생하면서 사람들은 점차 비트코인의 철학과 기술적 혁신에 관심을 갖게 되었고, 시간이 갈수록 비트코인으로 거래하고, 투자자산으로 보유하기 시작했다.

정부나 중앙은행의 비트코인에 대한 시각은 여전히 비판적이었지만, 블록체인 2.0 국면에 진입하면서 달라지고 있다. 이더리움 등이 나타나면서 블록체인 기술의 활용성이 인식되기 시작했기 때문이다. 사실 이더리움은 비트코인의 한계를 극복하는 과정에서 나왔고, 또 비탈릭 부테린 등 이더리움 재단은 자신들의 비전을 명확하게 설명하고 신경제에 대한 대안을 적극적으로 제시한 영향도 크다. 기업들이 블록체인 기술의 이점을 알아채면서 컨소시엄 등을 구성한 것도 정부의 인식변화에 영향을 끼쳤다.

최근 중앙은행들이 자신들이 통제하는 블록체인 기반의 디지털 화폐 도입을 연구 중이다. 영국, 네덜란드, 캐나다 중앙은행이 이에 대한 연구를 진행 중이다.

정부는 블록체인 기술을 공공서비스에 도입할 목적을 갖고 있다. 에스토니아에서는 주민의 기록을 관리할 수 있는 국가적인 블록체인 체제를 도입 중이다. 혁신적 시도에 가장 앞서 있다고 평가 받는 싱가포르는 다자간 거래, 무역과 금융 산업에 도입 등 광범위한 블록체인 도입을 준비하고 있다. 영국, 스웨덴, 러시아, 중동도 블록체인 도입이 활발하게 전개되고 있다. 블록체인 체제의 비용절감은 누구에게나 매력적일 것이다.

[도표 67] 블록체인 도입을 준비하고 있는 중앙은행 및 각국 정부

기관	내용
중앙은행	블록체인을 기반으로 디지털 화폐를 발행해 유통하는 방안에 대해 다양하게 연구 중 중앙은행 역시 실물화폐를 발행, 유통하는 데 많은 비용이 듬 (특히 동전) 또한 중앙은행이 디지털 기반으로 화폐를 발행 관리하면 오히려 탈세 추적 등이 용이 세계경제포럼에서는 800 명의 조세 전문가 중 73%가 2025 년 이전 블록체인 기반으로 조세를 걷는 사례가 있을 것으로 예상 영란은행은 디지털 화폐인 RSCoin 을 보고서를 통해 발표 네덜란드 중앙은행은 중앙은행이 통제하는 DBB 코인에 대한 아이디어 발표 캐나다 중앙은행도 블록체인 기반 중앙은행이 발행하는 CAD Coin 에 대해 연구 중
영국 정부	공공분야에서 블록체인을 활용할 수 있는 방안에 대해 적극적으로 연구 진행 블록체인이 보안, 프라이버시, 신뢰 등 문제를 극복한다면 공공분야에 다양하게 활용 가능 노동연금부는 바클레이스 은행 및 핀테크 스타트업과 함께 블록체인 네트워크를 통한 연금수령 및 사용기록에 대한 연구 진행
에스토니아 정부	블록체인을 전면적으로 도입하고자 하는 정부 중 하나 에스토니아 주민 기록, 관리하는 블록체인 플랫폼 e-residency 시스템 준비 중 나스닥과 함께 전자투표 플랫폼도 개발 중, 공공 서비스 이용 위한 통합 플랫폼 구축
싱가포르 정부	기업과의 협업을 통한 블록체인 활용방안 연구 중 IBM 과 협력해 블록체인 혁신센터 조성, 경제개발청과 통화청은 블록체인 다자간 거래 플랫폼 구축 항만청은 공급사슬 개선방안을 도출해 3 년 이내 금융과 무역 산업에 활용할 블록체인 기반 파일럿 프로그램 발표 예정
러시아 정부	비트코인 자체에 대해서는 회의적이나, 블록체인에 대해서는 개방적 태도, 적극 도입 추진 연방 반독점청은 하이퍼레저에 개입한 러시아 최대 금융기관인 Sberbank 와 블록체인 기반 문서관리 시스템 테스트
스웨덴 정부	블록체인을 활용하여 토지 소유권과 이전 내역을 기록하는 스마트 계약 플랫폼 연두 중
아랍에미리트 정부	블록체인을 신사업 육성 기술로 평가하고 이에 대한 개발을 진행
두바이 정부	2020 년까지 정부의 모든 문서 시스템에 블록체인을 도입하는 프로젝트 진행

자료: 한국은행「분산원장 기술의 현황 및 주요 이슈」2016년 공동연구

[도표 68] 블록체인 기술 도입 로드맵

활용 예	개요	편익	발전 단계
거래의 문서화 속도 증진	신뢰된 네트워크에서 대출 및 IPO 문서 공유와 승인	· 계약용어의 표준화 · 처리속도 증진 · 유동성 개선	1단계 (2016~2019)
조회데이터 원천의 공유	시장참가자의 일반적인 조회데이터를 분산원장에 갱신	· 이중 작업의 방지 · 자금세탁위험과 벌금부과가능성 경감	1단계 (2016~2019)
이질적 내부시스템 간의 데이터 분배	분산원장의 복수 내부시스템을 망라한 활용	· 내부조화 필요성 제거 · 정확하고 전체적인 견해 제공	1단계 (2016~2019)
비유동적 자산 정보를 위한 사적 네트워크 활용	비유동적인 장외시장 거래자산에 대한 거래상대방 발견	· 적절한 자산의 표준 정보 공유 · 중개수수료의 감소 · 큰 규모 자산풀에 제한된 접근 허용과 민감한 시장정보의 누출 방지	1단계 (2016~2019)
작업흐름과 분석을 지원하는 데이터 환경 구축	거래단계의 데이터를 암호화하여 안전한 스마트계약에 저장하고 사용자가 접속 노드를 통해 작업흐름에서 활용	· 데이터의 조화과정 제거 · 더욱 효과적인 투자분석	2단계 (2017~2025)
담보자산의 원천 및 활용 추적	분산원장을 통한 담보자산의 상태와 위치, 적격성, 재담보 설정, 초과담보 등 추적	· 복수의 마진계좌 연계 · 실시간 상태 파악 · 스마트계약과 함께 최적화 논리 지원	2단계 (2017~2025)
펀드 투자환경 개선	펀드의 이전과 소유권을 분산원장으로 추적	· 펀드가입과 상환 자동화 · 투자 사이클의 개선	2단계 (2017~2025)
규제기관의 셀프서비스 분석보고 가능	허가되고 분할된 분산원장에 대한 규제기관의 셀프서비스 분석보고서	· 규제기관의 분석보고 실패 가능성 경감	2단계 (2017~2025)
고객을 위한 분석 포탈 활용	고객이 실시간으로 직접 또는 포탈을 통해 투자포트폴리오와 실적을 분석	· 실시간으로 풍부한 정보 제공 · 개별 고객의 분석니즈에 부합	2단계 (2017~2025)
T+0 결제환경 구축	청산과 결제 과정을 단축시키는 시스템 구축	· 결제유동성 위험의 현저한 감소 · 자본의 효율적 배치	3단계 (2020~2030)
주권 관련 활동 개선	대리투표, 수익분배 등의 관리 효율화	· 관리 비용 및 수작업 경감	3단계 (2020~2030)
마진콜의 자동 실행	스마트계약을 통한 마진증거금 산출과 갱신	· 중앙거래당사자의 일중 유동성위험 제거와 전반적인 마진증거금 감소 · 관리 부담의 감소	3단계 (2020~2030)
새로운 상품 개발 활용	분산원장에 디지털화된 지분을 소유함으로써 새롭게 결합된 상품의 개발과 스마트계약의 활용	· 거래 및 관리에 수반한 간접비 경감 · 일중 유동성 제공 필요성 경감	3단계 (2020~2030)
P2P 보관과 결제 네트워크 활용	분산원장에 등재된 디지털화된 자산의 개인간 장외거래 네트워크 구축	· 중개자의 필요성 제거 · 결제 속도의 대폭 개선	3단계 (2020~2030)

자료: 한국은행 「분산원장 기술의 현황 및 주요 이슈」 2016년 공동연구, J.P.Morgan and Oliver Wyman, Unlocking Economonic Advantage with Blockchain

중앙집권, 자본주의, 화폐에 대한 거인들의 통찰

「1984」의 빅 브라더

중앙집권은 느리고, 절대권력은 부패하며, 전체주의는 인간을 절망케 한다.

조지 오웰(1903~1950)의 소설 「1984」는 1984년(집필 당시 미래)을 배경으로 한다. 극단적인 전체주의 사회인 오세아니아의 정치 통제 기구인 당은 허구적 인물인 빅 브라더를 내세워 독재 권력의 극대화를 꾀하는 한편, 정치 체계를 항구적으로 유지하기 위해 텔레스크린, 사상경찰, 마이크로폰, 헬리콥터 등을 이용해 당원들의 사생활을 철저히 감시한다. 그리고 당의 정당성을 획득하는 동시에 당원들을 사상적으로 통제하기 위해 과거를 끊임없이 날조한다. 존재하지도 않는 반역자 골드스타인을 내세워 사람들의 증오심을 집중시키는가 하면 인간의 기본적 욕구인 성욕까지 통제하려 든다.

주인공 윈스턴 스미스는 이 같은 당의 통제에 반발을 느끼고 저항을 시작한다. 그는 지하 단체인 '형제단'에 가입해 당의 전복을 기도하지만 함정에 빠져 사상경찰에 체포되고 만다. 윈스턴은 모진 고문과 세뇌를 받은 끝에 연인마저 배반하고 당이 원하는 것을 아무런 저항 없이 받아들인다. 그리고 인간의 모든 가치를 상실한 채 빅 브라더를 사랑하게 되고, 조용히 총살형을 기다린다.

조지 오웰은 인도의에서 영국 하급 관리의 아들로 태어났다. 영국에 귀국해 명문인 이튼 학교를 졸업했으나 대학 진학을 포기하고 미얀마에서 경찰로 근무한다. 그러나 식민 체제와 제국주의에 대한 혐오감을 견디지 못 해 경찰직을 그만 두고 작가의 길을 걷기로 한다. 1945년에는 러시아 혁명과 스탈린에 대한 정치 우화 「동물농장」을 출간해 명성을 얻었고, 1949년 인간의 존엄성과 자유를 박탈한 전체주의를 비판한 「1984」를 출간했다. 조지 오웰은 사회주의자로 전향했으나 공산주의가 되지는 못했다. (네이버 지식백과 中 1984, 조지오웰 참조)

[도표 69] 빅 브라더에 통제 당하는 개인

자료: Google 1984 관련 이미지

자본주의와 화폐제도의 위기

애덤 스미스(1723~1790)가 「국부론」을 저술한 이후 전세계 경제를 이끈 자본주의 시스템이 위기를 맞고 있다. 성장저하, 분배악화 상태가 개선되지 않기 때문이다.

자본주의는 대체로 4단계로 구분된다. 자본주의 1.0은 애덤 스미스 이후~세계 대공황 시기로 자유방임주의와 1~2차 산업혁명으로 경제가 빠르게 성장했다. 그러나 1차 세계대전과 시장실패로 대공황이 나타냈다. 자본주의 2.0은 1930년대 뉴딜정책~1970년대 석유파동까지로 시장실패를 정부가 개입해야 한다는 케인지안이 나타났다. 자본준의 3.0은 1980년대 신자유주의~2008년 금융위기로 정부개입의 비효율을 지적하고, 세계화 및 시장중심주의로 회귀했다. 자본주의 4.0은 2008년 금융위기 이후 현재까지로 저성장, 고령화, 과잉부채 등으로 구조적 문제가 나타나고 있다. 지금까지의 경제이론으로는 재차 정부의 개입 등이 요구되며 온정적 자본주의를 요구한다. 그러나 온정적 자본주의는 실현되지 않고 불균형은 확대되어 시장과 정부에 대한 불신이 커졌다.

화폐제도는 자본주의 시대 구분과 대체로 일치한다. 1930년대 대공황 이전 금 본위제였다. 중세시대부터 금은 통화와 신용의 지렛대 역할을 해 왔다. 그러다 대공황 이후 전개된 브레튼우즈체제는 미국 달러화를 기축통화로 정하며 금 1온스당 $35로 고정시켰다. 글로벌 경제가 악화되면서 기축통화 제도에 있어 '트리핀의 딜레마(기축통화의 국제 유동성과 신뢰도는 상충)' 제기로 킹스턴 체제로 전환되었다. 이 때부터 각국은 통화량을 적극적으로 조절하고 자유변동환율 제도로 전환되었다. 2008년 글로벌 금융위기 이후, 악화된 경제를 복구하기 위해 화폐의 가격, 즉 금리는 대체로 제로로 하락시켰다. 중앙은행 예치금리는 마이너스로 진입하고, 본원통화는 크게 늘렸다.

[도표 70] 자본주의와 화폐제도의 시기적 구분

구분	시기	특징	화폐제도	특징
자본주의 1.0	애덤 스미스~1929 년 세계 대공황	고전학파, 자유방임주의	금 본위제	금 기축통화
자본주의 2.0	1930 년대 뉴딜정책~1970 년대 석유파동	케인지안, 정부개입주의	브레튼우즈체제	달러 기축통화, 금 가치에 고정
자본주의 3.0	1980 년대 신자유주의~2008 년 금융위기	신자유주의, 시장중심주의	킹스턴체제	자유변동환율제
자본주의 4.0	2008 년 글로벌 금융위기 이후	온정적 자본주의, 정부와 시장의 유기적 상호작용		제로대출금리, 마이너스 예치금리, 양적완화 정책

자료: 교보증권 리서치센터

2008년 글로벌 금융위기 이후 10년 가량이 지났다. 겉으로 보기에 세계 경제는 어느 정도 평안을 되찾은 것으로 보이나, 실상은 그렇지 않다. 잃었던 일자리에 복귀하지는 쉽지 않고, 중산층 이하의 소득은 하락하고 있다. 반면 저금리로 유동성이 풀리면서 부의 집중 현상은 더욱 심화되었다. 정부 등 중앙기관에 대한 신뢰를 하락하고 있고, 많이 풀린 유동성으로 자산가치는 상승하고 있으며, 화폐의 실질구매력을 하락하는 등 자본주의, 화폐제도는 위기를 맞고 있다. 솔직히 말하면 자본주의의 타락이다.

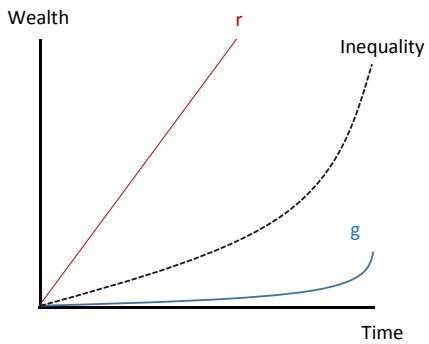
칼 마르크스의「자본」, 토마 피게티의「21세기 자본」

칼 마르크스(1818~1883)는 생산활동이 인류 역사발전의 원동력이라고 봤다. 농업사회에서 농민은 지주나 영주와 관계를 맺어 생산수단인 토지를 갖고 곡물을 생산했다. 자본주의에서는 부르주아가 생산수단인 토지, 자본을 소유하고, 농민은 임금을 받는 구조로 전환되었다. 이는 산업사회에서도 마찬가지다. 자본자가 공장, 기술을 갖고, 노동자는 임금을 받게 된다. 이 과정에서 자본가는 잉여가치를 소유해 노동자의 몫을 착취한다고 주장했다. 자본주의에서 이는 계약관계를 통해 나타나 통용된다.

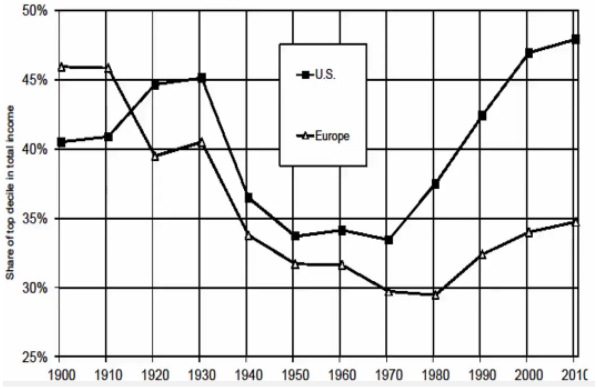
마르크스는 자본주의는 외부 공격이 아닌 자신의 운동 법칙 때문에 위기와 몰락한다고 예견했다. 자본가는 이윤확대를 위해 설비투자를 늘리고, 경쟁심화와 생산성 저하로 이윤을 오히려 하락한다. 이에 따라 노동자에 대한 임금을 줄이고, 구매력이 떨어져 생산이 감소한다. 경제는 침체되고 자본가는 과잉설비와 수요부족 사태를 동시에 직면해 위기에 빠진다. 결국 경제의 생산활동이 저하되어 자본주의는 몰락한다. (이코노미스트 Cover Story <자본론> 출간 150주년, 무엇을 남겼나 2017.6.19 참조)

토마 피게티(1971~)는 자본수익률은 경제성장률을 언제나 상회하며, 이에 따라 부의 불균형은 확대된다고 봤다. 특히 경제성장률에 비해 노동에 대한 분배율을 불안정하고 낮다. 고용은 항구적이지 않아 경제성장에 의해 창출된 부는 모든 사람에게 분배되지 않는다. 또한 기업들의 유보를 생각해 보면, 노동수익률은 경제성장률보다 낮다. 따라서 자본수익률은 경제성장률보다 높고, 노동수익률은 경제성장률보다 낮아 불평등이 확대된다. 피게티는 역사적으로 볼 때, 자본수익률은 대체로 일정하고, 경제성장률은 장기간 낮은 상태에서 머무르다 산업혁명 이후 올라오기 시작했다는 점도 지적한다. 자본의 소유여부에 따라 경제적 불평등은 확대되고, 대다수 자본을 소유하지 못 한 계층의 구매력이 하락하기 때문에 자본주의는 수정이 필요하다는 생각이다. (위키디피아 그림으로 보는 피게티의 21세기 자본 3분 요약 참조)

[도표 71] 자본수익률>경제성장률>노동수익률, 불평등 확대



[도표 72] 미국과 유럽의 경제적 불평등 확대



자료:「21세기 자본」토마 피게티

존 메이나드 케인즈의 정부개입과 기업가 정신, 조셉 슘페터의 창조적 파괴

존 메이나드 케인즈(1883~1946)와 조셉 슘페터(1883~1950)는 칼 마르크스가 세상을 떠난 해에 태어났다. 마르크스에 의해 자본주의에 대한 경고가 있던 시기였고, 1차 세계대전과 대공황을 겪으면서 실제로 자본주의가 위기에 빠지던 시기였다. 케인즈는 정부개입을 통한 자본주의의 극복, 슘페터는 창조적 파괴에 의한 자본주의의 몰락을 예고했다.

케인즈는 시장 기능에 의존하는 자본주의는 생명력이 없으며 시장의 자동조절 기능을 믿지 않았다. 케인즈 저축이 투자로 이어지지 않아 수요가 부족해질 것을 걱정했다. (이 때 유동성 함정과 디플레이션이 발생) 케인즈는 정부 지출의 기본적 기능을 투자 수요의 부족을 메우는 것이라 생각했다. 불황이 발생할 때 정부가 적극적으로 시장에 개입해서 효율적인 투자를 만들 수 있다고 봤다. 케인즈는 기업가 정신을 Animal Sprit 이라고 부르며 칭송했다. 기업가 정신은 투자의 근간이며 자본주의를 지탱하는 원동력으로 봤다. 케인즈는 기업가 정신을 유지시킬 거시경제적 환경 조성을 주장했다.

슘페터는 자본주의의 원동력은 기업가의 혁신과 창조적 파괴라고 보았다. 혁신은 생산력의 결합에 일어난 변화이며, 1) 새로운 재화 또는 새로운 품질의 재화 생산, 2) 새로운 생산방법의 도입, 3) 새로운 판로의 개척, 4) 원료 혹은 반제품의 새로운 공급원 획득, 5) 새로운 조직의 실현(트러스트의 형성이나 독점의 타파)으로 나타난다.

슘페터는 기업가와 사업가를 구분했다. 기업가는 현실의 상태를 뒤흔드는 (요즘 표현으로는 벤처) 혁신을 하고, 사업가는 모방을 통해 정태적 이윤창출에 가담할 뿐이다. 창조적 파괴는 기업가에 의해서 전개되는데, 이는 단순히 시장경쟁에 가담한 이윤 확보가 아닌, 기존 제품이나 서비스 등의 체제를 파괴하고, 새로운 시장과 방식을 창조하는 과정으로 봤다. 예를 들면 자동차가 만들어지면서 마차가 없어지는 것이다.

슘페터는 자본주의는 몰락하고, 사회 민주주의로 바뀔 것으로 예견했다. 자본주의의 발전은 기업가의 혁신과 창조적 파괴에 있어 내적 동기가 필요하다. 그러나 기업가의 혁신과 창조적 파괴에 의한 경제성장의 수혜로 인한 비판적 사고가 자본주의 체제로 확대되고 이에 따라 기업가의 혁신과 창조적 파괴의 내적 동기가 소멸되기 때문이다. (「조셉 슘페터-고고한 경제학자」 이토 미쓰하루, 네이 마사히로 저 참조)

프리드리히 하이에크의 「노예의 길」, 밀튼 프리드만의 통화 준칙주의

프리드리히 어거스트 본 하이에크(1899~1992)는 제2차 중앙집권과 계획경제를 비판한 정치경제학자다. 제2차 세계대전이 끝나갈 무렵, 영국에서는 민주의회 승인을 받은 경제계획을 통해 경제전체를 통합, 조직해 궁극적으로 더 큰 평등과 직업 및 소득의 보장과 같은 사회주의 이상을 민주주의와 함께 실천할 수 있다는 생각들이 인기를 끌었다. 전시, 무기개발 위한 과학자들의 동원이 빠른 기술진보를 이루었기 때문이다.

하이에크는 경제 전체를 조직화하려는 사상적 흐름이 궁극적으로 독일에서 '나치'를 등장시키고, 소련에서 '레닌주의'와 '스탈린주의'로 도달했음을 보고, 사회주의의 길은 '자유'의 길은 '독재'와 '노예'로 가는 길임을 알리기 위해 「노예의 길(Road to Serfdom」을 저술했다. 하이에크의 자유주의는 '대처리즘'과 '레이거노믹스'로 시작되는 신자유주의의 토대를 제공했다. (네이버 책 「노예의 길」 출판사 서평 참조)

밀튼 프리드만(1912~2006)은 하이에크와 함께 신자유주의를 대표하는 경제학자다. 그는 통화주의(Monetarism) 학파를 만들었고, 1970년대 이후 주류 경제학에 지대한 영향을 끼쳤다. 자유시장 내 정부의 역할이 축소되었다고 주장하면서 시장의 장점과 정부개입의 단점을 강조했다. 프리드만의 정치철학은 미국 보수주의자와 자유주의자들의 견해에 큰 영향을 미쳤다. 프리드만은 '흔들림 없는 자유주의자', '통화주의의 대부', '작은 정부론의 기수', '반 케인즈 학파의 창시자' 등 다양한 호칭이 따라 다닌다.

프리드만의 주장은 케인즈의 시장개입주의에서 시작한다. 국민경제에서 중요한 것은 케인지안들의 생각처럼 경제불황은 투자수요 부족, 과잉저축에서 발생하는 것이 아니라 통화량의 변동에서 발생한다. 통화량이 증가하면 경기가 과열되고, 통화량이 축소하면 경기가 위축되는데, 이 때 정부가 개입하면 더 큰 부작용을 초래한다는 것이다. 프리드만의 정부 및 중앙은행의 시장개입을 샤워기 온도조절 비유는 유명하다. 프리드만은 정부의 잘못된 통화정책이 통화교란을 낳고 다시 경제교란이 초래된다고 봤다.

프리드만이 주장한 화폐정책의 핵심은 정부 및 중앙은행이 일정한 통화증가율을 공시하고 이를 장기에 걸쳐 매년 철저하게 준수하는 준칙이다. 특정비율을 정한 간단한 준칙이라는 점에서 k% 준칙이라 불린다. 중앙은행은 이 준칙만 지키고 나머지는 민간에 맡기면 통화량의 급격한 변동 발생으로 인한 경기변동 및 혼란을 예방하고, 미래의 불확실성을 낮춰 경제주체들이 장기적인 계획에 입각한 합리적인 활동을 할 수 있게 된다는 것이다. 프리드만의 이러한 통화 준칙주의 제안은 통화량 목표제, 이자율 목표제로 나아가 중앙은행의 정책운용에 있어 중요한 기준이 되었다. (위키디피아 밀튼 프리드만 참조)

에르난도 데 소토의「자본의 미스터리」

에르난도 데 소토(1941~)는 페루의 경제학자로 제3세계와 과거 사회주의 국가들의 빈곤에 관한 연구를 활발히 진행 중이다. 그는 세계무역기구의 이코노미스트였으며, 알베르토 후지모리 전 페루 대통령의 경제자문역을 맡아 경제개혁 작업에 참여했다.

소토는 자본(Capital)의 어원의 의미를 파악했다. 중세 라틴어에서 자본(Capital)이란 단어는 가축의 머리를 지칭했던 듯 하다. 그 당시 가축은 단순히 고기가 아닌 중요한 부의 원천이었다. 가축은 이동할 수 있기 때문에 위험 요소에서 격리할 수 있고, 숫자를 파악할 수 있어 관리하기가 편했다. 더욱 중요한 점은 가축은 우유, 가죽, 양모, 고기, 연료 등 잉여가치를 창출할 수 있으며, 출산을 통해 새끼도 얻을 수 있다. 즉 자본은 자산의 물리적 차원과 잉여가치를 창출하는 특징을 가진다. 소토는 자본(Capital)은 잉여생산을 유발하고 생산성 향상을 촉진하는 국가의 자산으로 정의한다.

소토의 생각에 자본과 화폐가 혼용되고 있다. 자본은 가치순환의 고리이며, 화폐는 자산들을 교환할 기준을 제공하는 매개체에 불과하다. 제3세계와 과거 사회주의 국가들은 충분한 자본을 창출하지도 못 하면서, 화폐 때문에 발생하는 인플레이션으로 인해 심각한 경제 난을 겪게 된다. 서구 자본주의 국가들의 실정은 제3세계나 과거 사회주의 국가들보다는 나았지만, 최근 글로벌 금융위기 이후 유사한 상황에 직면하고 있다.

자산을 고정시켜 자본으로 인식하게 해 주는 여러 형태의 규칙에 의한 전환과정이 바로 합법적인 소유권이 명시된 재산(Property)이다. 합법적인 재산 체제는 자본이 탄생되는 곳이다. 소토는 합법적인 재산 체제로 1) 자산의 경제적 잠재력을 고정, 2) 산재한 정보를 하나의 체제로 통합, 3) 책임소재를 명확히 밝힘, 4) 자산을 대체 가능한 형태로 전환, 5) 수많은 사람들을 네트워크로 연결, 6) 거래를 보호하는 효과가 있다고 한다.

소토는 현재의 자본주의가 소수의 세계화된 엘리트에게만 문호를 개방하고, 대다수를 배제하는 현실을 타개하지 않은 개방경제의 개혁은 의미가 없다고 주장한다. 자본주의의 차별적인 재산체제를 폐지하고 경제학과 법의 경계를 초월해야만 한다고 한다. 자본주의 자체보다 더 중요한 문제는 가난한 사람들에 대한 배려와 자유이고, 사회계약과 동등한 기회에 대한 존중이라고 말한다. 이러한 목표를 달성할 때까지 자본주의는 그저 특정 계층을 위한 게임에 불과하다는 자본주의의 한계를 주장한다. (네이버 블로그 이광중 회계사, 경제와 금융/에르난도 데 소토 <자본의 미스터리> 윤영호 옮김 참조)

에필로그, 블록체인 3.0과 제4의 물결

앨빈 토플러가 예견한 부의 미래

금세기 최고의 미래학자 앨빈 토플러(1928~2016)는 인류의 역사를 3개의 물결로 구분했다. 제 1의 물결은 1만 년 전에 시작되어 수천 년에 걸쳐 인류의 문명을 서서히 바꾼 농업혁명, 제2의 물결은 300년이라는 비교적 짧은 시간에 인류를 변화시킨 산업혁명이다. 제3의 물결은 1950년대 중반에 시작되어 현재까지 계속되고 있는 지식혁명의 물결이다. 짐작하듯이 점차 문명 변화의 주기는 급속도로 짧아지고 있다.

토플러는 마지막 저서인 '부의 미래 (Revolutionary Wealth)'에서 다가올 미래를 예측했다. 토플러가 말하는 부(富, wealth)는 손으로 만질 수 있는 화폐가 아니다. 부는 인간의 욕망을 채워주고, 욕구를 해소시켜 주는 그 무엇이다. 토플러는 "미래의 부는 시간, 공간, 지식의 세 가지 심층기반(deep fundamental)이 어우러져 만들어진다."고 말한다.

첫째 기반은 '시간'이다. 토플러는 시간을 고속도로를 달리고 있는 자동차에 빗대어 말했으며, 자동차의 속도는 변화의 속도를 의미한다. 시속 160km로 가장 빨리 달리는 자동차는 '기업', 다음은 140km의 '시민단체', 95km의 '가족', 50km의 '노동조합', 40km의 '정부관료 조직', 15km의 '학교', 8km의 '국제기구', 5km의 '정치조직', 1.5km로 가장 느린 '법'의 순서다. 미래사회에서는 속도를 맞추는 일, 즉 동시화(synchronization)가 중요하며 또 다른 측면에서는 융합(convergence)를 의미하기도 한다.

둘째 기반은 '공간'이다. 교통과 인터넷이 발달하면서 지구는 하나의 마을로 비유할 수 있을 만큼 좁아졌다. 세계화(globalization)로 인해 국경의 의미가 점차 사라지고, 비즈니스나 시장뿐 아니라 직업까지도 세계를 무대로 하게 되면서 개인이 선택할 수 있는 공간의 범위는 더욱 넓어졌다. 이 역시 융합(convergence)의 개념을 내포한다.

셋째 기반은 '지식'이다. 오늘날 부의 창출은 점점 더 지식에 의존하고 있다. 지식은 '미래 경제의 석유'라 할 정도로 중요하다. 매장량이 한정된 석유는 쓰면 쓸수록 줄어들지만 지식은 무한하며 사용할수록 더 확장된다. 지식혁명 시대에 부를 창출하는 에너지원을 바로 무한한 지식이다. 지식 또한 융합(convergence)되면 더 강해진다.

토플러는 '미래에는 지금 우리가 상상하지도 못 하는 엄청난 일들이 벌어질 것'이라고 예측한다. 제 3의 물결에 이어 제 4의 물결이라 불릴만한 혁명적인 변화의 물결이 전개될 것이기 때문이다. (네이버 지식백과, 제4의 물결) 제 4의 물결은 '시간', '공간', '지식'이 융합되는 과정에서 새로운 부가 창출되는 과정으로 예견된다. 블록체인 기반의 거래체계에서는 '지식'이 '시간'과 '공간'의 장벽을 넘어 부를 창출하고, 이에 대해 장벽 없이 참여할 수 있다. 물론 가치가 있는 작업인지에 대한 혜안은 필요하다.

비탈릭 부테린의 비전, 크립토 3.0의 세계

이더리움의 창시자 비탈릭 부테린은 현재 블록체인의 리더라고 해도 과언이 아니다. 그는 블록체인 체계가 제대로 자리 잡을 수 있도록, 자신의 비전을 명확하기 밝히고 세계와 소통하고 있다. 따라서 그의 비전이 향후 블록체인의 미래가 될 것이다.

비탈릭 부테린은 암호학 진전을 3단계로 구분하고 있다.(본 자료의 블록체인 1, 2, 3 단계의 구분도 비탈릭 부테린의 구분을 따른 것이다. 비탈릭 부테린은 블록체인 1.0, 2.0, 3.0이 아닌 크립토 1.0, 2.0, 3.0으로 표현하고 있다.) 크립토 1.0은 사토시 나카모토가 2009년 1월 비트코인을 세상에 선보인 이후 4년간이다. 비트코인은 분권화 체제에서 강력한 보안과 사실입증을 신뢰할 프로토콜을 내 놓았지만, 화폐 체계에 머문 한계가 있다. 크립토 2.0은 다양한 애플리케이션으로 금융거래, 크라우딩펀딩 등으로 확장되었다. 비탈릭 부테린은 튜링완전 블록체인 컴퓨팅, 암호학적 기술을 사용한 탈중앙형 네트워크, 고급 암호학 기반의 블록체인, 이 세 가지의 조합을 크립토 2.0으로 부른다.

크립토 3.0은 어떤 모습일까? 비탈릭 부테린은 크립토 2.0에서의 경향이 일부 지속될 것이며, 컴퓨팅 추상화와 프라이버시를 제공하는 보편화된 프로토콜이 나올 것으로 봤다. 그러나 그에 못지 않게 중요한 점은 확장성의 문제라고 한다. 크립토 3.0 시대에는 기존 확장성의 한계를 뛰어넘어 주류에 도입될 수 있는 시스템을 제작하는 다양한 접근 방식이 등장할 것이라고 한다. 또한 혁신적인 애플리케이션의 등장을 예상한다. 신규 비즈니스의 9할이 실패하겠지만 성공하는 1할이 많은 사람들이 사용할 완전한 상품을 내놓을 만큼 규모가 성장할 것이며, 진짜 재미는 여기서 시작된다고 예상한다. (「비즈니스 블록체인」 윌리엄 무가야 지음 / 한빛미디어 머리말)

현재 블록체인의 리더 비탈릭 부테린이 말하는 (다소 이해가 되지 않는) 크립토 2.0과 3.0에서 나타날 변화를 수용하기 위해서는 블록체인에 대한 깊은 관심이 필요할 것이다. 성공적인 과정으로 전개된다면 탈중앙화된 세계에서 개인의 개성과 인권이 보호되고, 현재 자본주의의 맹점인 불평등과 정보의 비대칭성에 따른 비효율이 제거되며, 기업가 정신의 혁신과 창조적 파괴가 샘솟고, 정의로운 자본주의가 제대로 실현되는 토대가 될 것이다. 통화관리 측면에서는 밀튼 프리드만의 준칙주의 실현이다.

어쩌면 앨빈 토플러가 예견한 제4의 물결이 도래하는 시작이며 「블록체인 혁명」의 저자 돈 탭스콧이 예상하는 번영된 세계로 향하기 위해(Transformation for a prosperous world), 부를 재분배하기보다는(Rather than re-distributing wealth), 부를 원천적으로 배분하기 위해(could be pre-distribute wealth), 애초에 부가 창출되는 방법을 변화시켜, 부를 창출을 민주화하고(could be democratize the way that wealth gets created in the first place), 경제활동에 더 많은 사람들을 참여시키고(engaging more people in the economy), 공정한 보상을 받을(receive fair compensation) 시스템이 창출될 수 있다.

[도표 73] 앨빈 토플러의 인류문명 구분 중심의 세계사 연표, 제 3 의 물결은 정보기술, 제 4 의 물결은 블록체인이 요체

기원전	사건	기원 후	사건	IT 기술	기원 후	사건	IT 기술
400 만 년 전	오스트랄로 피테쿠스	1765 년	와트, 증기기관 완성		1966 년	중국, 문화 혁명	
160 만 년 전	호모 에렉투스	1776 년	미국 독립선언		1967 년	제 3 차 중동 전쟁	
40 만 년 전	불의 사용	1789 년	프랑스 혁명, 인권 선언		1969 년	아폴로 11 호 달착륙	
4 만 년 전	호모 사피엔스	1804 년	나폴레옹 황제 즉위		1971 년	중국, UN 가입	Xerox, Intel, Apple
1 만 년 전	농경과 목축 시작	1806 년	신성로마제국 멸망		1972 년	중국, 닉슨 방문	
3500 년	메소포타미아 문명	1834 년	독일, 관세동맹 성립		1978 년	소련, 아프가니스탄 침공	
3000 년	이집트 문명	1863 년	링컨, 노예해방 선언		1980 년	이란, 이라크 전쟁	IBM, MS, Apple
2500 년	인더스 문명	1868 년	일본, 메이지 유진			앨빈 토플러, 제 3 의 물결 저술	MS-DOS
2000 년	황하 문명	1869 년	수에즈 운하 개통		1986 년	소련, 체르노빌 원전 사고	Macintosh
1200 년	알파벳 발명	1871 년	비스마르크, 독일 통일		1987 년	미국, 소련 중거리 핵전력 폐기협정 조인	
6 세기 경	석가모니 탄생	1876 년	벨, 전화기 발명		1989 년	베를린 장벽 붕괴, 천안문 사건	
330 년	알렉산더 대제국 건설	1877 년	인도 제국 성립	기계식 계산기	1990 년	독일 통일	World Wide Web
221 년	진나라 중국 통일	1896 년	제 1 회 올림픽 개최		1991 년	걸프 전쟁, 유고 내전, 소련 해체	ARPANET→Internet
27 년	로마 제국 성립	1905 년	러시아, 피의 일요일		1993 년	유럽연합(EU) 출범	MS Windows
기원 후		1912 년	중화민국 성립		1994 년	아마존, 전자상거래 시작	
0 년	예수 그리스도 탄생	1914 년	제 1 차 세계대전		1995 년	세계무역기구(WTO) 출범	Linux OS
313 년	로마, 크리스트교 공인	1917 년	러시아 사회주의 혁명		1997 년	영국, 중국에 홍콩 반환	Yahoo
392 년	로마, 크리스트교 국교 승인	1918 년	미국 윌슨, 14 개조 평화원칙 발표			넷플릭스 설립	
500 년	인도, 힌두교 창시	1921 년	중국 공산당 성립		1999 년	유럽 11 개국, 유로화 채택	Google
570 년	모함마드 탄생	1922 년	이탈리아, 파시스트 성립		2001 년	미국 911 테러	
618 년	중국 당나라 건국	1929 년	세계 경제 대공황		2002 년	중국 주석 교체	
962 년	신성로마제국 탄생	1933 년	독일, 나치 정권 수립	알랜 튜링 계산 불가능성 연구	2003 년	이라크 전쟁	
1054 년	크리스트교, 동서 분열	1937 년	중, 일 전쟁			마크 주커버그, 페이스매시 서비스 시작	SNS
1215 년	영국 대헌장 제정	1939 년	제 2 차 세계대전		2004 년	페이스북 설립	
1375 년	르네상스 시작	1941 년	태평양 전쟁	전자식 컴퓨터	2007 년	애플 아이폰 출시	Smartphone
1492 년	콜럼버스, 신대륙 발견	1943 년	최초의 컴퓨터 에니악 발명		2008 년	글로벌 금융위기	
1498 년	바스코 다가마, 인도 항로 발견	1945 년	독일, 일본 항복		2009 년	연준, 1 차 양적 완화	
1517 년	루터의 종교 개혁	1948 년	이스라엘 공화국 성립, 세계인권선언		2009 년	사토시 나카모토, 비트코인 백서 발표	Crypto currency
1543 년	코페르니쿠스, 지동설 주장	1950 년	UN, 한국 파병 결의	프로그래밍 언어	2010 년	유럽 재정위기	
1590 년	도요토미 히데요시, 일본 통일	1960 년	아프리카 17 개국 독립	IBM, DEC, Bell	2011 년	연준, 2 차 양적 완화	
1600 년	영국, 동인도 회사 설립	1961 년	베트남 전쟁	개인용 컴퓨터	2013 년	연준, 3 차 양적 완화	
1616 년	중국 청나라 건국	1963 년	미국, 영국, 소련 부분적 핵실험 금지 조약 체결		2015 년	비탈릭 부테린, 이더리움 백서 발표	Blockchain

자료: 네이버 지식백과, 교보증권 리서치센터 정리

주요 참고 자료 - 문헌

「블록체인 혁명 / Blockchain Revolution」, 돈 탭스콧, 알렉스 탭스콧 지음 / 박지훈 옮김/ 박성준 감수 / 을유문화사

「비트코인, 블록체인과 금융의 혁신 / Mastering Bitcoin: Unlocking Digital Crytocurrencies」, 안드레아스 M. 안토노폴리스 지음 / 최은실, 김도훈, 송주한 옮김 / 코인플러스 기술감수 / 고려대학교 출판문화원

「비트코인 현상, 블록체인 2.0 / The Age of Crypto Currency」, 마이클 J. 케이시, 폴 비냐 지음, 유현재, 김지연 옮김 / 미래의 창

「비즈니스 블록체인 / Business Blockchain」 윌리엄 무가야 지음 / 박지훈, 류희원 옮김 / 한빛미디어

「분산원장 기술과 디지털통화의 현황 및 시사점」 한국은행 김동섭, 2016년 1월

「분산원장 기술의 현황 및 주요 이슈」 한국은행, 공동연구 2016년 12월

「디지털 혁신과 금융서비스의 미래: 도전과 과제」 한국은행, 2017년 1월

「비트코인의 진화와 생태계 내전(Civil War)」 산업은행 강준영, 2017년 8월

주요 참고 자료 - 동영상

「블록체인 혁명」 https://www.youtube.com/watch?v=4IrpEUvaRBM

「[TMook] 블록체인의 개념」 https://www.youtube.com/watch?v=662wnupq8fg

「이더리움이 뭔가요? 일반인을 위한 블록체인 강좌 block15」 https://www.youtube.com/watch?v=uUC3hELa-Oo

「EthStrong(한재영)의 이더리움(Ethereum) 블록체인 바로알기」 https://www.youtube.com/watch?v=uHFTAa-X24Q