

블록체인

이상과 현실, 어디쯤 와 있나



▶Analyst 김열매 | fruitism@hanwha.com | 02-3772-7657

“ 많은 기업이 블록체인에 뛰어들고 있다는 기사가 연일 보도되고 있습니다. 언론의 관심과 암호화폐 시장의 투자열기가 뜨거운 반면 사용자 입장에서 체감할 만한 변화는 아직 보이지 않습니다. 블록체인에 관심있는 투자자들이 블록체인의 기본 개념을 이해하고 현재 기술 수준과 논란의 쟁점을 들여다보며 이 기술을 유용하게 쓸 수 있는 방법과 미래에 대해 함께 고민해 보자는 취지에서 이 보고서를 작성했습니다. ”

| Contents |

I. 블록체인에 주목해야 하는 이유.....	03	VII. 블록체인과 디지털 경제, 그리고 크립토 에셋.....	45
II. 블록체인으로 구현된 1세대 암호화폐, 비트코인.....	04	1. 블록체인과 암호화폐, 분리할 수 있을까?.....	45
1. 탈중앙화 결제 네트워크.....	04	2. 비트코인은 미래의 화폐가 될 수 있을까?.....	46
2. 비트코인의 핵심기술.....	05	3. 디지털 경제의 시대, 새로운 자산으로 등장하는 크립토 에셋.....	53
3. 작업증명(PoW) 방식의 합의 알고리즘.....	09	4. 밀레니얼 세대는 게임같은 금융상품을 원한다.....	55
4. 비트코인에 제기되는 논란: 마이닝 풀(Mining Pool).....	11	5. 디지털 트랜스포메이션, 그리고 디지털 경제의 확장.....	56
5. 비트코인 하드포크와 비트코인 캐시의 탄생.....	13	6. 비트코인 선물거래 개시, 디지털 금(Gold)이 될 가능성.....	58
III. 블록체인 생태계의 확산, 이더리움.....	15	VIII. 크립토 버블에 대한 생각.....	60
1. 스마트 계약을 구현할 수 있는 새로운 프로토콜.....	15	1. 툴립버블, 닷컴버블과 비교한 암호화폐 버블.....	60
2. 스마트 컨트랙트와 EVM.....	17	2. ICO 참여 전 생각해볼 질문들.....	63
3. 토큰(Token)과 ICO(Initial Coin Offering).....	19	IX. 블록체인, 과연 세상을 바꿀 기술인가?.....	66
4. 탈중앙화 어플리케이션(DApp)과 디지털 소유권 거래.....	21	1. 잘 돌아가고 있는 기존 인프라를 바꿀 필요는 없다.....	66
IV. 퍼블릭, 프라이빗, 그리고 컨소시엄 블록체인.....	23	2. 신흥국을 움직일 블록체인.....	67
1. 퍼블릭(Public) 블록체인.....	23	3. 부패한 중개자를 배제한, 신속하고 투명한 원조.....	69
2. 프라이빗(Private) 블록체인.....	24	4. 블록체인이 바꾸는 사회, 탈중앙화와 검열저항성.....	70
3. 컨소시엄(Consortium) 블록체인.....	24	5. 초연결사회, 4차 산업혁명의 핵심이 될 블록체인.....	72
V. 블록체인에 대한 주요 국가 동향.....	26	6. 블록체인이 해결해야 할 과제: 기술은 번영을 보장해주지 않는다.....	74
1. 블록체인과 암호화폐에 대한 국가별 동향.....	26	X. 불임.....	77
2. 에스토니아 디지털 시민권.....	30	1. 암호화폐 시가총액과 시장점유율.....	78
3. 스위스 크립토 밸리.....	32	2. 비트코인 주요차트.....	80
VI. 블록체인 기반의 비즈니스 사례.....	34	3. 이더리움 주요차트.....	81
1. 다양한 분야의 스타트업.....	34		
2. 빔(VEEM)의 국제 송금 서비스.....	37		
3. 마이크로그리드에 블록체인 기술을 결합한 에너지 P2P 거래.....	38		
4. 영상, 음악 등 디지털 콘텐츠 거래와 저작권 수익 배분.....	39		
5. 중개자가 없는 글로벌 상거래 플랫폼.....	40		
6. 글로벌 기업들의 블록체인 추진 현황.....	43		

I. 블록체인에 주목해야 하는 이유

- 데이터 기술의 시대** 2015년에 마윈 알리바바 회장은 ‘세상은 지금 IT(Information Technology, 정보기술) 시대에서 DT(Data Technology, 데이터기술) 시대로 가고있다.’고 말한 바 있다. 그의 예견대로 데이터가 새로운 석유이자 자원인 시대가 도래하고 있다. 어쩌면 이미 와버린 미래인지도 모른다. 블록체인은 데이터 기술의 시대를 사는 우리가 반드시 주목해야 할 기술 중 하나다.
- 데이터 독점 기업의 출현** IBM은 전 세계에서 사용하는 컴퓨팅 장치가 2014년 약 100억 개에서 2020년에는 약 250억 개, 2050년에는 1천억 개로 증가할 것이라고 전망했다. 현재까지 사물인터넷은 클라우드 컴퓨팅에 기반을 두고 발전해 왔다. 이대로라면 연결되는 기기가 많아질수록 중앙 서버 역할을 하는 대규모 데이터 센터가 필요하다. 비용이 많이 들 뿐 아니라 확장성과 보안성, 그리고 데이터 독점에 대한 우려가 존재한다. 모든 사물을 컨트롤하는 데이터 센터가 해킹을 당하면 도시 전체가 마비될 지도 모르며 데이터 독점 기업이 국가를 뛰어넘어 사회 전반에 막대한 영향력을 행사하게 될 지도 모른다.
- 데이터 독점에 대한 대안** 블록체인은 데이터 독점에 대한 대안이 될 수 있을 것이다. 블록체인 기술을 적용하게 되면 개별 기기 스스로가 블록체인의 노드로 작동하게 되며 중앙에 대형 서버가 불필요해진다. 참여 노드가 많아질수록 데이터의 위변조도 어렵다.
- 초연결사회의 기반기술이 될 블록체인** 자율주행과 사물인터넷(IoT) 등 초연결사회(Hyper-connected society)를 구현하는데 블록체인은 기반 기술이 될 전망이다. 인터넷·통신 기술의 발전으로 사람과 사람이 연결되었다면 앞으로의 사회는 사람과 사물, 사물과 사물 간에 연결되어 자동으로 컨트롤 되는 사회가 될 것이다. 사람이 배제된 기계간(Machine to Machine) 거래도 가능해질 것이다. ‘비즈니스 블록체인’의 저자 윌리엄 무가야는 블록체인 기술이 월드와이드웹 이후 가장 혁신적인 인터넷 기술이라고 말한다. 웹이 IT 생태계를 뒤흔들고 다양한 산업에 변화를 불러왔듯 블록체인 역시 중앙집중형 시스템 체제에 변화를 예고하고 있다.

[그림1] IBM은 2025년 이후 사물인터넷이 분산 네트워크로 연결될 것이라고 전망



자료: IBM, 한화투자증권

II. 블록체인으로 구현된 1세대 암호화폐, 비트코인

1. 탈중앙화 결제 네트워크

블록체인을 이해하려면
비트코인을 먼저 봐야 한다.

블록체인을 이해하기 위해서는 비트코인을 먼저 들여다볼 필요가 있다. 비트코인은 블록체인 기술로 구현된 1세대 암호화폐다. 비트코인 이전에도 디지털 암호화폐는 존재했지만 블록체인 기술에 기반한 것은 아니었다.

비트코인은 익명의 사토시 나카모토(Satoshi Nakamoto)가 글로벌 금융위기 발생 직후인 2008년 11월, 백서(Bitcoin: A Peer-to-Peer Electronic Cash System)를 공개함으로써 세상에 등장했다. 제 3자를 배제하고 네트워크에 참여하는 개인 간에 거래하고 그 정보를 함께 검증, 기록하는 시스템이다. 중앙은행이 보증하는 법정화폐와 달리 중앙집권적인 통제, 관리 기구가 없다는 점이 비트코인의 가장 큰 특징이다.

새로운 지불 시스템

'Bitcoin.org' 웹사이트에서는 비트코인을 '새로운 지불 시스템'이자 '완전한 디지털 화폐를 가능하게 하는 합의된 네트워크'라고 설명하고 있다. 비트코인 소프트웨어를 다운로드 받아 네트워크에 연결되어 있는 참여자들을 노드라고 부르는데 각각의 노드는 모두가 비트코인 네트워크 상에서 생성된 거래 데이터를 공유하고 각자 저장한다. 전세계 곳곳에서 거래한 기록을 동시에 여러 대륙에 퍼져 있는 참여자 노드들이 검증하고 모두가 다 같이 블록 단위로 추가 생성되는 원본을 저장한다. 이러한 설명을 들으면 다음과 같은 의문이 생길 것이다.

거래 기록의 프라이버시를 어떻게 지킬 것인가?

무한정 발생하는 수많은 거래 기록을 개인 PC에 저장할 수 있을까?

비트코인 네트워크는 암호화(Cryptography)와 분산네트워크를 통해 이 두 가지 문제에 대한 해결책을 제시했다. 이에 대해 좀더 살펴보자.

[그림2] 비트코인 백서

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
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 financial institution. Digital signatures 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 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.

자료: Bitcoin whitepaper, 한화투자증권

2-1. 비트코인의 핵심기술(1) 암호화 기술(Cryptography)

프라이버시 문제 네트워크 상에서 모든 거래를 전파하고 참여자 모두가 공유하는 비트코인 네트워크를 상상해보자. A가 B에게 1비트코인을 전송하면 A의 잔액은 1비트코인이 줄어들고 B의 잔액은 1비트코인이 늘어난다. 이러한 거래를 있는 그대로 공유한다면 누가 얼마를 소유했는지, 누가 누구와 거래했는지 비밀이 사라지게 된다. 프라이버시 문제와 보안 문제가 발생할 것이다.

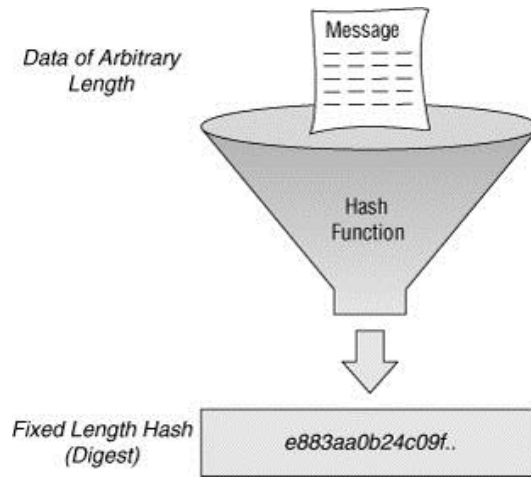
거래 절차와 방식이 투명한 것은 좋지만 내 잔액이 얼마인지를 모두에게 알리고 싶지는 않다. 그리고 내 지갑에 남아있는 비트코인을 다른 사람이 사용할 수 있게 두어서도 안 될 것이다. 비트코인은 암호화 기술을 통해 이 문제를 해결했다.

해시함수 거래 내역을 암호화 하는 데 해시 함수가 쓰인다. 해시 함수는 비트코인뿐 아니라 정보 보안 분야에서 널리 쓰이는 함수로 데이터를 정해진 길이의 무작위 문자열로 치환하는 함수다. 동일한 데이터를 입력하면 해시 함수의 결과값이 항상 동일하게 나타나고, 입력하는 데이터에 아주 미세한 변화만 주어도 결과값은 완전히 다르게 바뀐다. 결과값에서 규칙성을 찾을 수 없어 역으로 입력 데이터를 추론할 수 없다. 우연히 다른 데이터를 입력했을 때 동일한 결과값이 나올 경우도 있으나 확률은 극히 낮으며 이러한 특성 때문에 입력 데이터의 추론은 더욱 불가능하다.

‘SHA-256’ 함수 비트코인에서 쓰이는 해시 함수는 ‘SHA-256’이라는 함수다. SHA(Secure Hash Algorithm) 함수는 1993년 미국 국가안보국(NSA)에서 처음으로 설계했으며 SHA-0, SHA-1, SHA-2로 점차 변형되며 발전했다. 해시 함수 ‘SHA-256’은 입력하는 데이터의 내용과 상관없이 항상 64자리의 16진법 문자열을 산출한다. 특정한 문자열이 나오게 하는 입력 데이터를 찾으려면 2^{256} 개(256비트로 나올 수 있는 모든 경우의 수)의 데이터를 일일이 확인해야 한다. 2^{256} 을 10진법으로 표시하면 10^{77} 정도다. 해시 값으로 입력 데이터를 찾는 것은 거의 불가능하다.

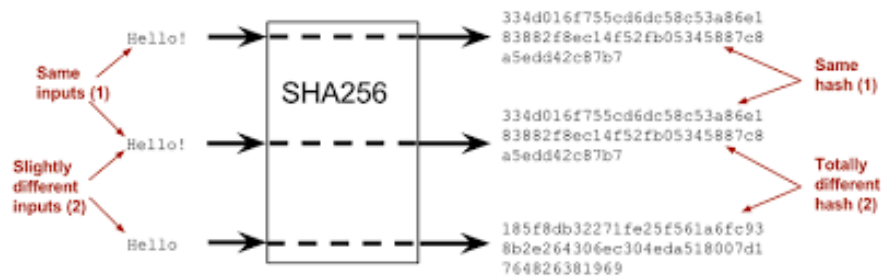
세계 모든 비트코인 거래 내역은 해시함수로 암호화 돼 일정시간마다 순차적으로 블록이 생성된다. 비트코인은 공개된 퍼블릭 분산원장으로서 비트코인 주소 간에 발생한 거래 내역을 어느 누구나 확인할 수 있다. 그리고 암호화된 주소가 누구의 소유인지는 장부 자체만으로 알아낼 수 없다.

[그림3] 해시 함수의 개념도



자료: ETI, 한화투자증권

[그림4] 입력값에 미세한 차이로도 해시값은 완전히 달라짐

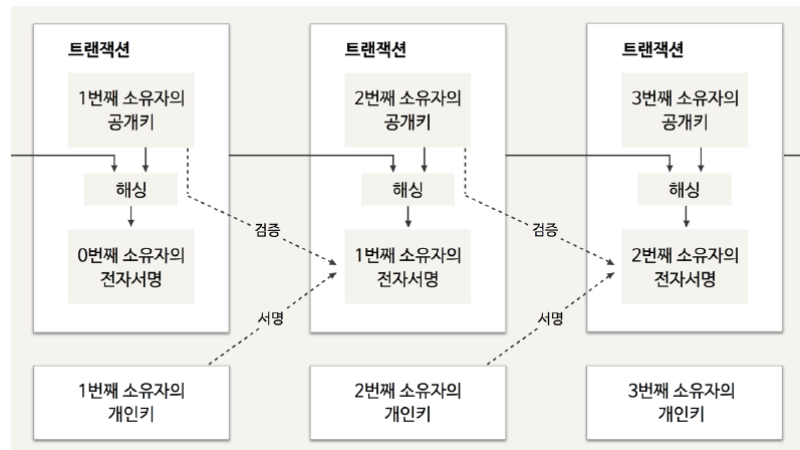


자료: 한화투자증권

디지털 서명: 개인키와 공개키

- 디지털 서명** 모두가 공유하는 원장에서 내 자산의 소유권을 증명하려면 어떻게 해야 할까? 중앙 서버에 원장을 보유하고 있는 시중은행 사이트에 접속해 내 계좌를 확인하고 송금할 때 우리는 공인인증서와 비밀번호를 사용한다. 이와 유사하게 비트코인 분산원장에서는 내가 소유한 비트코인의 주소에서 송금할 때 디지털 서명을 사용한다.
- 개인키와 공개키** 디지털 서명은 개인키(Private key)와 공개키(Public key)가 쌍으로 구성된다. 개인키는 공개키에 대한 비밀번호 같은 것으로 개인키로부터 공개키를 알아낼 수 있으나 공개키로부터 개인키를 알아낼 수는 없다. 비트코인 네트워크에서 송신자는 '거래 내역'과 '자신의 개인키로 암호화한 디지털 서명' 두 가지를 동시에 수신자에게 보낸다. 수신자는 디지털 서명이 된 데이터를 송신자의 공개키로 복호화하고 이를 같이 받은 거래 내역과 대조하여 일치하는지를 체크함으로써 전송 과정에 위변조가 없는지를 검증한다.
- 체인으로 연결** 비트코인 블록체인은 디지털 서명의 체인이다. 코인 소유자는 거래 내역에 디지털 서명을 한 후 다음 사람에게 전달하고 이를 받은 사람은 자신의 공개키를 코인 맨 뒤에 붙인다. 돈을 받은 사람은 앞 사람이 유효한 소유자였다는 것을 확인할 수 있다.
- 혹자는 양자컴퓨터 시대가 도래하면 암호화된 데이터가 모두 복호화될 수 있다고 우려한다. 하지만 그런 날이 온다면 현재 우리가 쓰고 있는 대부분의 인증, 보안 기술이 무력화될 것이다. 또한 양자컴퓨터가 상용화될 정도로 기술이 발전한다면, 블록체인 암호화에 쓰이는 암호학과 정보보안 기술 역시 함께 발전할 가능성이 높다.

[그림5] 비트코인 거래: 공개키와 개인키



자료: 한화투자증권

2-2. 비트코인의 핵심기술(2) 분산원장기술

분산 네트워크와 노드

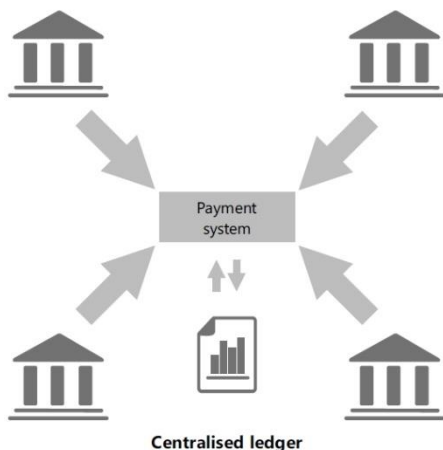
블록체인은 피어 간(Peer to Peer)에 완전하게 공유되는 분산 네트워크를 기반으로 한다. 피어(Peer)라는 의미는 네트워크에 참여하는 개인이 서로에게 동료이자 동등한 지위를 가지고 있는 것으로 볼 수 있으며 모든 노드(node)가 네트워크를 함께 공유하는 것을 의미한다. 인터넷 상에서 일반적으로 사용하고 있는 서버-클라이언트 방식의 경우 중앙 서버에 모든 원본 데이터를 저장하는 반면, 블록체인은 분산된 서버로서 네트워크 참여자들 모두가 각각 전체 원장을 공유하고 보관한다.

블록체인을 암호화폐가 존재하지 않는 분산원장만 개발하자고 한정한다면 분산형 데이터베이스와 큰 차이가 없다는 주장이 타당할 수 있다. 데이터베이스를 여러 개의 노드에 분산해 저장하는 기술은 블록체인 이전에도 존재했던 기술이며 지금도 클라우드 컴퓨팅과 함께 발전하고 있는 기술 중 하나다.

비트코인에 적용된 암호화 기술과 분산 원장 기술 각각만 놓고 보면 대단한 혁신이라고 보기 어려울 수 있다. 각각의 요소기술은 오래 전부터 존재했고 여전히 발전하고 있는 기술이기 때문이다. 하지만 비트코인이 혁신이 될 수 있었던 것은 이미 존재하는 요소 기술들을 잘 융합함으로써 새로운 방식의 소통 방식을 성공하게 했다는 것이다.

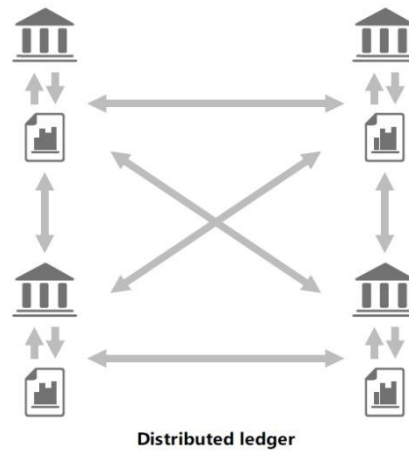
비트코인은 서로 모르는 사람 또는 기계 간에 중앙집권적 기관이나 서버 없이도 정보를 교환하고 장부에 기록할 수 있게 만들었다. 서로는 모르는 상태에서 네트워크에 전파되는 정보가 사실인지 거짓인지 어떻게 확인하고 기록할 수 있을까? 이를 이해하기 위해서는 비트코인의 채굴 방식을 이해할 필요가 있다.

[그림6] 중앙집중식 서버-클라이언트 방식



자료: BIS, 한화투자증권

[그림7] 분산원장 네트워크 방식



자료: BIS, 한화투자증권

3. 작업증명(PoW) 방식의 합의 알고리즘

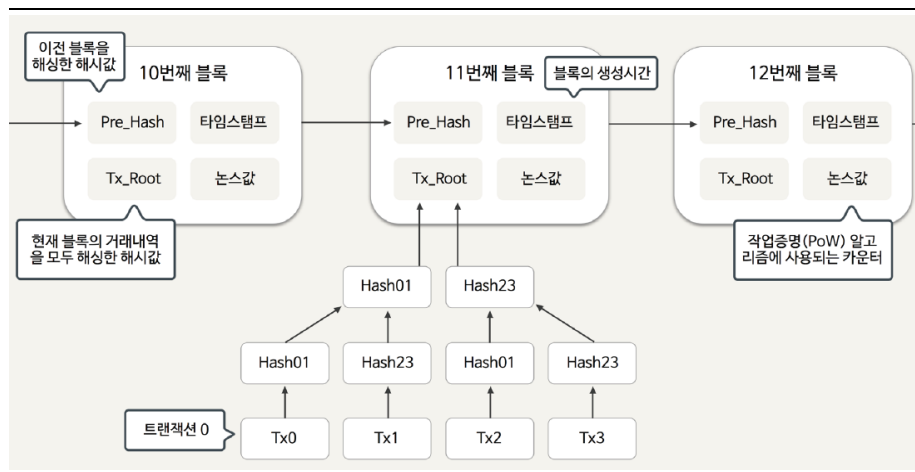
비트코인 채굴 새로운 비트코인을 취득하기 위해서는 채굴(mining)이라는 작업을 해야 한다. 채굴이란 비트코인 입출금 거래내역을 검증하고 이를 담은 신규 블록을 생성하는 작업이다. 신규 블록을 생성하는 채굴자에게 채굴 보상으로 새로운 비트코인이 발행된다. 채굴에 참여하는 모든 참가자는 거래 내역을 해시 함수로 돌려 시스템이 요구하는 목표값을 찾기 위해 경쟁을 벌인다.

작업증명(PoW) 목표값을 찾는 작업을 작업증명(Proof of Work)라고 하며 이는 끊임없는 해싱 작업을 통해 이뤄진다. 채굴자들은 직전 블록의 해시값과 미승인 거래기록(UTXO; Unspent Transaction Output)에 논스(nonce)라 불리는 임의의 숫자를 입력함으로써 새로운 블록의 해시값을 계산해 목표값과 비교하는 과정을 반복한다.

블록 구성 특정 참여자가 목표값을 찾는 데 성공하게 되면 블록을 발행하고 네트워크에 이를 전파한다. 블록에는 이전 블록을 해싱한 해시값, 현재 블록의 타임스탬프, 난이도(해시 목표값), 논스값, 그리고 현재 블록에 기록된 거래내역을 모두 담은 해시값이 기록된다.

채굴은 끊임없는 해싱 작업을 통해 임의로 나오는 값을 목표값과 대조해보는 작업이기 때문에 컴퓨팅 파워를 많이 투입할수록 목표값을 찾아내는 경쟁에서 성공할 가능성이 높아진다. 비트코인 채굴 초기에는 노트북 등 일반적인 개인용 컴퓨터의 연산능력으로도 채굴이 가능했으나 트랜잭션이 증가하고 채굴 노드가 증가할수록 채굴의 난이도가 높아져 전문적인 채굴용 장비가 개발, 활용되고 있다.

[그림8] 비트코인 블록체인 구성 개념



자료: 피넥터, 한화투자증권

비트코인 총 공급량 2100 만개로 제한

블록보상과 수수료

목표값을 찾아내는 참여자에게는 블록발행에 대한 보상으로 신규 비트코인과 수수료가 지급된다. 2009년에는 블록발행 보상으로 지급되는 비트코인의 양이 50비트코인이었으나 약 4년 뒤인 2013년 말부터 25비트코인으로 줄었으며 2016년 7월부터는 그 절반인 12.5비트코인으로 줄어들었다.

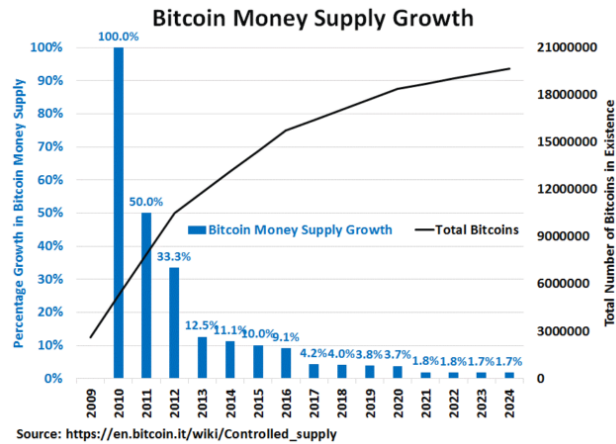
블록 하나 당 채굴되는 비트코인은 21만 번째 블록이 생성되는 약 4년마다 절반으로 줄어들도록 설계되어 있으며 총량은 2,100만 개로 제한되어 있다. 현재까지 1,702만 개 이상이 채굴되었다. ‘블록체인 혁명’의 저자 돈 탭스콧은 비트코인의 채굴이 종료되는 시점을 2140년으로 예상한 바 있다.

늘어나는 분산원장 용량, 생각보다 크지 않다.

비트코인은 2009년 1월 최초의 블록 생성 후 발생한 모든 거래 내역이 암호화되어 저장되어 있다. 암호화 기술을 통해 공개된 원장에서 익명으로 각자 본인의 거래기록을 확인할 수 있다. 게다가 해시 함수를 통해 거래기록의 용량은 현저하게 축약돼 저장된다. 비트코인은 약 1MB로 제한된 한 개의 블록에 약 2천건의 거래를 저장할 수 있으며 약 10분마다 1개씩 신규 블록이 생성된다.

지난 10년간 거래기록 전체를 보관한 분산원장의 용량은 현재 약 167GB로 개인 PC에도 보관이 가능하다. 비트코인은 현존하는 암호화폐 중 전세계에 걸쳐 가장 널리 퍼져 있는 공개된 분산원장이자 가장 오랜 기간 동안 검증된 블록체인 기반의 암호화폐다.

[그림9] 비트코인 공급



자료: Bloomberg, 한화투자증권

4. 비트코인에 제기되는 논란: 마이닝 풀(Mining Pool)

마이닝 풀의 파워 비트코인은 탈중앙화된 P2P 거래의 무결성을 추구했으나 암호화폐 채굴 풀(Pool)이 기업화되면서 특정 집단의 이해관계에 의해 휘둘리게 될 것이라는 우려가 제기된 바 있다. 비트코인 블록체인은 과반수 이상의 다수결을 참(True)으로 보는데 채굴 노드의 51% 이상을 특정 집단이 차지하게 되면 비트코인 블록체인의 장부 조작이 가능하다.

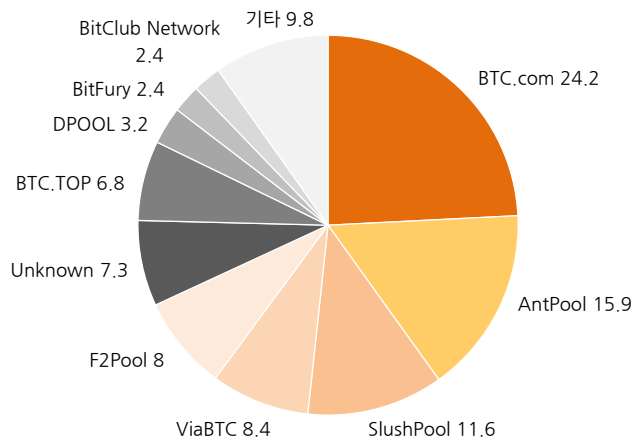
현재 비트코인 마이닝 풀의 시장 점유율을 살펴보면 상위 3개사가 약 50%를 차지하고 있고 상위 5개사의 점유율은 약 70%에 달한다. 암호화폐 시장에서 이미 대기업이 된 마이닝 풀 몇 개가 모여 담합한다면 어떻게 될까? 이론적으로는 담합에 의한 블록체인 조작이 가능하다.

51% 공격 가능성 하지만 아직까지 그런 일은 일어나지 않았다. 블록을 조작하는 것은 가능하지만 조작함으로써 얻을 수 있는 이익보다 비용이 훨씬 크기 때문이다. 게임이론으로 이를 설명할 수 있다. 네트워크를 공격하는 것과 협력하는 것 중 협력하는 것이 참여자에게 유리하다. 비트코인 장부를 조작하는데 성공하게 된다면 이는 곧 비트코인의 신뢰를 무너뜨리게 되고 이미 보유하고 있는 비트코인의 가치를 붕괴시킬 것이다.

특히 이미 기업화된 마이닝 풀은 채굴 보상뿐 아니라 수수료 수익도 얻고 있는데 네트워크가 붕괴되면 수익을 모두 포기해야 한다. 이미 150조원이 넘는 비트코인의 가치를 잃었고 이로부터 발생할 수수료 수익까지 없애는 데 동의할 채굴업자가 얼마나 나타날 수 있겠는가.

가능성은 희박하지만 물론 미래는 장담할 수 없다. 악의적인 노드의 51% 공격 가능성은 퍼블릭 블록체인에 제기되는 리스크 요인이다.

[그림10] 비트코인 채굴 풀(Mining Pool) 시장 점유율



자료: Blockchain.info, 한화투자증권

비트코인이 반갑지 않은 정부, 어려운 과제에 직면하다

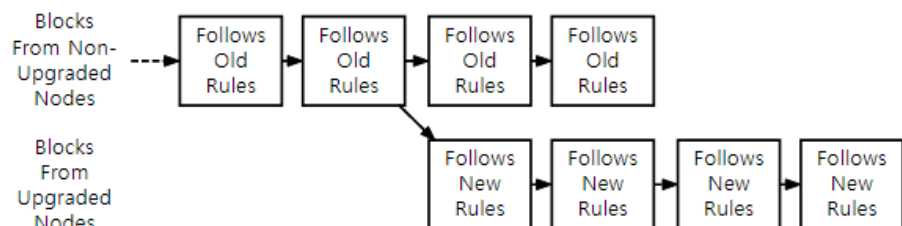
지하경제와 자금세탁 문제	대부분의 정부가 비트코인을 반기지 않는 상황이다. 가장 큰 문제는 익명성으로 인해 탈세나 검은 거래, 즉 지하경제에서 유통될 수 있다는 점이다. 비트코인은 국경을 넘어 거래되고 있으며 암호화로 익명성이 보장돼 탈세와 자금세탁에 쓰일 수 있다. 유로 폴(Europol)은 최근 유럽에서 콜롬비아의 마약조직에 코카인 대금을 지불하는데 암호화폐가 사용됐다고 밝혔다. 범죄자들은 암호화폐 거래소에서 유로를 암호화폐로 교환해 디지털 지갑으로 송금한 후 이 암호화폐를 다시 온라인 거래소에서 페소로 교환했다. 이 과정에 암호화폐를 수십 개의 주소로 나눠 송금함으로써 자금 세탁을 했다고 한다.
AML, KYC	범죄를 차단하기 위해 한국, 일본, 미국 등 선진국 주요 거래소들은 자금세탁방지(AML; Anti-Money Laundering)와 고객알기제도(KYC; Know Your Customer)를 따르고 있다. 실명인증도 강화하고 있는 추세다. 하지만 거래소를 통하지 않는 거래의 경우 여전히 익명성을 범죄에 악용할 가능성이 존재한다.
탈세 가능성	암호화폐의 성격이 규명되지 않은 상태에서 각종 조세 회피 가능성도 있다. 비트코인을 비롯한 암호화폐가 증권인지, 상품인지, 화폐인지에 따라 과세 기준이 달라지게 되는데 아직까지 대부분의 국가에서 명확하게 정의되지 않았다. 조세 가이드라인이 부재한 상황에서 의도했거나 의도하지 않았거나 탈세 행위가 발생했을 가능성은 농후하다.
외환거래법 위반	외환거래법 위반 가능성도 있다. 지난해 암호화폐 투자 열풍이 불었을 때 한국의 비트코인 가격은 다른 나라 대비 약 40%까지 프리미엄이 상승했다. 외국 거래소에서 비트코인을 매수한 후 한국 거래소에서 매도하면 시세차익을 누릴 수 있었던 것이다. 정확한 규모는 알려지지 않았지만 실제로 이러한 차익거래로 환치기를 했던 사람들이 있었다고 보도됐다. 탈세와 외환거래법 위반은 명백한 범죄행위다.
규제 강화	비트코인을 범죄행위에 사용할 가능성이 남아있는 한 이에 대한 규제 논의는 지속될 수밖에 없다. 근본적인 문제는 중국처럼 인터넷을 완전히 검열하지 않는 한 범법 행위를 적발하는 데 한계가 있다는 점에 있다. 민주주의 국가에서는 암호화폐로 인한 범죄가 우려된다고 해서 인터넷을 모두 검열할 수도 없다. 정부는 매우 어려운 과제에 직면해 있다.

G20 정상회담에서도 이는 중요한 화두로 떠올랐다. 앞으로도 많은 국가들이 논의하게 될 것이다. 장점이 많은 기술이라 해도 나쁜 용도로 쓰이게 되면 규제는 강화될 수 밖에 없고 이는 암호화폐 생태계 전반에 리스크 요인이다.

5. 비트코인 하드포크와 비트코인 캐시의 탄생

- 긴 체인을 참으로 인정** 블록체인은 새로운 블록이 거의 동시에 생성될 수 있고 이때 분기(fork)가 일어난다. 한 줄기에서 나와 여러 줄기로 갈라지는 모양이 실제 포크 모양과 비슷하다. 이때 노드들은 길이가 긴 쪽을 참으로 보고 작업증명을 수행한다.
- 소프트포크와 하드포크** 누구나 비트코인 소프트웨어에 대한 수정안을 제시하고 함께 변경하자고 제안할 수 있다. 비트코인의 노드를 운영하고 있는 참여자들이 동의하면 새로운 버전의 소프트웨어를 다운받아 실행하게 되는데 이전 버전으로 생성된 블록들과 호환이 가능한 변경을 소프트포크(soft fork), 호환되지 않는 완전한 변경을 하드포크(hard fork)라고 부른다.
- 비트코인 캐시의 탄생** 2017년 8월 1일, 비트코인과 비트코인 캐시(Bitcoin Cash)로 갈라지는 하드포크가 일어났다. 블록 크기와 처리속도를 개선하기 위해 오랜 기간 논의해온 비트코인 커뮤니티가 합의를 이루지 못해 비트코인은 478558번 블록에서 두 줄기로 갈라졌다.
- 각자의 이해관계** 오리지널 비트코인을 지지하는 측을 비트코인 코어 진영이라고 부르는데 블록스트림(Blockstream)의 CEO인 아담 백(Adam Back)이 대표적이다. 비트코인 코어 진영의 개발자들은 비트코인의 블록 크기를 늘리면 블록체인의 용량이 빠르게 증가해 개별 노드의 서버가 대형화되어야 하므로 개인들의 참여를 유지하기 위해 블록 크기를 늘려서는 안된다고 주장한다.
- 일부 개발자들은 비트코인을 ‘금’과 같은 자산으로 봐야 한다며 처리 속도를 빠르게 할 필요가 없다고도 주장했다. 아담 백은 비트코인을 현금처럼 사용하기 위한 방법으로 블록 크기를 늘리는 대신 라이트닝 네트워크(Lightning Network)를 주장하고 있다.

[그림11] 블록체인의 하드포크(Hard Fork)



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

비트코인 캐시를
지지하는 측의 주장

한편, 마이닝 풀 비트메인(Bitmain)사의 중국인 CEO 우지한은 비트코인 캐시가 진짜 비트코인이라고 주장한다. 사토시 나카모토가 만든 화폐 시스템으로서 진짜 화폐처럼 거래 가능해야 비트코인 정신의 본질을 되찾을 수 있다는 것이다. 블록사이즈를 늘려 더욱 빠른 거래가 가능해야 화폐로서 비트코인이 자리잡을 수 있다는 주장이다.

날선 대립각

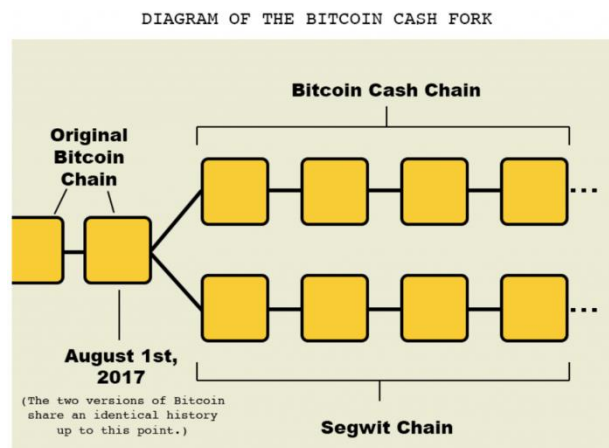
양측은 날선 대립각을 세우며 상대측이 각각의 이해관계를 추구하는 것일 뿐이라고 비난한다. 아담 백은 블록스트림이 라이트닝 네트워크 기술을 개발해 돈을 벌기를 바라기 때문에 비트코인 코어를 지지하는 것이라는 공격받는다. 한편, 거래건수를 늘리고 블록 생성 시간을 줄일수록 마이닝 풀은 채굴 수익과 수수료 수익을 모두 늘릴 수 있다. 채굴 수익이 늘어나면 채굴기 판매도 함께 늘어난다. 우지한은 채굴기 판매와 채굴 수익을 모두 높이기 위해 비트코인 캐시를 지지하는 것이라고 비난 받는다.

지속되는 하드포크의 위험성

비트코인과 비트코인 캐시의 하드포크 이후에도 비트코인 골드 등 하드포크로 새로운 암호화폐 발행이 지속됐다. 2017년 암호화폐 투자 열풍이 거센 상황에서 하드포크로 새로운 암호화폐를 만들면 기존 비트코인 보유자들에게 자동으로 새로운 코인이 생성되는 것은 보너스를 주는 것으로 인식됐다. 하지만 이는 엄밀히 말하면 보너스가 생성된 것이 아니라 기존 커뮤니티가 갈려나간 것이다. 커뮤니티의 가치가 커지기보다 오히려 줄어들 수도 있는 요인이다. 가장 오랜 기간 동안 전세계에서 가장 많은 참여자가 검증해왔다는 점이 비트코인의 강점인데 하드포크가 잦아지면 검증되지 않은 새로운 위험이 발생할 수 있다.

물론 집단 지성이 토론해 다각도로 시험해 볼 수 있고 가장 많은 사람들이 합의하는 블록체인이 살아남을 것이기에 하드포크 자체는 별로 문제가 되지 않을 것이라는 의견도 있다. 커뮤니티 구성원들 간의 합의와 하드포크는 앞으로 주목해야 할 이슈다.

[그림12] 오리지널 비트코인의 하드포크, 비트코인 캐시



자료: 코인투데이, 한화투자증권

III. 블록체인 생태계의 확산, 이더리움

1. 스마트 계약을 구현할 수 있는 새로운 프로토콜

19 세 천재소년 비탈릭 부테린과 이더리움의 등장

분산 어플리케이션을
구현하는 플랫폼

비트코인이 화폐냐 아니냐는 논쟁이 확산되는 사이에 이더리움이 등장했다. 이더리움은 P2P 전자 화폐 시스템을 넘어서 스마트 계약이라는 개념을 도입함으로써 블록체인 2.0 시대를 열었다. 이더리움은 기본적으로 비트코인의 결제네트워크 기능을 갖춘 동시에 분산화된 P2P 네트워크 안에서 실행되는 분산 어플리케이션(DApp)을 구현하기 위한 플랫폼이다.

천재소년, 비탈릭 부테린

이더리움의 창시자는 1994년생 비탈릭 부테린(Vitalik Buterin)이다. 어릴 때부터 수학과 프로그래밍에 특출난 재능을 보였던 비탈릭 부테린은 2007년부터 2010년까지 ‘월드 오브 워크래프트(World of Warcraft)’라는 게임에 빠져 있었다고 한다. 게임 제작사인 블리자드(Blizzard)가 비탈릭이 아끼던 캐릭터의 기능을 갑작스레 없애버리자 중앙집권적인 서비스의 문제점을 실감하고 게임을 중단했다. 제작사에 분노한 비탈릭은 2011년 삶의 새로운 목적을 찾던 중에 비트코인을 발견했다고 말했다.

2014년 처음 발표

비트코인의 매력에 빠져든 비탈릭은 비트코인 커뮤니티에서 활동하다 위털루 대학을 중퇴하고 크립토 프로젝트에 몰두했다. 2013년 말 이더리움 기본 개념을 구상해 2014년 1월 미국 플로리다 마이애미에서 열린 북미 비트코인 컨퍼런스에서 이더리움의 개념을 발표했다. 이후 2014년 4월 개빈 우드 박사(Dr. Gavin Wood)가 이더리움의 기술적 세부 내용을 담은 옐로 페이퍼(Ethereum Yellow Paper)를 발표했다.

[그림13] 이더리움의 창시자, 비탈릭 부테린



자료: about.me/vitalik_buterin, 한화투자증권

이더리움 재단 설립과 이더 발행

2014년 6월 비탈릭은 동료 개발자들과 함께 이더리움 재단(Ethereum Foundation)을 스위스 주크시에 설립했다. 7월에는 이더(Ether) 프리세일을 42일간 진행했다. 이 때 이더리움 재단은 60,102,216 개의 이더를 팔아 31,591 개의 비트코인을 받았는데 당시 시세로 약 18백만 달러의 자금조달이었다.

세계의 컴퓨터

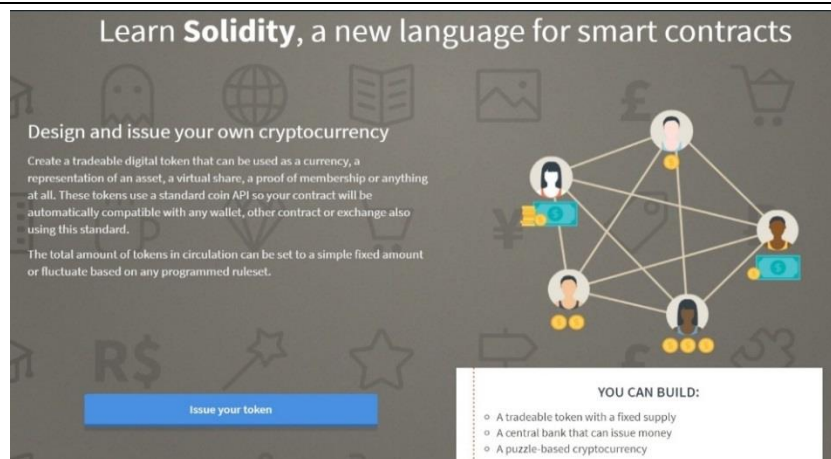
이더리움은 비트코인과 마찬가지로 어느 누구나 참여할 수 있는 오픈 소스의 공개된 프로젝트다. 블록체인 기술을 기반으로 전 세계 수많은 사용자들이 보유하고 있는 컴퓨팅 자원을 활용해 정해진 규칙대로 각종 데이터를 검증하고 기록한다. 세계 어디서나 자유롭게 참여할 수 있고 서로 연결되어 동일한 규칙대로 소프트웨어를 구동한다. 이더리움은 ‘세계의 컴퓨터(World Computer)’라고도 불리며 탈중앙화된 최초의 월드 컴퓨터라고 볼 수 있다.

이더리움은 비트코인과 유사한 Ethash라는 수정된 작업증명(Proof-of-work) 방식을 통해 거래를 기록하고 신규 이더를 발행하게 설계되어 있다. 작업증명 방식이지만 이더리움은 비트코인보다 처리 속도가 빠르다. 12초에서 15초마다 새로운 블록이 생성되고 채굴 보상으로 3개의 이더가 발행된다.

블록체인 앱 플랫폼

이더리움은 화폐 거래를 넘어 새로운 플랫폼을 지향한다. ‘bitcoin.org’에 접속하면 ‘혁신적인 결제 네트워크이자 신중 화폐’라고 비트코인을 설명하고 있는 반면 ‘ethereum.org’의 첫 화면에는 ‘Blockchain App Platform’이라고 쓰여있다. 비트코인이 화폐 거래의 탈중앙화를 추구하는 결제 네트워크로서 ‘세계의 은행’을 표방한다면 이더리움은 유사한 결제 네트워크를 기반으로 하되 다양한 어플리케이션을 구동할 수 있는 플랫폼으로 영역을 확장하고 있다.

[그림14] 이더리움 안에 누구나 다양한 스마트 계약을 만들 수 있음



자료: ethereum.org, 한화투자증권

2. 스마트 컨트랙트와 EVM

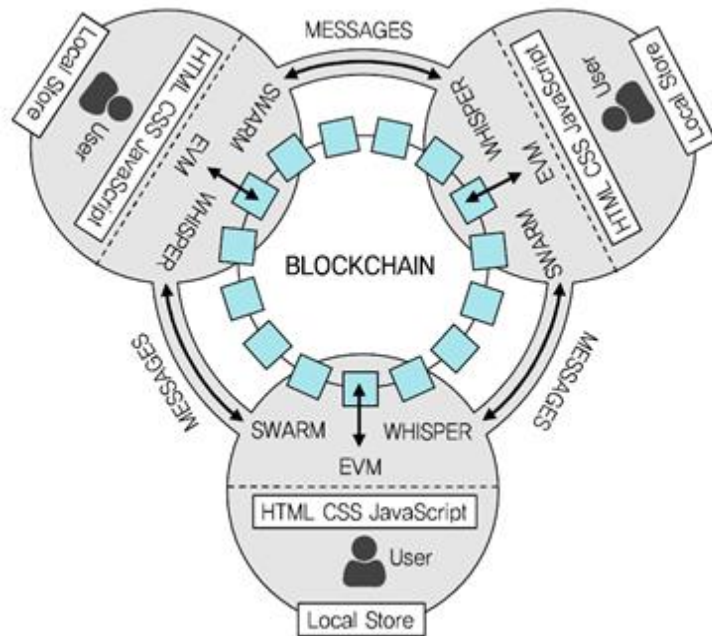
스마트 계약과
이더리움 가상기계

이더리움 파운더들은 블록체인에 거래내역뿐 아니라 계약 등 추가 정보를 기록할 수 있다는 점에 착안해 스마트 계약(Smart Contract)을 도입했다. 스마트 계약이란 입력한 조건이 만족했을 때 계약을 실행하도록 코딩해 넣은 것이다. 이더리움에서 스마트 계약을 생성하면 이더리움 가상기계(EVM; Ethereum Virtual Machine) 안에서 동작하게 되며 스마트 계약의 검증, 실행은 모두 블록체인 안에 기록된다.

이해를 돕기 위해 간소한 스마트 계약의 예를 살펴보자.

앨리스는 내일 아침에 비가 올 것이라고 생각한다. 밥은 내일 아침에 비가 오지 않을 것이라고 생각한다. 각자 만원씩을 걸고 내기를 할 수 있다. 이 때 서로가 서로를 신뢰할 수 없다면 중간에 3자를 세워 3자에게 돈을 주었다가 내일 아침에 비가 오면 앨리스에게, 비가 오지 않으면 밥에게 돈을 주라고 해야할 것이다. 이 때 이더리움의 스마트 계약을 활용하면 3자가 불필요해진다. 서로 합의한 조건을 이더리움 블록체인에 코딩해 넣으면 이더리움 블록체인 상 노드들이 이 계약을 검증하고 조건이 만족됐을 때 자동적으로 계약을 집행한다. 이더리움 같은 암호화폐를 프로그래밍 가능한 돈(programmable money)라고도 부른다.

[그림15] 이더리움의 창시자, 비탈릭 부테린



자료: about.me/vitalik_buterin, 한화투자증권

조건문 수행	이더리움은 튜링완전언어(Turing Complete Language)를 스마트 계약 작성 언어로 선택해 다양한 응용이 가능하다. 튜링완전언어란 조건 분기문(if 조건문, For, While 등의 반복문)이 존재하고 메모리의 임의 위치 값을 변경할 수 있는 언어로 C/C++, Java, Python 등이 있다. 이더리움에서는 Solidity라는 언어를 사용해 이더리움 플랫폼 상에서 스마트 계약을 코드로 넣으면 지정된 조건을 만족했을 때 계약이 이행되도록 할 수 있다. 단순한 금액 이체뿐 아니라 대상물, 이체 조건, 권한, 방법 등을 정교하게 설계할 수 있다.
분산 어플리케이션	스마트 계약이 이더리움 플랫폼 안에서 동작할 수 있도록 만든 어플리케이션을 DApp(Decentralized application)이라 한다. DApp이라는 이름만 봐도 이더리움 역시 비트코인과 마찬가지로 탈중앙화(Decentralization)를 중요하게 여기고 있음을 알 수 있다. 이더리움 플랫폼 상에 다양한 종류의 DApp을 만들 수 있다. 비탈릭은 이더리움을 스마트폰 안의 플랫폼, 즉 앱스토어나 구글플레이에 비유한 바 있다. 현재까지 약 1500개 이상의 DApp이 만들어졌다.
이더리움과 계정	이더리움 플랫폼에서 기본 화폐는 이더(Ether)이며 결제·송금 등 비트코인에서 가능한 모든 거래가 가능하다. 비트코인의 주소와 유사하게 이더리움에서는 계정(Accounts)이 생성된다. 이더리움의 계정은 이더를 비트코인처럼 단순 결제·송금 용으로 사용할 수 있는 외부소유계정(Externally Owned Accounts)과 스마트 계약을 실행하는 용도로 사용하는 계약계정(Contract Accounts)으로 구분된다. 외부소유계정은 비트코인과 동일하게 개인키에 의해 통제되며 계약계정은 스마트 계약 코드에 의해 통제된다.
가스	이더리움 안에서 스마트 계약을 구동하려면 이더리움 네트워크에 참여하는 노드의 컴퓨팅 파워를 사용해야 한다. 이때 연료의 개념으로 가스(gas)가 필요하다. 코드 연산을 수행할 때마다 정해진 양의 가스가 소모되며 가스 가격은 미리 책정된 금액의 이더로 지불된다.
토큰 발행	이더리움 플랫폼에서 사용할 수 있는 어플리케이션인 DApp을 개발하는 스타트업들은 DApp 안에서 사용할 수 있는 토큰을 발행한다. 이더리움 홈페이지에 접속하면 ‘당신만의 토큰’을 만들어 보라는 페이지가 나온다. 이더리움이 누구나 토큰 발행을 할 수 있는 플랫폼을 제공한 후 블록체인 생태계가 빠른 속도로 커져가고 있다. 인터넷 초기에 홈페이지를 만들기 위해서는 html 같은 언어를 배워야 했고 많은 작업이 필요했지만 인터넷 포털 사이트들이 생겨나면서 개인 블로그나 카페 개설이 쉬워진 것을 생각해보자. 블록체인 역시 이더리움의 등장으로 인해 스마트 컨트랙트 아이디어를 블록체인 상에 구현하는데 진입장벽이 낮아진 셈이다.

3. 토큰(Token)과 ICO(Initial Coin Offering)

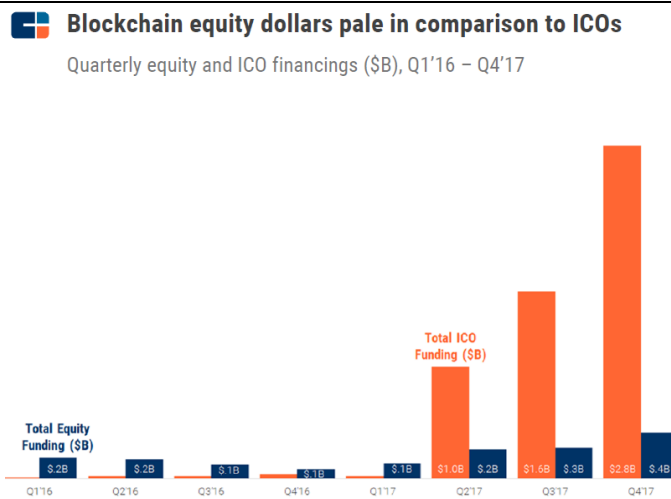
ICO 이더리움뿐 아니라 다양한 블록체인 네트워크 상에서 토큰(또는 암호화폐) 발행을 통해 자금을 모집하는 것을 ICO(Initial Coin Offering)라고 한다. 블록체인 스타트업을 창업할 경우, 초기 자금을 모집하는데 있어 ICO는 매우 빠르고 편리한 방법으로 인기를 끌고 있다. ICO는 벤처캐피탈(VC; Venture Capital) 투자를 받거나 크라우드 펀딩(Crowdfunding)을 받는 것과 유사한 점이 많다. 통상 ICO는 토큰 설립자들이 먼저 사업 아이디어를 담은 백서를 온라인 상에 공개하고 지지하는 사람들에게 토큰을 판매하는데 이 때 법정화폐 대신 비트코인이나 이더 같은 암호화폐로 거래한다.

IPO와 비교 ICO는 기업들의 주식 상장인 IPO(Initial Public Offering)와 유사하다고 볼 수 있지만 실제로 토큰을 구매하는 것은 주식을 사는 것과 다소 차이가 있다. 가장 큰 차이는 ICO와 IPO의 시점이다. 창업 후 몇 년간의 재무제표에 대한 회계 감사 후 진행되는 IPO와 달리 ICO는 아이디어가 실제로 구현되기 훨씬 이전부터 아이디어만을 가지고 투자를 모집할 수 있다.

IPO는 시간과 비용이 상당히 필요해 아주 작은 규모의 회사가 상장을 추진하기 어려운 반면, ICO는 몇 개월 만에 비즈니스 아이디어만 가지고도 시도해볼 수 있다는 점이 장점으로 꼽힌다. 블록체인 스타트업 입장에서는 ICO를 하게 되면 지분 구조를 자유롭게 가져갈 수 있는데다 사업을 본격적으로 론칭하기 전부터 홍보효과도 얻을 수 있어 ICO에 대한 선호도가 높다.

코인스케줄(CoinSchedule)에 따르면 2017년 ICO 건수는 211건(38억 8천만 달러)으로 2016년 45건(95백만 달러) 대비 대폭 증가했다. 코인데스크(CoinDesk)는 2018년 1분기에 모집된 ICO 자금이 63억 달러로 이미 2017년 연간 조달된 규모를 넘어섰다고 보도했다.

[그림16] 2017년 블록체인 ICO 금액은 Equity 투자를 넘어 빠르게 성장

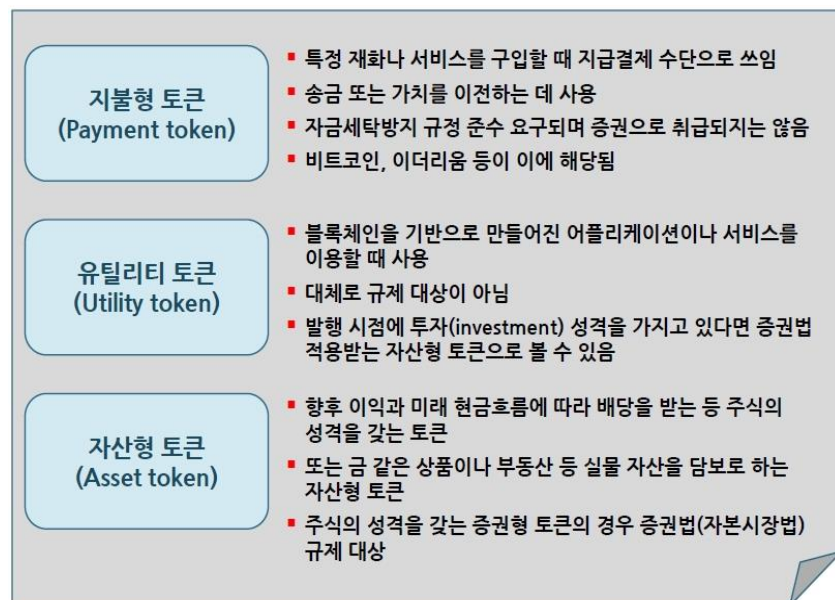


자료: CBInsights, 한화투자증권

스위스 금융감독청(FINMA)의 ICO 가이드라인

토큰의 3가지 종류	토큰의 성격이 주식과 유사한 토큰도 있지만 주식이 아닌 상품권 성격의 토큰이나 재화의 성격을 가지는 토큰도 있다. 2018년 2월 스위스 금융감독청(FINMA)은 토큰의 종류를 지불형 토큰(Payment token), 유틸리티 토큰(Utility token), 자산형 토큰(Asset token)의 3가지로 구분해 ICO 가이드라인을 발표했다.
지불형 토큰	지불형 토큰(Payment token)은 특정 재화나 서비스를 구입할 때 지급결제 수단으로 쓰는 토큰을 말하며 비트코인, 이더리움 등이 이에 해당된다. 기본적으로 자금세탁방지 규정 준수가 요구되나 증권으로 취급되지는 않는다.
유틸리티 토큰	유틸리티 토큰(Utility token)은 블록체인을 기반으로 만들어진 어플리케이션이나 서비스를 이용할 때 사용하는 토큰으로 대체로 규제 대상이 아니다. 하지만 발행 시점에 투자 성격을 가지고 있다면 증권법 적용을 받는 자산형 토큰으로 볼 수도 있다.
자산형 토큰	향후 이익과 미래 현금흐름에 따라 배당을 받는 등 주식의 성격을 갖는 토큰은 자산형(Asset Token)에 해당된다. 금 같은 상품(Commodity)이나 부동산 등 실물 자산을 담보로 하는 경우에도 자산형 토큰이다. 주식의 성격을 갖는 증권형 토큰의 경우에는 증권법이나 자본시장법 규제 대상이 될 수 있다.

[그림17] 스위스 FINMA 가이드라인에 따른 토큰의 분류



자료: 스위스 FINMA, 한화투자증권

4. 탈중앙화 어플리케이션(DApp)과 디지털 소유권 거래

킬러 앱의 부재

ICO 열풍과 함께 다양한 종류의 코인과 토큰이 연일 출시되고 있음에도 불구하고 블록체인으로 구현된 실질적인 비즈니스를 찾아보기는 어려운 것이 현실이다. 비트코인을 제외하면 이더리움이 현재 가장 많은 어플리케이션이 구동되고 있는 플랫폼 프로토콜인데 이더리움 DApp 중에도 트랜잭션이 많이 일어나는 킬러 앱(Killer App)이라 부를만한 어플리케이션을 찾기 어렵다. 현재 구현된 Dapp만 보자면 블록체인 기술이 ‘엔지니어들의 장난감’일 뿐이라고 폄하하는 것도 납득할 만 하다.

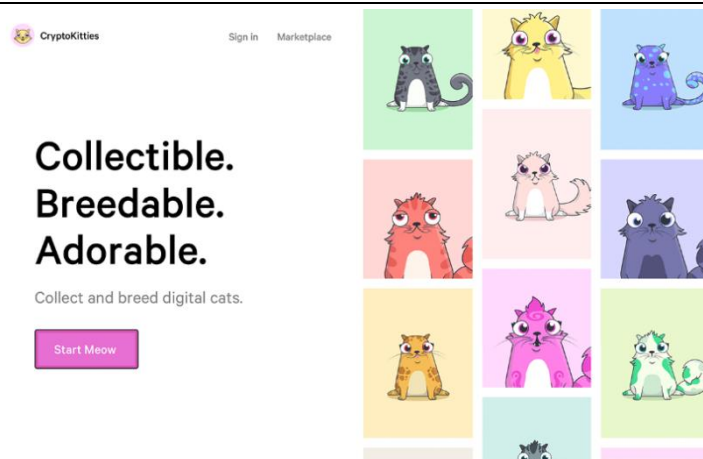
크립토 키티

현재까지 가장 인기를 끈 DApp어플리케이션은 크립토키티(CryptoKitties)라는 게임이다. 이더리움 스마트 계약에 입력된 코딩에 따라 새로운 고양이 15분마다 탄생하며(5만 마리로 제한됨) 모든 고양이는 각기 다른 특성을 가진다. 참여자들은 특성이 모두 서로 다른 다양한 종류의 고양이 캐릭터를 사고 팔 수 있으며 원한다면 다른 고양이와 교배해 새로운 고양이를 만들어낼 수 있다.

이 게임은 2017년 12월에 공개됐는데 초기 생성된 100마리의 창업자(Founder) 키티가 한 마리 당 100이더 이상의 가격에 팔렸다. 최고가 고양이는 253이더(당시 약 11만 달러)를 기록했다. 실물 고양이도 아닌 인터넷 상에 존재하는 가상 고양이 한 마리가 한화로 1억원이 넘는 가격에 팔린 것이다.

주목할 점은 ICO 시장이 폭발적으로 커지고 있던 시기에 이들은 ICO를 하지 않았다는 사실이다. 크립토키티 팀은 블록체인과 암호화폐에 대한 대중의 관심이 높아지는 것은 긍정적이지만 호화로운 미사여구로 실현하기 어려운 아이디어를 내세워 자금을 모집하는 ICO에 반대 입장을 밝혔다.

[그림18] 이더리움 블록체인에 기록되는 크립토 키티



자료: CryptoKitties, 한화투자증권

크립토키티는 ICO로 자금을 모으는 대신 게임 론칭 후 바로 매출이 발생하도록 설계됐다. 15분마다 새로 태어나는 고양이 캐릭터를 판매하고 사용자간 캐릭터 판매 금액의 3.75%를 수수료로 취함으로써 매출이 발생하는 구조다. 2018년 3월 안드레센 호로비츠 (Andreessen Horowitz)와 유니언 스퀘어 벤처스(Union Square Ventures)가 12백만 달러를 투자했다. 블록체인 산업에 가장 적극적으로 투자하고 있는 벤처캐피탈이다.

크립토키티가 앞으로 얼마나 인기를 얻을 수 있을지 알 수 없다. 어쩌면 나중에는 아무도 거래하지 않게 될 지도 모른다. 하지만 아무도 사용하지 않는다 해도 이미 생성된 크립토키티의 거래내역과 소유권은 이더리움 블록체인 상에 영구히 보존된다. 일반적인 온라인, 모바일 게임의 경우 제작사가 사라지면 내 아이템뿐 아니라 내 아이디, 접속기록이 모두 사라질 수 있는 반면 블록체인에 올려진 게임은 더 이상 제작사가 독자적으로 수정하거나 삭제할 수 없다.

디지털 수집품 거래(Non-Fungible Token)

ERC721 토큰 이더리움 블록체인에서 발행된 대부분의 토큰이 ERC 20 기반인데, 크립토키티 토큰은 ERC 721로 발행됐다. ERC 20로 발행된 토큰은 화폐처럼 발행된 토큰들의 단위 당 가치가 동일하다. 발행된 순서와 상관없이 1달러는 동일하게 1달러의 가치를 가지는 것처럼 ERC 20로 발행된 토큰 역시 마찬가지다. 이러한 토큰을 대체 가능한 토큰(Fungible Token)이라고 하며 화폐나 상품권처럼 사용된다.

대체 불가능한 암호 수집품 한편, 크립토키티 토큰은 개별 캐릭터가 탄생할 때마다 새로운 토큰이 발행되는데 각 캐릭터의 특성이 모두 다르듯 토큰의 가치도 모두 다르게 책정된다. 이러한 토큰을 대체 불가능 토큰(Non-Fungible Tokens)이라고 한다. 크립토키티의 개별 토큰은 각기 다른 한마리의 디지털 고양이 캐릭터 그 자체다. 크립토키티 프로젝트는 NFT 토큰 발행을 통해 실물 경제에서 그림같은 수집품을 사고 팔 듯, 디지털 세계에서 암호화된 디지털 수집품을 소유하거나 사고 팔 수 있게 한 프로젝트다.

복제 불가능한 디지털 고양이에 대한 소유권을 거래할 수 있다면 음악 콘텐츠나 게임 아이템 같은 다양한 디지털 콘텐츠에 대한 소유권 역시 거래 가능할 것이다. 뿐만 아니라 복제가 불가능한 장부 거래의 대표적인 자산 부동산도 블록체인을 통해 거래할 수 있을 것이라는 상상을 해볼 수 있다. 물론 부동산 거래 장부가 표준화된 디지털 데이터로 완비 되었을 때 가능한 상상이긴 하지만 충분히 실현 가능한 시나리오다.

어플리케이션 개발이 가장 활발한 이더리움에서조차 크립토키티, 이더구(EtherGoo) 같은 단순한 게임 이상으로 구현되는 앱을 찾기 어렵다. 탈중앙화 어플리케이션의 개념에 매료된 많은 사람들이 다양한 종류의 Dapp을 개발하고 ICO를 진행하고 있지만 이더리움 프로토콜 자체의 처리속도나 저장용량 등의 문제를 해결해야 한다. 당분간은 실물 경제보다 디지털 콘텐츠 분야에서 활용 가능성이 높아 보인다.

IV. 퍼블릭, 프라이빗, 그리고 컨소시엄 블록체인

비트코인, 이더리움을 비롯해 지금까지 논의한 블록체인은 모두 퍼블릭(Public) 블록체인이다. 블록체인의 종류는 참여자 범위에 따라 퍼블릭(Public), 프라이빗(Private), 컨소시엄(Consortium) 3가지로 구분할 수 있다. 각각의 블록체인의 특성에 대해 살펴보자.

1. 퍼블릭(Public) 블록체인

비트코인은 참여자 모두에게 정보가 공개되는 퍼블릭(Public) 블록체인이다. 중앙에서 통제하는 조직이나 대표자가 없으며 누구나 자유롭게 소프트웨어를 다운로드 받아 네트워크에 접속하면 거래내역을 검증하거나 생성할 수 있다. 퍼블릭 블록체인은 비트코인과 이더리움을 비롯해 현재까지 구현된 블록체인 중 가장 광범위하게 채택된 방식이다.

퍼블릭 블록체인에 암호화폐는 필수적

퍼블릭 블록체인은 자발적인 참여를 전제로 하기에 참여자에게 부여할 인센티브로서 암호화폐가 필수적이다. 거래 검증 역할을 하는 노드, 즉 참여자는 본인의 컴퓨터를 분산된 하나의 서버로 제공하게 되는 셈이며 작업 검증 시 전기요금이 발생한다.

암호화폐가 존재하지 않는 퍼블릭 블록체인을 설계하는 것은 기술적으로 문제가 없다. 하지만 아무런 보상 없이 본인의 컴퓨터를 퍼블릭 블록체인에 무상으로 제공하고 전기요금까지 지불하게 한다는 것은 현실적으로 불가능에 가깝다. 아무런 보상을 바라지 않는 선의의 자발적 참여자가 충분히 많아야 거래 검증의 신뢰를 확보할 수 있는데, 충분히 많지 않다면 퍼블릭 블록체인은 실패할 것이기 때문이다.

한편 서로 누가 누구인지 알 수 없는 상태에서 다수의 참여자 간에 오로지 소프트웨어를 통해 진위를 검증해야 하니 거래속도가 느리다는 단점이 있다. 참여자가 많으면 많을수록 해킹이나 위변조 가능성이 낮아지지만 동일한 원장을 지나치게 많은 참여자가 보유할 경우 컴퓨팅 파워나 전력 낭비라는 측면에서 비효율적이라는 비판도 받는다.

이더리움은 현재 전력 소모가 많은 PoW(Proof of Work) 작업증명 방식을 PoS(Proof of Stake) 지분증명 방식으로 변경하는 것을 검토 중이다. 퍼블릭 블록체인의 특성 상 다수의 노드가 합의하지 않으면 변경할 수 없다. 이것은 퍼블릭 블록체인의 장점이자 동시에 단점이 될 수 있는 중요한 특징이다. 참여자 누구나 아이디어를 제안할 수 있는데 다수의 합의를 얻어야만 변경을 실행할 수 있다. 합의를 얻지 못한 코드 변경은 실패하거나, 블록체인을 두 갈래로 쪼개는 하드포크를 초래한다.

중앙집권적 의사 결정 기구가 존재하지 않고 민주적인 의사결정이 필요하다는 점은 탈중앙화를 이룬 퍼블릭 블록체인 강력한 강점이지만 합의를 이루지 못한다면 커뮤니티가 분열될 수 있다. 커뮤니티의 잦은 분열은 해당 블록체인의 암호화폐 가치를 크게 훼손하는 요인이다.

2. 프라이빗(Private) 블록체인

퍼블릭 블록체인의 단점을 보완하고 특정 참여자들만 공유하기 위해 프라이빗(Private) 블록체인이 만들어졌다. 프라이빗 블록체인은 중앙 관리 조직 또는 소유자가 존재하고 허가된 참여자만 네트워크에 들어올 수 있어 참여자 간 식별이 가능하며 특화된 데이터 공유가 가능하다. 허가받은 참여자만 참여할 수 있어 처리속도를 획기적으로 개선할 수 있고 기업형 블록체인으로 활용될 가능성이 높다. 공개된 인터넷 사이트와 기업 내부에서만 사용하는 인트라넷의 차이를 떠올려 보면 이해가 빠를 것이다.

2015년 미국 나스닥에서는 블록체인 시범사업으로 비상장 주식 거래를 위한 프라이빗 블록체인, 나스닥 링크(Linq)를 도입했다.

프라이빗 블록체인은 관리자의 의도대로 구동 방식을 변경할 수 있기 때문에 기업 입장에서 편리하게 활용할 수 있으나 블록체인의 장점이자 특성인 투명성과 탈중앙화는 사라지게 된다. 암호화폐가 불필요한 프라이빗 블록체인은 단순한 분산형 데이터 베이스라고 보는 시각도 있다.

3. 컨소시엄(Consortium) 블록체인

컨소시엄(Consortium) 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인의 중간 형태로 소유자가 모든 권한을 가지게 되는 형태인 프라이빗 블록체인과 달리 미리 선정된 노드들이 권한을 가지게 되는 블록체인이다. 컨소시엄 블록체인은 분산형 구조를 유지하면서 제한된 참여를 통해 보안을 강화할 수 있고 퍼블릭 블록체인에서 제기된 느린 거래 속도와 네트워크 확장성의 문제도 해소시켜주기 때문에 은행들 간 트랜잭션과 같은 용도로 개발되고 있다.

R3CEV의 코다(Corda)와 리눅스 재단을 중심으로 하는 하이퍼레저(Hyperledger)가 대표적이다. R3CEV는 핀테크 스타트업인 R3가 주도하는 컨소시엄으로 금융산업 내 블록체인 기술을 표준화를 목표로 2015년 9월에 결성됐다. 송금 시간과 비용을 절감하고 다양한 금융서비스를 구현하기 위해 코다(Corda)라는 분산원장 플랫폼을 개발했다. 컨소시엄에 참여한 기관 간에 합의한 데이터를 기반으로 스마트 계약을 작성할 수 있으며 원하는 데이터를 서로 공유해 자산을 교환할 수 있다.

한국에서도 KB국민은행, 신한은행, 우리은행, 하나은행 등이 가입해 컨소시엄에 참여하고 있으며 세계 약 80개 이상의 기업들이 참여하고 있다. 코다 플랫폼에는 암호화폐가 존재하지 않으며 스마트 계약을 담은 DApp을 구현할 수 있다.

하이퍼레저(Hyperledger) 프로젝트는 리눅스 재단의 오픈소스 프로젝트다. IBM의 주도로 인텔, 엑센츄어, SAP 등 세계 약 130여개 회사가 참여하고 있다. 하이퍼레저 프로젝트는 금융, IoT, 공급망 관리, 제조업 물류 등 산업 전반에서 활용할 수 있는 범용 블록체인을 만들고자 한다.

퍼블릭 블록체인보다 효율성을 높여 실제 기업 간 비즈니스에 활용하고자 개발 중이다. 다이아몬드의 채굴부터 모든 거래 내역을 기록하는 블록체인 프로젝트인 에버레저(Everledger)는 하이퍼레저에 기반한 블록체인이다.

[표1] 블록체인 유형별 특징

요소	퍼블릭 (Public)	프라이빗 (Private)	컨소시엄 (Consortium)
관리주체	모든 거래 참여자(탈중앙화)	한 중앙기관이 모든 권한 보유	컨소시엄에 소속된 참여자
거버넌스	한번 정해진 법칙을 바꾸기 매우 어려움	중앙기관의 의사결정에 따라 용이하게 법칙을 바꿀 수 있음	컨소시엄 참여자들의 합의에 따라 상대적으로 용이하게 법칙을 바꿀 수 있음
거래속도	네트워크 확장이 어렵고 거래 속도가 느림	네트워크 확장이 매우 쉽고 거래 속도가 빠름	네트워크 확장이 쉽고 거래 속도가 빠름
데이터 접근	누구나 접근 가능	허가받은 사용자만 접근가능	허가받은 사용자만 접근가능
식별성	익명성	식별 가능	식별 가능
거래증명	검증 알고리즘에 따라 거래 증명자가 결정되며 거래 증명자가 누구인지 사전에 알 수 없음	중앙기관에 의하여 거래증명이 이루어짐	거래 증명자가 인증을 거쳐 알려진 상태이며 사전 합의된 규칙에 따라 거래검증 및 블록생성이 이루어짐
활용사례	Bitcoin, Ethereum 등	나스닥 링크(Linq) 등	R3CEV, Tendermint 등

자료: 금융보안원, 한화투자증권

V. 블록체인에 대한 주요 국가 동향

1. 블록체인과 암호화폐에 대한 국가별 동향

블록체인에 대해 각 국가마다 입장 차이를 보이고 있다. 규제부터 강화하는 국가가 있는 반면 정부가 주도적으로 기술 개발을 지원하고 공공 부문에의 도입도 적극적인 나라들이 있다. 먼저 미국은 현재 주정부마다 블록체인에 대해 각기 다른 입장을 취하고 있는데 미국 정부 정책은 세계적으로 영향을 줄 수 있어 향후 동향을 주시할 필요가 있다.

뉴욕 비트라이선스

2015년 6월 뉴욕에서는 비트코인 규제로서 ‘비트라이선스(BitLicense)’를 도입해 거래소를 허가제로 만들었다. 암호화폐의 매매, 중개, 수탁, 이체, 채굴 관련 사업자는 모두 비트라이선스를 취득해야 한다. 암호화폐 사업자는 최소 자본금 요건을 갖춰야 하고 암호화폐 관련 리스크 및 계약 조건을 공지해야 하며 감독당국에 보고 의무 등을 준수해야 한다. 이로 인해 일부 거래소는 뉴욕주를 떠났지만 엄격한 규제에 맞춰 운영하고 있는 거래소들은 신뢰도가 더 높아졌다는 긍정적인 평가도 받고 있다.

블록체인 기술 개발을 장려하는 중국 정부

중국은 정부가 나서 적극적으로 블록체인 인프라를 구축하려 하고 있다. 정부 부처인 공업정보화부는 2016년 10월 ‘중국 블록체인 기술과 어플리케이션 발전 백서’를 발간해 블록체인 기술 발전 표준화에 대한 로드맵을 제시했다. 중국 최대 자동차부품 그룹인 완샹그룹, 텐센트의 중국 최초 온라인 은행인 위뱅크, 알리바바가 운영하는 금융 자회사 앤트파이낸셜 등 글로벌 기업들도 백서 발간에 참여했다. 2018년 3월에는 ‘전국 블록체인 및 분산장부 기술 표준화 기술위원회’를 발족해 블록체인 기술 표준화 속도를 높이겠다고 선언했다.

중국의 블록체인 특허 증가

2018년 3월 특허청이 발표한 자료에 따르면 블록체인 관련 특허가 최근 4년간 22배 이상 증가했는데 특히 중국의 특허가 빠르게 증가하고 있다. 코트라(KOTRA)는 2017년 세계지적재산권기구(WIPO)에 등록된 블록체인 관련 특허출원 406건 중 중국이 225건으로 1위를 기록했으며 중국의 특허출원 건수는 2016년 대비 3배 이상으로 증가했다고 발표했다.

[표2] 연도별, 국가별 블록체인 관련 특허 출원 현황

(단위: 건)

출원인 국적	'07년	'08년	'09년	'10년	'11년	'12년	'13년	'14년	'15년	'16년	'17년	'18년	합계
미국	4	4	5	2	10	12	18	62	136	186	58		497
중국		4	2	2		3	3	9	25	321	103		472
한국				1			2	11	33	41	10	1	99
일본		4	2		2	1	2	4	11	2	8		36
유럽				1		2	2	6	24	22	16		73
기타				2	1	3		6	29	22	8		71
총합계	4	12	9	8	13	21	27	98	258	594	203	1	1,248

자료: 특허청, 한화투자증권

블록체인 기술 특허를 낸 상위 10위권 내에 7개의 중국기업이 포진해 있다. 중국의 대표적인 인터넷 포털 기업 바이두(Baidu)는 자체 개발한 블록체인 플랫폼을 오픈하고 이더리움의 크립토키티와 매우 흡사한 ‘라이츠거우’라는 가상 강아지 게임을 출시했다. 바이두는 강아지 캐릭터를 암호화된 수집품(Crypto-Collectible)이라고 정의했으며 블록체인에 기록돼 소장하거나 사고팔 수 있다.

이때 거래는 바이두 지갑을 통해 일종의 포인트로 거래하는데 이 포인트는 현금화 되지 않으나 바이두 서비스를 이용할 때 포인트를 획득하거나 사용할 수 있다. 최근에는 이미지 지적재산권을 보호하기 위한 블록체인 기반의 사진 서비스인 토템(Totem)이 출시됐다. 블록체인 기술을 활용해 원본 사진에 ‘타임스탬프’를 찍고 분산 네트워크에 이를 저장해 저작권을 기록하고 저장할 수 있는 서비스다.

이밖에도 알리바바, 텐센트 등 인터넷 기업들도 블록체인 관련 특허를 지속 출원하고 있고 관련 인력을 충원하는 등 블록체인 사업을 적극적으로 추진하고 있다.

[그림19] 중국 바이두의 ‘라이츠거우’



자료: <https://pet-chain.baidu.com/>, 한화투자증권

영국 영국 정부는 'Beyond Blockchain 전략'을 제시하고 국가적으로 블록체인 활용을 촉진하고 있다. 정보 보안, 정부 문서의 위변조 방지, 사회 보장 부정 수급 방지 등 공공분야에 스마트 계약을 다양하게 시도하고 있다. 2016년 영국 노동연금부(Department for Work and Pensions)는 블록체인 시범사업을 시작했다. 모바일 앱으로 수당을 청구하면 모바일로 지급받게 되고 거래내용은 분산원장에 기록되는 방식이다.

영국 정부는 학자금 대출이나 그밖에 공적 자금 지출, 납세 내역에 대해서도 분산원장 도입을 추진하고 있다. 법무부도 유사한 방식으로 범죄 기록에 대해 블록체인 기술 도입을 검토 중이라고 밝혔다. 한편, 암호화폐에 대한 영국 정부의 입장은 아직 매우 보수적이다. 테레사 메이 영국 총리는 자금 세탁이나 테러 자금 지원에 암호화폐가 사용될 수 있다는 점을 지적하며 강력한 규제가 필요하다고 말했다.

독일과 일본 독일과 일본은 블록체인 기술뿐 아니라 비트코인 등 암호화폐 거래에 대해서도 개방적인 정책을 취하고 있다. 독일은 2015년에 세계 최초로 비트코인을 지급결제 수단으로 인정했다. 일본은 2014년 4월 암호화폐 거래소인 마운트곡스(Mt. Gox) 파산 이후 오랫동안 암호화폐에 대한 소비자 보호 및 사고 방지에 대한 논의를 활발히 해왔다. 그리고 2017년 4월 자금결제법을 개정해 암호화폐를 지급결제 수단으로 정식 인정했다.

이와 함께 암호화폐의 매매, 교환, 중개, 관리 등 암호화폐 취급업을 영위하려는 업체는 금융청에 등록하고 최소 자본금 요건을 충족하도록 했다. 그리고 소비자 보호를 위해 거래소 이용자의 재산과 사업자 재산의 분리 보관, 보안사고 방지체계 구축, 분쟁해결장치 마련 의무 등을 부여했다. 또한 사업자는 거래장부 및 감사보고서를 작성·제출하고 필요 시 현장검사를 수감하도록 하는 등의 감독사항도 포함했다.

2017년 10월에는 일본 정부와 금융감독청(FSA)이 BitFlyer 등 11개의 암호화폐 거래소를 공식적으로 허가했다. BitFlyer는 80만명이 넘는 회원을 보유하고 있는 일본 최대 거래소다. 정식 승인 후 BitFlyer의 CEO는 일본의 암호화폐 거래가 폭발적으로 증가할 것이며 암호화폐 시장을 일본이 선도할 것이라며 기대감을 밝혔다.

일본이 암호화폐 거래를 합법화 한 반면 중국은 2017년 9월 암호화폐 거래소를 폐쇄하고 ICO를 전면 금지했다. 그 영향으로 비트코인 거래 중 중국 위안화 비중은 급락했고 일본 엔화는 비중 1위로 급상승했다. 한국은 현재 일본, 미국에 이어 세 번째로 거래 비중이 높는데, 우선적으로 ICO를 금지했고 거래소 추가 규제 가능성도 있어 향후 정부 정책을 지켜볼 필요가 있다.

암호화폐 과세

암호화폐 사업자에 대한 기초적인 규제가 마련된 국가들을 중심으로 과세 논의도 활발하다. 암호화폐의 성격을 자산, 상품, 지급수단 등 어떻게 보느냐에 따라 세금이 다르게 부과되는데 현재까지 국가마다 다양하게 해석하고 있다.

한국은행이 발간한 '2017 지급결제 보고서'에 따르면, 미국은 암호화폐의 성격을 자산(Property)으로 보고 자산에 관한 세법상 일반원칙(general tax principles)을 적용하고 있다. 암호화폐를 이용한 물품서비스 구매 및 암호화폐 매매로 발생한 소득에 대해 양도소득세를 부과한다. 일본은 암호화폐를 상품(Commodities)으로 보고 세법상 과세 요건 충족 시 과세 대상에 포함시킨다. 암호화폐 매매차익 등을 잡소득(기타소득)으로 인정하고 관련 세금을 부과하고 있다.

대부분의 국가에서 암호화폐 매매 시 부가가치세는 부과하지 않는 추세다. 암호화폐 매입 시 부가가치세를 부과할 경우, 소비자가 가상통화를 매입하고 이를 지급수단으로 활용하여 물품을 구매할 경우 부가가치세가 이중으로 부과되는 점을 고려한 것이다. 당초 부가가치세를 검토했던 일본과 호주는 2017년 7월 미국, 영국, EU 등과 마찬가지로 부가가치세를 비과세하기로 결정했다.

전반적으로 블록체인에 대해서는 긍정적인 국가가 많은 반면 암호화폐에 대해서는 보수적인 국가들이 많다. 익명으로 거래가 가능하고 국가의 통제를 벗어나 국경 뛰어넘어 개인 간 거래를 할 수 있다는 점은 국가가 암호화폐를 반길 수 없게 하는 탈중앙화 암호화폐의 중요한 특성이다. 현재 많은 국가들이 암호화폐에 대한 규제 이전에 암호화폐의 성격을 무엇으로 볼 것인가에 관해 논의하고 있다.

그렇다면 많은 국가가 규제를 강화한다면 암호화폐는 사라질까? 중국의 거래소 폐쇄와 같이 거대한 국가에서 강력한 규제가 나올수록 시장은 충격을 받을 가능성이 높다. 실제로 중국의 거래소 폐쇄 당시 암호화폐 시장의 시가총액은 빠른 속도로 폭락한 바 있다. 하지만 실물경제와 달리 국경 없는 인터넷 상에서 일어나는 암호화폐의 발행과 거래는 어떠한 국가도 완벽하게 차단하기 어렵다. 중국에서는 거래소 폐쇄 이후 개인간 P2P 거래가 급증했다고 한다. 거래소가 없어져 규제할 수 있는 창구만 사라진 셈이다.

암호화폐를 새로운 시대의 디지털 자산으로 합법화 하는 국가가 늘어날수록 이 시장은 더욱 빠르게 성장할 전망이다. 인터넷 강국인 대한민국에서 암호화폐를 완전히 차단하는 것은 사실 상 불가능하다. 그렇다면 대한민국도 주요국과 협력 하에 거래 절차와 방법 등을 적절히 규제하는 동시에 크립토 경제특구 도입 등 인센티브에 대한 고민도 필요하다. 강압적인 규제로 발전 가능성까지 차단해버리기 보다 제도권 하에서 건전한 거래를 유도하고 발전적인 창업 환경을 조성해야 하지 않을까?

2. 에스토니아 디지털 시민권

각국의 사례를 조사해보니 가장 흥미로운 국가는 에스토니아다. 이 나라는 ‘e-Estonia’와 ‘e-Residents’라 불리는 디지털 국가의 전자 시민 모델을 만들어 가고 있다. 에스토니아는 이러한 절차 대부분을 블록체인이 등장하기 전에 구축했는데 최근 수년간 블록체인과의 절묘한 통합을 추구하고 있어 주목할 만 하다.

북유럽 발트 3국 중 하나인 에스토니아는 인구가 130만명에 불과하고 면적은 한국의 절반 정도인 작은 국가다. 1991년 구소련으로부터 독립한 후 정부 역할에 대해 많이 고민해왔다고 알려져 있다. 블록체인 도입 검토 이전에도 오랫동안 IT 강국을 국가 정책으로 내걸고 전 세계적으로 최고의 전자정부를 구현한 것으로 유명하다.

디지털 ID ‘e-Estonia’ 모델의 핵심은 디지털 ID다. 에스토니아인들은 전자 ID 카드로 정부 서비스를 이용할 수 있다. 카드에 내장된 칩은 카드 소유자의 기본 정보 외에 다음 두 가지 인증서를 담고 있는데, 하나는 ID를 인증하는 인증서이고 다른 하나는 디지털 서명을 제공하는 인증서다. 시민들은 이 칩을 활용해 투표를 하고 사회 보장 서비스에 지원하거나 은행 서비스와 대중교통을 이용할 수 있다. 휴대전화에 모바일 ID만 입력하면 칩과 똑같은 기능을 구현할 수 있으며 EU 내 어느 곳이라도 자유자재로 여행할 수 있다.

에스토니아는 국가가 보유한 백만 건의 건강기록의 안전성을 확보하기 위해 블록체인 기술을 채택하고 있다. 건강관리에 대한 모든 기록과 접근이 블록체인에 등록되어 의료 사기를 방지하고 해커가 자신의 흔적을 숨길 수 없도록 한다. 향후 온라인 상으로 다양한 건강 관련 서비스를 제공할 계획이다.

E-Residency 2015년 5월부터는 이와 유사한 디지털 시민권인 ‘e-Residency’를 외국인들에게도 발급하고 있다. 에스토니아 시민과 마찬가지로 디지털 시민(e-residents)이 되면 암호화된 디지털 ID 카드를 발급 받아 다양한 공공 서비스를 이용할 수 있다. 하루 만에 법인을 설립할 수 있고 계좌 개설, 온라인 송금, EU 국가 내 결제 서비스 등 다양한 활동을 할 수 있다.

현재까지 약 33천명이 디지털 시민이 되었고 5천개 이상의 기업이 설립됐다. 수많은 스타트업들이 에스토니아에 법인 설립을 검토하고 있다. 국토가 넓지 않고 인구도 많지 않은 작은 국가가 디지털 시민들을 기반으로 새로운 디지털 국가 개념을 만들고 있다는 것은 매우 흥미롭다.

에스트코인 발행 검토

2017년 8월 25일 에스토니아는 중앙은행이 지원하는 암호화폐 에스트코인(Estcoin)을 발행할 것이며 에스트코인 발행을 ICO를 통해 진행하겠다고 발표했다. 암호화폐 거래나 ICO를 전면 규제하는 국가도 있는 상황에서 에스토니아는 정부가 암호화폐를 직접 발행하겠다고 선언한 것이다. 유럽 주요국가들과 ECB는 이에 대해 매우 비판적인 태도를 보였다. 드라기 총재는 ‘유로존의 통화는 유로만 존재한다’고 선언하며 노골적으로 불편함을 드러냈다. 이런 상황에서 에스토니아가 암호화폐 ICO에 성공하게 될 지는 아직 알 수 없다. 현재로서는 이 국가가 얼마나 적극적으로 디지털 국가를 추진하고 있는지 지켜보는 것만으로도 흥미로울 따름이다.

에스토니아처럼 적극적인 정부가 나타난다는 것은 이를 규제하는 국가들에게 잠재적 위협이 될 수 있다. 사실 상 국경이 없는 디지털 세계에서 점차 규제를 강화하는 국가를 회피하고 새로운 시도를 해볼 수 있는 국가를 선호하는 사람이 늘어나는 것은 자연스러운 흐름이다. 물론 그렇다고 해서 아무런 규제를 하지 않고 방관할 수도 없다. 많은 나라 정부가 규제와 개방 사이에서 깊은 고민을 해야 할 것으로 예상된다.

[그림20] 에스토니아 정부의 E-Residency



자료: Republic of Estonia E-Residency, 한화투자증권

3. 스위스 크립토 벨리

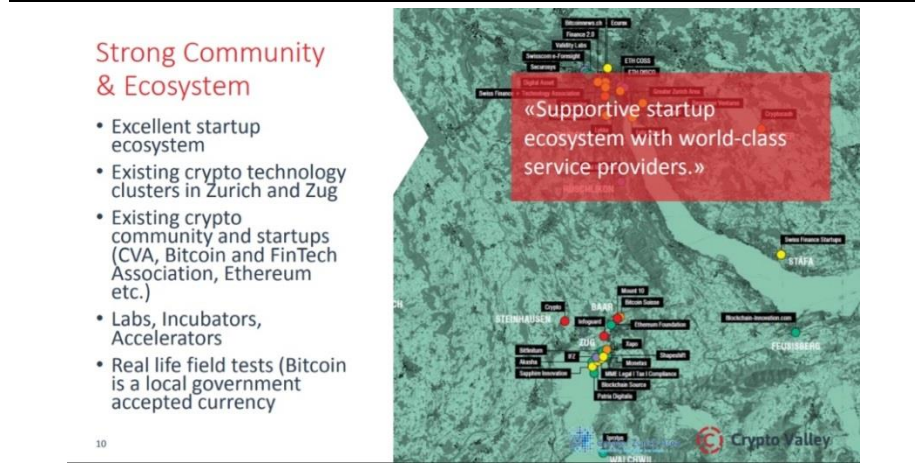
크립토 국가	스위스는 주크(Zug)시에 암호화폐 특성화 지역으로 크립토 벨리(Crypto Valley)를 조성했다. 또한 스위스는 2016년 7월에 세계 최초로 블록체인 기반의 암호화폐와 관련된 세제와 법령을 마련했다. 요한 슈나이더 암만(Johann Schneider-Ammann) 스위스 경제장관은 스위스가 '크립토 국가(Crypto-nation)'가 되어야 하며 주크시는 크립토 국가의 수도를 목표로 한다고 말했다.
스위스로 모여드는 블록체인 기업들	주크시는 암호화폐로 공공요금 결제를 할 수 있게 했다. 주크시 동사무소에 가면 비트코인이나 이더리움 같은 암호화폐로 비용을 지불할 수 있다고 한다. 주크시는 최소한의 합리적인 규제와 발달한 금융산업, 글로벌 네트워크 등을 강점으로 내세우고 있으며 블록체인과 관련된 많은 스타트업들이 주크시로 모여들고 있다. 이더리움 재단을 비롯해 ASIC 채굴기 제조업체이자 전세계 채굴사업의 절반 가량을 차지하는 중국 비트메인(Bitmain)이 이곳에 비트메인 스위스(Bitmain Switzerland)라는 지사를 설립했다. 주크시는 관련 협회 및 업계 관계자들과 협의해 자율규제를 하고 있다. 자율규제에는 중개자에 의한 제 3자 거래, 자금세탁방지(AML), 고객실명확인(KYC) 등에 대한 필수적인 규제 등이 포함되어 있다.
규제 샌드박스	주크시는 크립토벨리로서 혁신적인 아이디어를 다양하게 실험해볼 수 있도록 규제 샌드박스 제도를 시행하고 있다. 암호화폐를 포함한 핀테크 회사는 100만 스위스 프랑(CHF, 한화 11억 5천만원)까지 FINMA의 은행 허가를 받지 않고 공공 계좌를 보유할 수 있고 새로운 비즈니스 모델을 실험할 수 있다. 물론 자금세탁방지(AML) 규정을 준수해야 하며 핀테크 기업이 관리하는 펀드 규모는 1억 스위스 프랑(CHF, 한화 1,161억 원)을 넘어서는 안된다. 새로 허가를 받는 기업은 수탁받은 펀드의 최소 5%에 달하는 자본을 보유해야 하며, 30만 스위스 프랑(CHF, 3억원) 이상 보유해야 하는 등 최소 자본 기준도 요구된다.
디지털 ID	주크시는 2017년 11월 블록체인에 기반한 신분인증으로 디지털 ID를 도입해 파일럿 테스트 중이다. 디지털 ID 하나로 온라인 도서관을 이용하거나 공공 자전거를 타는 등 디지털 정부가 제공하는 다양한 공공 서비스를 이용할 수 있게 하는 것이 주크시의 목표다. 블록체인에 기반한 전자 투표도 시험 중이다. 주크시는 궁극적으로 스마트 시티를 꿈꾸고 있으며 블록체인은 스마트 시티에 필수적인 인프라로 활용될 것이다. 스위스 철도회사인 SBB는 셀프 드라이빙 버스를 블록체인 기반으로 운영하는 사업을 주크시에서 시험 중이다.

스위스 ICO 증가

PwC에 따르면, 지난 해 세계 ICO의 4분의 1 가량이 스위스에서 있었고 모집된 자금 기준으로 상위 10개 ICO 중 4개가 주크시에 재단을 두고 있다. 그렇다고 해서 스위스가 무분별한 ICO까지 모두 환영하는 것은 아니다. 스위스의 금융감독 기관인 FINMA는 공공기관으로서 세계 최초로 2018년 2월 ICO에 대한 가이드라인을 제시했으며 주의 사항을 알리는 데에도 적극적이다.

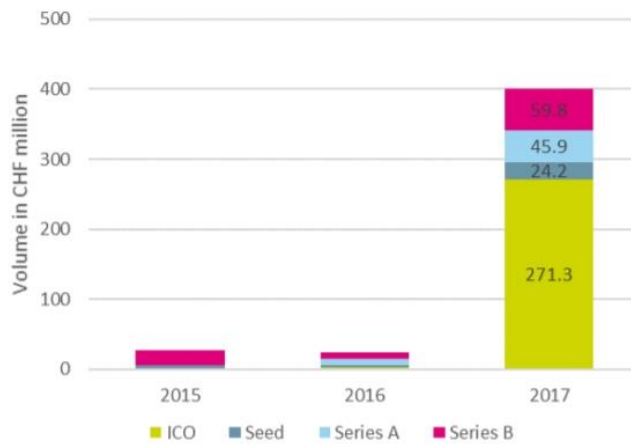
주크시는 기업에 부과하는 세금이 10% 초반 대로 다른 국가나 스위스의 주요 도시들보다 낮으며, 블록체인과 암호화폐에 관해 전문가라고 할 수 있는 회계사나 변호사 같은 전문인력이 많다는 점도 강점으로 홍보하고 있다. 암호화폐와 관련된 각종 컨퍼런스 와 이벤트도 크립토 밸리에서 개최되고 있다. 앞으로 더욱 많은 스타트업들이 모여들어 이를 벤치마킹하려는 국가와 도시도 늘어날 것으로 예상된다.

[그림21] 스위스 주크시, 크립토 밸리(Crypto Valley)



자료: <https://cryptovalley.swiss>, 한화투자증권

[그림22] 스위스 핀테크 벤처캐피탈 투자와 ICO 추이



자료: The Institute of Financial Services Zug IFZ, 한화투자증권

VI. 블록체인 기반의 비즈니스 사례

1. 다양한 분야의 스타트업

탈중앙화, 분권화라는 개념으로 인해 블록체인 기술의 혁신적인 실험은 대기업보다 소규모 스타트업들을 중심으로 일어나고 있다. 특히 ICO 시장 성장으로 인해 블록체인을 활용한 각종 아이디어를 구현하려는 스타트업이 증가하고 있다. 이 중에 얼마나 성공하게 될 지는 알 수 없지만 이들의 다양한 시도를 들여다 볼 필요가 있다. 작은 도전이 파괴적 혁신이 되어 어느 산업이나 기업을 위협하게 될 지 알 수 없는데다 많은 도전들을 실패함으로써 기대치 않았던 새로운 아이디어를 얻게 될 지도 모르기 때문이다.

암호화폐 거래소

최근 몇 년간 채굴 경쟁은 치열해졌다. 일반인이 개인 PC로 채굴을 하기 어렵다면 암호화폐를 어떻게 취득할 수 있을까? 이를 사업 기회로 보고 시작된 것이 바로 암호화폐 거래소다. 암호화폐 거래소는 사토시 나카모토가 애초에 설계한 모델은 아니다. 처음에 거래소는 비트코인을 채굴 보상으로 획득한 사람들이 비트코인을 소유하고 싶어하는 사람들과 거래할 수 있도록 만들어 졌다. 거래소 창업자들은 수요와 공급에 따라 가격이 결정되는 자본주의 경제에서 비트코인을 대상으로 새로운 비즈니스를 창출한 것이다.

블록체인이 탄생한 후 가장 빠르게 성장한 비즈니스가 암호화폐 거래소다. 최초의 암호화폐 거래소는 2010년에 오픈한 'Bitcoin Market'이었다고 하나 현재 존재하지 않으며 같은 해 마운트고크스(MtGox)가 일본에 설립됐다. 한국 최초의 원화 거래소는 2013년 설립된 코빗(Korbit)이다. 이후 암호화폐 종류가 늘어나고 가격이 상승하면서 세계 각지에 다양한 거래소가 설립되었다.

2018년 5월 8일 현재 1일 거래량 기준으로 암호화폐 거래소 1위와 2위는 오케이이엑스(OKEx), 바이낸스(Binance)다. 두 거래소는 모두 홍콩에 설립돼 주로 중국인들을 대상으로 영업을 하다 최근 몰타로 이전했다. 몰타 정부는 '몰타 디지털 혁신 기구(Malta Digital Innovation Authority)'를 설립했으며 몰타를 하나의 블록체인, 암호화폐 허브로 만들 계획을 설계하고 있다. 두 거래소 모두 법정화폐를 받지 않고 비트코인이나 이더리움을 다른 암호화폐로 교환해주는 거래소다.

4위인 비트플라이어(BitFlyer)는 일본 정부에 공식 등록된 거래소로 미국 뉴욕주로 진출할 계획인 것으로 알려져 있다. 코인 상장에 매우 보수적이며 비트코인 거래량만을 기준으로 보면 세계 1위 거래량을 기록하고 있다.

10위권 내에 한국 거래소는 2개로 업비트와 빗썸이 있다. 암호화폐 투자 열풍이 불던 지난 해 빗썸이 한 때 세계 1위 거래량을 기록하기도 했으나 이후 한국 정부의 규제입장 발표, 실명인증제 영향으로 순위가 하락했다.

한국에서 암호화폐 거래소는 초창기에 인터넷 ‘통신판매업’으로 분류되었고 암호화폐 거래는 일반적인 인터넷 상거래로 간주됐다. 애초에 암호화폐의 성격에 대한 규명이 없었기에 거래소에 대한 규정도 미비할 수 밖에 없었던 것이다. 암호화폐 거래가 활발해지면서 거래소는 급격하게 늘어난 상황에서 거래의 투명성, 서버의 보안성, 고객 자산관리 등 거래소에 대한 우려가 일고 있다. 보안성이 뛰어나다고 알려진 블록체인 기반의 암호화폐를 거래하는 거래소의 보안 상태가 전통적인 금융기관의 관리 수준에 비해 현저히 취약하다는 것은 참으로 모순된 현실이다.

2014년 마운트곡스가 해킹으로 파산한 후 일본에서는 거래소 보안, 고객 자산관리 등에 대한 논의가 활발해졌다. 이와 동시에 암호화폐의 성격을 무엇으로 볼 것인지, 얼마나 규제해야 할 것인지에 대한 논의도 시작됐다. 수년간의 실태조사와 토론 끝에 일본은 2017년 비트코인을 지급결제 수단으로 인정했고 암호화폐 거래소에 대한 엄격한 등록 기준을 공개했다. 어찌보면 거래소 파산으로 인해 일본은 국가 차원에서 암호화폐에 대해 적극적인 검토를 할 수 있었던 것 같다.

물론 한국에서도 거래소 해킹에 의해 고객 자산이 유실되고 거래소가 파산하는 등 다양한 사건, 사고가 있었다. 하지만 한국에서 국가 차원의 적극적인 규제 검토가 시작된 계기는 암호화폐 투자 열풍이었다. 2017년 한국 거래소 거래대금이 무서운 속도로 급증하자 정부와 민간의 본격적인 토론이 시작됐다.

이후 금융당국은 일부 거래소의 실태조사를 하는 한편, 블록체인협회에서는 자율규제안을 발표하고 거래소 요건을 강화하려 하고 있으나 여전히 불완전한 상태다. 다른 금융 거래와 마찬가지로 암호화폐 거래소에 대한 규정도 강화될 것으로 예상된다. 나아가 암호화폐 관련산업이 성장할수록 주식이나 예금을 취급하는 전통적인 금융업과는 근본적으로 다른 방식의 제도가 요구될 것이다.

[그림23] 암호화폐 거래소 순위 (암호화폐 전체 거래량을 비트코인으로 환산해 산출)



자료: Coinhills, 한화투자증권

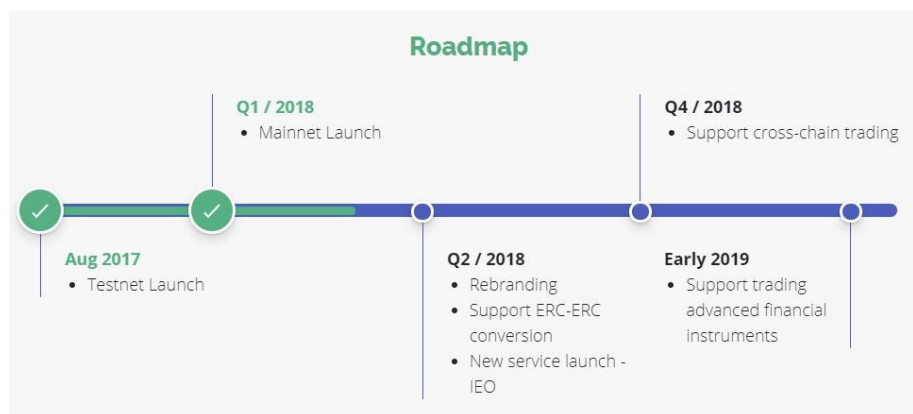
탈중앙화 거래소(DEX: Decentralized Exchanges)

중앙집중식 거래소 문제를 해결하려는 시도로 블록체인 기반의 탈중앙화 거래소 프로젝트도 등장하고 있다. 중앙 집중 서버가 없는 블록체인 상에서 개인과 개인이 토큰을 직접 거래할 수 있는 거래소다. 0x 프로젝트, 에어스왑(AirSwap), 카이버네트워크 등 다수의 프로젝트가 있는데 최근에는 이미 중앙집중식 거래소를 운영하고 있는 바이낸스도 탈중앙화 거래소를 바이낸스 체인이라는 이름의 퍼블릭 블록체인으로 공개하겠다고 밝혔다. 탈중앙화 거래소가 활성화되면 중앙집중식 거래소보다 해킹이 어려워지고 익명성을 유지할 수 있으며 수수료도 낮출 수 있다.

하지만 현재 블록체인 기술로는 탈중앙화 거래소가 기존 거래소를 대체하기보다는 상호 보완관계로 점차 발전할 가능성이 높다. 탈중앙화 거래소는 블록체인 상에 거래 승인을 받는 데 시간이 필요하고 사용자가 충분히 확보되지 않으면 거래가 어렵다는 단점이 있다. 만약 사용자가 급증할 경우에는 거래 승인에 상당한 시간이 필요할 것이다. 따라서 현재 퍼블릭 블록체인의 초당 거래 승인 건수로는 대규모 거래를 반영하기 어렵다.

퍼블릭 블록체인의 확장성 문제가 하나씩 해결될 때, 탈중앙화 거래소 프로젝트도 함께 성장할 수 있을 전망이다. 최근 논의되는 상황에 비춰 볼 때, 빠르면 2020년경에는 탈중앙화 거래소가 상용화될 수 있지 않을까? 사람마다 기대하는 시점의 차이는 있겠지만, 블록체인 기반의 암호화폐를 블록체인을 통해 개인 간에 거래하려는 탈중앙화 거래소의 시도는 지속될 것이다.

[그림24] 카이버 네트워크 로드맵



자료: Kyber Network, 한화투자증권

2. 빔(VEEM)의 국제 송금 서비스

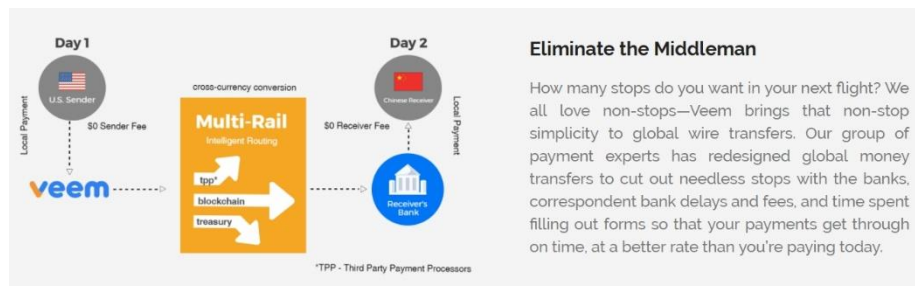
국경을 넘어 자유로운 송금을 할 수 있다는 점이 비트코인의 강점인 덕분에 블록체인 관련 스타트업 중에는 국제 송금 서비스를 제공하는 스타트업이 상당히 많다.

미국 스타트업 빔(VEEM)은 블록체인 기술을 활용해 저렴한 수수료로 신속한 국제 송금 서비스를 제공하고 있다. 2017년 11월 현재 60개 국가에서 송금과 수취가 가능하다. 이 회사는 2015년 4월 서비스를 개시했는데 1년만에 누적 100만 달러 이상의 국제 송금을 완료했다.

비용과 시간이 많이 소요되는 국제 송금 절차를 해결하기 위해 블록체인 기술을 적용했고 송금 절차에서 암호화폐를 사용함으로써 비용과 시간을 절약했다. 처리 과정은 웹사이트에 투명하게 공개되며 송금 수수료는 1%대로 시중은행의 5분의 1에 불과하다.

이 회사는 GV(Google Ventures), SBI Investment 등으로부터 투자를 받았다. 투자자를 잘 기억해두자. 블록체인 업계에서는 탈중앙화에 대한 논란이 많은데 블록체인 스타트업에 가장 많이 투자하고 있는 기업들은 구글 같은 거대 공룡기업이다.

[그림25] 미국 스타트업 VEEM의 국제 송금 서비스



자료: VEEM, 한화투자증권

3. 마이크로그리드에 블록체인 기술을 결합한 에너지 P2P 거래

금융에 이어 블록체인을 적극적으로 시험하고 있는 산업으로 에너지 산업이 있다. 지금까지 전기는 중앙 집중형 발전소에서 생산되어 먼 거리까지 송전했는데 P2P 거래를 통하면 비용을 줄이고 효율을 높일 수 있는 가능성이 있다. 대부분의 선진국에서는 신재생 에너지를 개발하면서 분산 전력 시스템과 스마트그리드에 대한 연구와 투자를 오랫동안 해왔기에 제도적 저항도 크지 않다. 아직 대규모로 적용하기에는 블록체인 기술의 한계도 분명 존재하지만 기존 시스템이 잘 갖춰진 산업에서 블록체인이 대부분 실패할 가능성이 높은 상황에서 에너지 P2P 거래는 실현 가능성이 높은 분야로 꼽힌다.

옆집에서 생산하는 태양광 에너지를 전력 회사가 도매가로 사가는데 이 과정에서 상당한 전력 손실이 발생한다. 전력원에서 거리 하나 떨어진 집은 여전히 전력회사를 통해 전력을 공급받으며 이웃에서 생산한 신재생 에너지를 사는데 소매가를 지불한다. 효율적이지 않은 것은 물론이며 불합리한 구조가 아닐 수 없다.

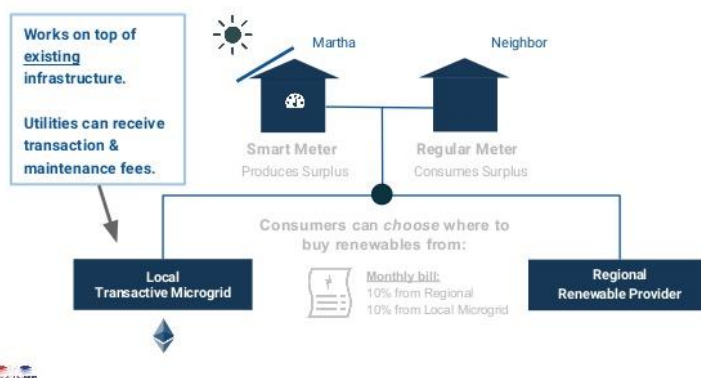
미국 뉴욕 브루클린에서는 'LO3ENERGY'라는 스타트업이 지멘스와 협업해 '브루클린 마이크로그리드'라는 시범 프로젝트를 시행하고 있다. 브루클린 마이크로그리드는 기존의 전력 에너지 마이크로그리드에 블록체인 기술을 결합해 전기를 P2P로 거래할 수 있게 해주는 프로젝트다. 이 프로젝트는 이더리움 플랫폼을 기반으로 구현됐다.

이더리움을 기반으로 에너지 산업에 블록체인 기술을 활용하기 위해 EWF(Energy Web Foundation) 재단도 다양한 프로젝트를 추진하고 있다. 글로벌 에너지 기업인 셸(Royal Dutch Shell), 스타트오일(Statoil), 도쿄 전력 등이 250만 달러의 기금을 출연하고 공동 연구 중이다.

사물인터넷 시대가 오면 전력을 소비하는 연결된 장치의 종류가 지금보다 몇배로 늘어날 전망이다. 매번 사람이 직접 제어할 필요 없이 기계 간에 설정된 스마트 계약대로 정보를 교환하고 거래를 기록하는 블록체인에 대한 니즈는 앞으로 더욱 커질 것이다.

[그림26] 브루클린 마이크로그리드의 스마트 에너지 P2P 블록체인

Transacting Local Energy with Neighbors



자료: Brooklyn Microgrid, 한화투자증권

4. 영상, 음악 등 디지털 콘텐츠 거래와 저작권 수익 배분

디지털 콘텐츠 산업에도 변화가 기대된다. 콘텐츠 생산자와 소비자가 블록체인을 통해 직접 거래할 수 있다. 미국 스타트업 Streamium은 마이크로 페이먼트를 사용해 스트리밍 서비스로 동영상을 제공하는 생산자와 시청자 간에 시청 시간만큼 암호화폐로 거래할 수 있는 서비스를 실험했다. 제작자는 시청자가 시청하는 만큼 시청료를 받을 수 있고 시청자 역시 소비한 만큼 소액 결제가 가능하며 블록체인 상에 투명하게 기록된다. 블록체인을 활용하게 되면 소액의 종량제 과금이 가능해진다.

저작권 관리와 관련된 프로젝트도 많아 지고 있는데 특히 음악계에서 거는 기대가 크다. 인터넷 시대로 넘어오면서 수많은 디지털 콘텐츠가 무료로 소비되고 있으며 작곡가나 음악가보다 거대 플랫폼 기업이나 제작사가 대부분의 수익을 가져간 지 오래다. 아직 실험적인 단계이기는 하지만 블록체인 기술은 이러한 구조적 문제점을 해결해 줄 수 있는 가능성을 보여주고 있다.

영국 싱어송라이터인 이모젠 힙(Imogen Heap)은 2015년 ‘Tiny Human’이라는 신곡을 블록체인 기반의 음원 유통 서비스 ‘우조 뮤직(Ujo Music)’에 독점 공개했다. 우조 뮤직은 사용자가 이더리움으로 음원을 구입할 수 있는 곳이다. 사용자가 음원을 구매하면 그 금액은 곧바로 프로듀서와 작사가, 엔지니어 등 곡 생산에 참여한 전문가들에게 배분된다. 이더리움의 스마트 계약을 활용한 것이다. 블록체인을 활용하면 중개자 없이 저작권자와 사용자간 직접 거래를 할 수 있어 중개 비용을 없앨 수 있으며 거래 현황이 모두 투명하게 공개된다.

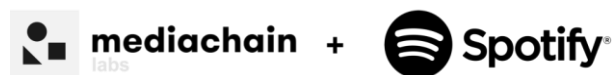
유니콘으로 성장한 세계적인 음악 스트리밍 업체, 스포티파이(Spotify)는 2017년 4월 블록체인 기술 기업인 미디어체인랩(Mediachain Labs)을 인수했다. 앞으로 많은 플랫폼들이 블록체인을 활용해 음원에 대한 저작권 문제를 해결하고 투명한 과금을 할 수 있을 것으로 기대한다.

[그림27] 영국 싱어송라이터, 이모젠 힙



자료: CIO Korea, 한화투자증권

[그림28] 스포티파이의 미디어체인 인수



자료: 한화투자증권

5. 중계자가 없는 글로벌 상거래 플랫폼

오픈바자(Open Bazaar)는 P2P 기반으로 개인 간 상거래를 할 수 있게 해주는 블록체인 플랫폼이다. 아마존이나 이베이처럼 중앙 서버를 두고 기업이 운영하는 것이 아니라 물건을 팔고 싶은 누구나 들어가서 제품을 내놓으면 사고 싶은 사람과 직접 거래할 수 있다. 거래 중개자나 운영 주체가 없으므로 중계 수수료나 플랫폼 사용료가 발생하지 않는다.

오픈바자 홈페이지에서 소프트웨어를 다운로드 받아 실행하면 오픈바자의 노드로 참여할 수 있다. 네트워크에 접속해 개인과 개인이 직접 조건을 설정하고 거래한다. 2016년 오픈할 당시에는 비트코인으로만 거래가 가능했는데 결제수단을 점차 다양한 암호화폐로 확대하고 있다.

영세 상인이 온라인 커머스 플랫폼에서 상품을 판매하려면 은행 계좌 개설부터 많은 절차를 밟아야 하고 특히 국경을 넘어 판매하려면 더욱 복잡해진다. 은행이나 카드사 등 금융기관과 플랫폼에 지불해야 하는 수수료도 부담이다. 오픈바자를 이용하게 되면 은행 계좌 개설이 불필요하고 금융기관이나 플랫폼에 수수료도 지불하지 않는다.

오픈바자 소프트웨어를 개발하고 있는 팀은 캐나다의 스타트업 OB1이다. 창업자들은 초기 비트코인 커뮤니티에서 P2P 기반의 직거래 플랫폼을 개발할 수 있다는 아이디어에 열광해 이 프로젝트를 시작하게 되었다고 말한다. 오픈바자는 무료로 배포되는 오픈 소스 프로젝트로 코드가 모두 공개되어 있다. 누구나 새로운 아이디어나 코드 수정을 제안할 수 있다. 2017년 하반기에는 모바일로도 풀 노드로 참여할 수 있는 어플리케이션을 개발했다.

오픈바자에서는 거의 모든 것을 거래할 수 있다. 현재 품목 카테고리를 물리적 상품(physical goods), 디지털 상품(digital goods), 서비스로 구분하고 있는데 암호화폐도 새로운 품목으로 추가할 계획이다.

[그림29] 오픈 바자: 누구나 무엇이든 수수료 없이 사고 파는 플랫폼

Sell Anything. Pay Zero Platform Fees.
Create a store. Sell whatever you'd like. Reach a new audience. Get paid in cryptocurrency.

<p>Forever Tomorrow [EP] ★ 4.7 (132) \$4.99</p>	<p>Summer Shades (original art) ★ 4.2 (23) \$500.00</p>	<p>Blue Tank Top ★ 4.8 (242)</p>

- ✓ No Platform Fees
- ✓ No Monthly Fees
- ✓ No Listing Fees
- ✓ No Bank / CC Required
- ✓ Live Chat with Customers
- ✓ Customize Your Store
- ✓ Peer to Peer (no middleman)

자료: www.openbazaar.org, 한화투자증권

오픈바자는 디지털 파일 거래를 암호화폐 기반의 자동화된 스마트 계약으로 구현 할 계획이다. 사진이나 음악, 문서 등 각종 파일을 개인 간에 직접 거래할 때 편리하게 사용할 수 있을 것으로 기대된다.

OB1은 현재까지 안드리센 호로비츠(Andreessen Horowitz), 유니온 스퀘어 벤처(Union Square Ventures)와 같은 저명한 벤처 캐피탈 회사와 디지털 커런시 그룹(Digital Currency Group), 블루야드(Blueyard Capital) 등 크립토 투자사를 포함해 약 4백만 달러 이상의 시리즈A 투자를 받았다.

벤처투자 자금으로 소프트웨어를 개발해온 OB1은 곧 비영리법인인 오픈바자 재단(Openbazaar Foundation)을 설립하고 오픈바자토큰(OBT; OpenBazaar Token)도 발행 할 계획이다. 아직까지는 ICO 유무나 토큰 발행 및 배분에 관한 구체적인 내용은 공개 되지 않았다. 사용자와 개발자, 그리고 큐레이터가 함께 이 커뮤니티를 성장하게 하는데 OBT 토큰을 인센티브로 활용할 계획이다. 토큰을 발행한다고 해도 오픈바자 플랫폼에 수수료를 부과하는 일은 없을 것이라고 공언했다.

현재까지 구현된 수준만 놓고 보자면 오픈바자는 아마존이나 이베이보다 경쟁력이 없다. 소비자 입장에서는 최저가나 최단시간에 배송해주는 아마존이 훨씬 매력적이다. 하지만 오픈바자는 아직 완성된 플랫폼이 아니다. 블록체인으로 상거래가 어떻게 변화할 수 있는지 그 가능성을 보여주고 있다.

은행계좌나 신용카드가 없는 사람들 간에도 거래가 가능하고 국경을 뛰어 넘는 거래가 개인 간에도 가능하다. 소소한 디지털 사진 파일도 개인 간에 얼마든지 거래할 수 있다. 오픈바자가 얼마나 성공적으로 성장하게 될 지 속단할 수 없지만 아마존에서 구매하기 어려운 상품, 아마존에 진입하기 어려운 판매자를 끌어모을 수 있다는 잠재력이 있다. 인터넷의 등장으로 오프라인 유통업을 온라인 플랫폼이 잠식했듯 블록체인의 등장으로 또 한번 커머스 생태계에 지각변동이 일어날 수 있을지 귀추가 주목된다.

[그림30] 오픈 바자 개발팀이 제안하는 오픈바자의 특징

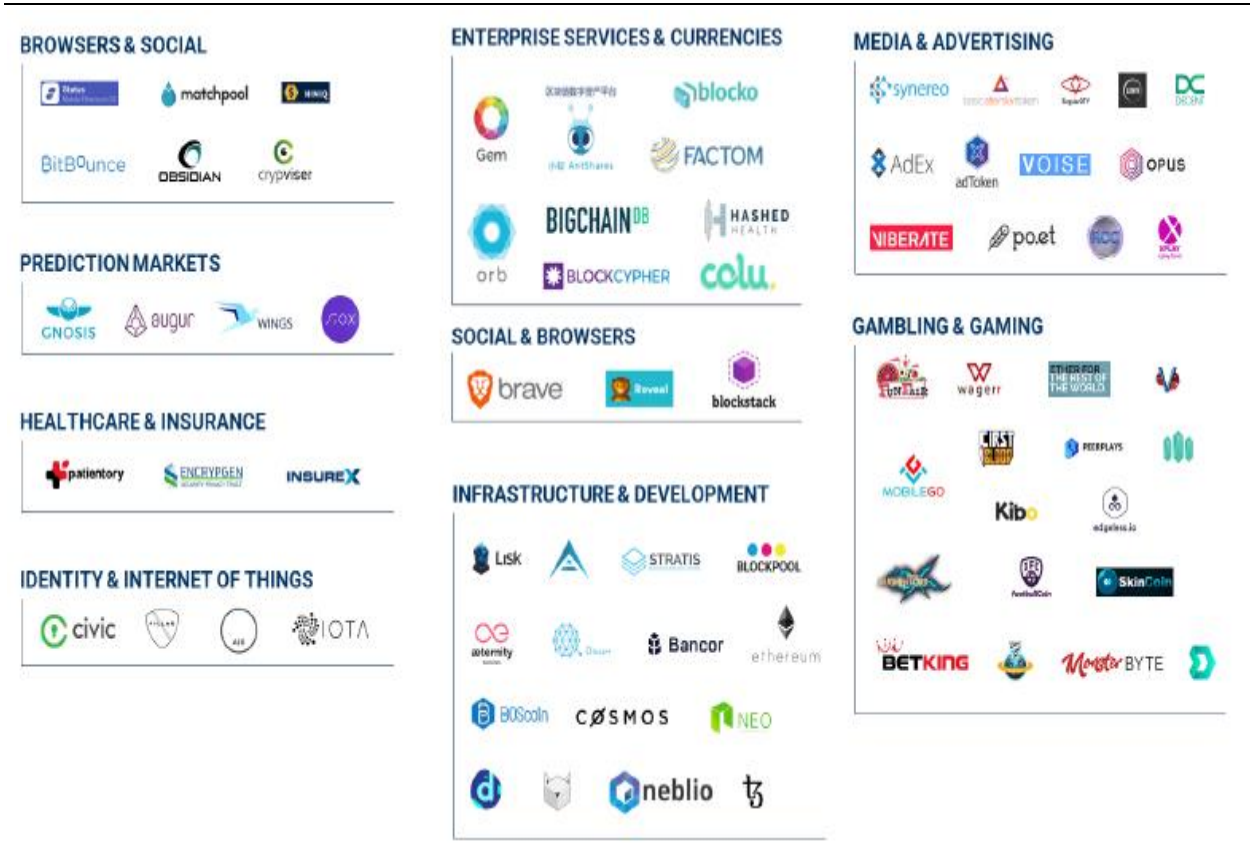
1. **Anyone Can Buy and Sell Anything to Anyone Anywhere for Free**
 - Free to download and use
 - Permissionless (No banks, credit cards, paperwork, or approval needed)
 - No restrictions on who can buy or sell
 - No restrictions on what you can buy or sell
 - No restrictions on where trade can occur (borderless)
2. **You Control Your Own Trade**
 - Decentralized (controlled by no one; belongs to everyone)
 - You control your own information
 - Private (identity, location and activity are yours to control)
 - No one can censor your trade
 - Open source; anyone can add to or modify code with no restrictions
3. **P2P Trade for Everyday People**
 - It's equal to or better than other professional e-commerce platforms
 - It's secure and trustworthy
 - It's easy to use and understand
 - Removes as many barriers to trade as possible

자료: www.openbazaar.org, 한화투자증권

이밖에도 부동산 등기, 문서 공증, 유연장 등 제 3자의 인증이 필요한 분야와 SCM(공급망 관리) 등 시간 흐름에 따른 추적이 필요한 많은 분야에서 블록체인 기술을 활용하는 기업들이 탄생하고 있다. ‘블록체인 혁명’의 저자 돈 탭스콧은 유니콘으로 성장한 우버나 에어비앤비 같은 공유경제 모델도 블록체인으로 대체될 가능성이 있다고 말한다.

현재의 기술로는 처리 속도·용량의 문제나 법률적·제도적 문제로 기술 확산에 한계가 있으며 수익을 창출하지 못하고 실패하는 프로젝트가 대다수일 것이다. 그러나 기술은 점차 발전하고 있고 더 많은 기업들이 다양한 시도를 거듭할수록 한계를 극복할 가능성도 높아진다. 블록체인을 통해 중개자를 배제하거나 중개자의 역할을 축소하고 투명한 계약 이행과 거래가 가능해질 수 있는 분야는 점점 늘어날 것이다.

[그림31] 블록체인 관련 다양한 스타트업



자료: CBInsights, 한화투자증권

6. 글로벌 기업들의 블록체인 추진 현황

다양한 스타트업이 생겨나는 동시에 글로벌 기업들도 블록체인에 뛰어 들고 있다. 글로벌 기업들은 대체로 퍼블릭 블록체인 보다 하이퍼레저나 코다(Corda) 같은 프라이빗 블록체인 기반으로 시범 프로젝트를 먼저 추진해보려는 분위기다. 독자적인 퍼블릭 블록체인을 목표로 하는 기업도 있지만 현재까지는 여러 기업들이 연합해 추진하는 허가형 블록체인 프로젝트가 많다.

하이퍼레저와 R3CEV의 코다(Corda)

IBM과 머스크의 합작

2018년 1월, IBM과 머스크(Maersk)는 합작법인 설립계획을 발표했다. 글로벌 해운 생태계 전반에 적용할 수 있는 국제무역 블록체인 플랫폼을 공동 개발해 화물의 무역 운송 절차를 단순화하고 투명성을 높이는 동시에 비용을 감축하겠다는 취지에서다.

세계선사협의회(WSC)에 따르면 현재 연간 해상운송 화물은 미화 4조 달러 이상이며, 이 중 일상 소비재가 전체 화물의 80% 이상을 차지한다. 세계무역 생태계는 비용과 규모가 증가함에 따라 점점 더 복잡해지고 있다. IBM과 머스크는 블록체인을 활용하면 비용과 시간을 절약할 수 있을 것으로 기대하고 있다.

이들은 블록체인을 통해 다수의 교역 파트너가 같은 내용의 거래 내역을 공유하되 세부 사항과 기밀정보 등에 대한 정보 보안은 강화하고자 한다. 제조사, 해운사, 포워딩 업체, 항만 터미널 운영사, 화주 및 세관 등 관련 업계와 기관, 그리고 고객들에게까지 광범위한 혜택을 제공할 것이라는 포부를 밝혔다. IBM이 참여하고 있는 리눅스 재단의 하이퍼레저 패브릭 (Hyperledger Fabric)을 기반으로 한다.

금융권 R3CEV 컨소시엄

금융권에서는 컨소시엄 블록체인의 사례로는 앞서 기술한 R3CEV 컨소시엄이 대표적이다. 그밖에도 미국 나스닥은 비상장 주식을 거래할 수 있는 프라이빗 블록체인을 개발에 투자했고 AIG, 알리안츠 등 보험사들은 스마트 계약을 활용하는 블록체인 프로젝트를 추진하고 있다.

마이크로소프트와 ID2020 얼라이언스

ID2020

마이크로소프트는 유엔 주도 하에 진행되고 있는 'ID2020'이라는 프로젝트에 참여하고 있다. 세계 약 11억 명 이상의 사람들은 공식적으로 정부에게 신원을 인정받지 못해 교육, 보건, 투표 참여, 은행 계좌 개설 등 국가의 시민들에게 제공되는 기본적인 혜택조차 받지 못하고 있다. 'ID2020 얼라이언스'는 세계 모든 사람들에게 출생 등록을 포함하여 합법적인 법적 신분을 제공하려는 프로젝트다. 마이크로소프트는 엑센추어와 함께 개인 신원을 영구적으로 등록하고 관리할 수 있는 블록체인 프로토타입을 발표했다. 성공한다면 신분증 없는 난민도 블록체인으로 신분을 증명할 수 있게 된다.

세계 4대 자동차 기업들과 블록체인 스타트업의 연합

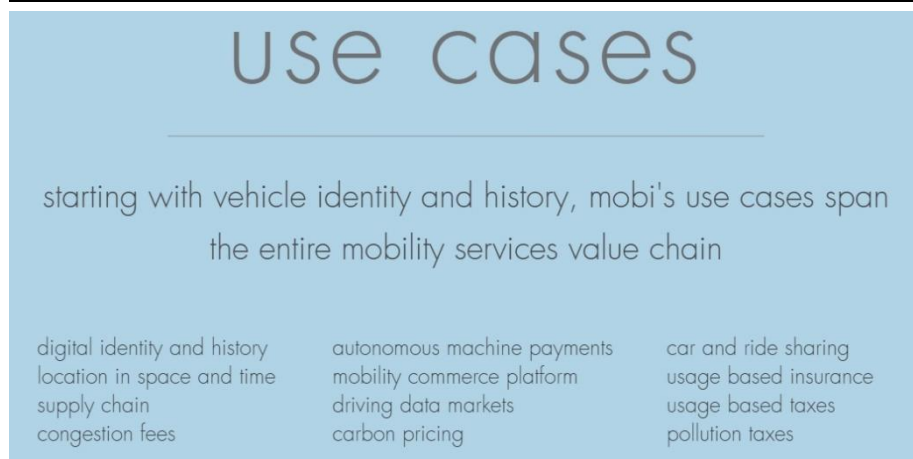
자동차 산업에서는 차량 공유 서비스(Car sharing)나 자율주행차가 주요 화두도 자리잡았다. 당장 내일은 아닐지라도 앞으로 다가올 새로운 모빌리티 시대에 자동차 산업에는 큰 지각 변동이 일어날 수 있다. 우버의 성장과 구글의 진입에 위협을 느끼고 이미 빅데이터와 인공지능을 연구하기 시작한 자동차 회사들은 블록체인 프로젝트도 시작했다.

2018년 5월, 세계 4대 자동차 기업들은 블록체인 스타트업과 연합해 자동차 산업에서 블록체인을 도입하는 방안을 연구하고자 컨소시엄 모비(MOBI; Mobility Open Blockchain Initiative) 출범을 발표했다. BMW, 포드, GM, 르노(Renault)를 비롯해 컨센시스(Consensys), 빅체인디비(BigChainDB), 대시라이드(Dashride) 등 블록체인 스타트업들과 IBM, 엑센추어, 하이퍼레저(Hyperledger)등이 모비 컨소시엄에 참여한다. 이들의 목표는 자동차들 간에 데이터를 공유하고 결제할 수 있는 표준 플랫폼으로 자율주행이나 차량 공유 서비스 등을 구현할 수 있는 기반을 함께 만드는 것이다.

구글과 애플, 아마존 알렉사까지 거대 플랫폼 기업들이 자동차 산업으로 침범해온 지 수년째다. 산업간 경계가 무너지고 있다. 자동차 하드웨어를 만드는 산업보다 자동차 안과 밖에서 취득할 수 있는 데이터를 활용해 만들어낼 수 있는 산업의 규모가 더 커질 것이다. 위치 정보, 이동 경로 정보뿐 아니라 차 안에서 보고 듣는 콘텐츠, 주변의 대기 상태나 기후, 이산화탄소 배출량에 이르기까지 다양한 데이터를 취득할 수 있다면 이를 기반으로 활용할 수 있는 서비스가 무궁무진할 것이기 때문이다.

자율주행은 기술만으로 구현할 수 있는 것이 아니라 제도 변화와 사회적 합의도 필요하다. 물론 현재 블록체인의 한계로 지목되는 확장성과 처리속도, 분산 저장 문제를 해결해야 한다. 기술 역시 아직 초기 단계임을 감안하면 아주 오래 걸릴 일인 지도 모른다. 하지만 블록체인으로 인해 오랫동안 상상 속에 머물러 있던 미래가 한 발짝 가까워지고 있는 듯 하다.

[그림32] 모비 컨소시엄이 구현하고자 하는 블록체인의 용도



자료: MOBI, 한화투자증권

Ⅶ. 블록체인과 디지털 경제, 그리고 크립토 에셋

1. 블록체인과 암호화폐, 분리할 수 있을까?

지난 해 암호화폐 투자가 과열되자 젊은이들의 암호화폐 투자열풍이 사회적인 문제로 부각됐다. TV와 라디오에서는 연일 공학박사와 경제학자, 정치인들까지 나서 열띤 공방을 벌였다. 일부 학자들은 국가가 보증하지 않는데다 통제도 어려운 암호화폐에 대해 비판을 쏟아냈고 강력한 규제를 통해 이를 제어해야 한다거나 규제가 어렵다면 완전히 금지해야 한다는 얘기까지 나왔다.

블록체인 예찬론자들은 암호화폐와 블록체인은 분리할 수 없으며 4차 산업혁명이나 일자리 창출을 논하는 한국 정부에서 암호화폐 거래를 전면 금지한다는 것은 어불성설이라고 비판했다. 한편, 암호화폐 거래를 반대하는 측에서는 암호화폐가 가지고 있는 부정 부주의적 속성을 비판했다. 화폐라고 부를 수 있는 것은 국가나 중앙은행이 발행한 법정화폐뿐인데 국가가 보증하지 않는 가상의 화폐를 만들어 이것도 화폐라고 주장하는 것은 의도적인 사기라는 것이다.

그래서 암호화폐를 강하게 반대하는 측에서는 사기가 빈번하게 일어나고 국가 경제를 교란 시킬 수 있는 암호화폐를 전면 금지하라고 주장한다. 그렇다면 블록체인과 암호화폐를 분리할 수 있을까?

프라이빗과 컨소시엄 블록체인에서 암호화폐는 필수요소가 아니다. 하이퍼레저(Hyperledger)나 코다(Corda)의 경우에도 암호화폐는 존재하지 않는다. 암호화폐 없이도 자본을 보유한 대기업들이 블록체인을 만드는 것은 얼마든지 가능하다. 하지만 컨소시엄 블록체인에서도 암호화폐 없이는 성과보상이나 분배가 어렵다. 출자한 지분만큼 영향력을 행사하거나 이익을 얻지 못하면 컨소시엄에서 탈퇴하는 사례도 있었다. 금융업계 최대 블록체인 컨소시엄인 R3에서도 JP모건과 골드만삭스 등 많은 회사가 중간에 탈퇴했다.

암호화폐 없는 블록체인 개발의 더 큰 난제는 초기자본이 없으면 진입하기 어렵다는 점이다. 누구나 자유롭게 참여하거나 떠날 수 있는 공공재나 다름없는 퍼블릭 블록체인에 암호화폐가 없다면 어떻게 될까? 과연 누가 본인의 컴퓨터와 전기요금, 시간을 들여 데이터 검증과 저장에 참여할 것인가? 비트코인의 경우, 작업증명 노드에게 신규 비트코인을 발행해줌으로써 인센티브를 지급한다. 참여자들은 인센티브를 받기 위해 네트워크에 참여하고 비트코인의 가치를 더욱 키우기 위해 참여한다. 비트코인이나 이더리움이 네트워크 참여자에게 신규 암호화폐를 보상으로 지급하지 않았더라면 참여하는 사람이 그만큼 늘어나지 않았을 것이다.

블록체인은 참여자가 많으면 많을수록 네트워크의 가치가 상승한다. 비트코인의 시가총액이 현재 가장 높은 것은 비트코인 네트워크에 참여하는 노드와 사용자가 가장 많기 때문이다.

2. 비트코인은 미래의 화폐가 될 수 있을까?

비트코인이 화폐냐, 아니냐 논쟁이 한창이던 때, 여섯 살 아이들이 놀이하러 가는 장면을 보았다. 아이들은 색종이를 오려 시장놀이를 하고 있었는데 빨간동전 1개는 노란동전 10개, 노란동전 1개는 파란동전 10개라는 식으로 계산하는 것이었다. 노란동전 1개로 사탕 하나를 살 수 있다면 노란동전 5개로는 과자 한봉지, 빨간동전 하나는 캐릭터 장난감을 살 수 있는 식이다.

필자가 초등학교일 때, 동네에서는 남자아이들이 모여 구슬치기를 했었다. 구슬을 열개, 스무개, 백개를 따는 아이가 있었고 아이들은 구슬 몇 개와 지우개, 공책 같은 것들을 교환하곤 했다.

아이들에게 색종이로 만든 동전과 구슬은 아이들의 세계에서 화폐로 기능한다. 가치의 교환이나 저장, 가치의 척도 모두 그들 사이에서는 충분히 적용된다. 종이동전과 구슬이 그들만의 화폐라면 그 가치는 얼마쯤일까?

개념적으로 보자면 아이들이 가지고 있는 자산(?) 규모와 생산할 수 있는 가치를 교환하는 횟수에 따라 화폐 가치가 결정될 것이다. 아이 셋이 참여하는 종이동전 경제의 규모만큼 종이동전의 가치가 정해지고 아이 서른 명이 참여하는 구슬 경제의 규모만큼 구슬의 가치가 정해진다.

커뮤니티에 참여하는 사람들이 가지고 있는 자원, 자산의 크기와 산출물의 가치에 따라 그 사회의 경제규모가 결정된다. 화폐의 가치는 해당 사회의 경제규모와 비례한다. 아이들 사이의 놀이라고는 해도 시장놀이와 구슬놀이는 많은 것을 보여준다. 놀이에 참여하는 아이들이 많으면 많을수록, 그리고 아이들이 생산할 수 있는 재화와 아이들이 보유한 재화가 많을수록 종이동전과 구슬의 가치는 상승한다.

아이들은 시간이 지나면서 관심사가 바뀌고 더 이상 종이동전이나 구슬을 얻기 위해 모이지 않는다. 구슬을 더 많이 모으겠다고 비밀 서랍 속에 숨겨두었다가 그 존재조차 잊어버린다. 결국 종이동전과 구슬의 가치는 사라진다.

그렇다면 비트코인의 가치는 어떻게 될까? 비트코인의 미래 가격을 예측할 수는 없겠지만 비트코인은 종이동전처럼 사라질 가능성은 매우 낮다고 생각한다. 이미 전세계에 비트코인 장부를 기록한 풀 노드가 1만 개 이상으로 많아 기록된 내역을 모두 없애기 어렵다. 아이들의 약속은 지키지 않을 수도 있고 시간이 지나면 잊혀질 수 있다. 그래서 어른들에게 종이동전은 가치가 없다. 비트코인 역시 아무도 쓰지 않으면 가치가 사라질 수 있지만 기록이 조작될 수 없고 디지털로 영구히 저장 가능하다는 점에서 종이동전과는 큰 차이가 있다.

비트코인의 첫번째 사용, 세상에서 가장 비싼 피자

비트코인이 처음부터 이렇게 각광 받은 것은 아니었다. 비트코인은 탄생한지 벌써 10년 차에 접어들었는데 대중의 관심을 받으며 거래가 본격적으로 활발해진 것은 몇 년 되지 않았다. 비트코인은 초기에 가치가 없었고 실물 경제에서 존재감을 드러내지도 못했다. 소수의 엔지니어들이 호기심을 가지고 오픈소스인 비트코인 소프트웨어를 구동해 보고 의견을 교환했을 뿐이다.

2010년 최초의 비트코인 거래소가 설립되었지만 당시 비트코인 가격은 채굴하는 데 드는 전기요금만도 못했고 교환가치도 없었다. 비트코인은 디지털 기술일 뿐 자본시장 참여자들의 관심사가 아니었다.

비트코인으로 구매한 첫번째 실물 거래는 다름아닌 피자였다. 2010년 5월 22일, 미국 플로리다의 잭슨빌에서 라스즐로 한예츠(Laszlo Hanyecz)라는 개발자가 사상 처음으로 비트코인을 실물 거래에 사용했다. 그는 비트코인 커뮤니티인 'https://bitcointalk.org' 사이트 Bitcoin Forum 게시판에 10,000개의 비트코인을 지불할 테니 라지 사이즈 피자 두 판을 배달해줄 사람을 찾는다라는 글을 올렸다. 글을 올린 지 사흘 후 'jercos'라는 닉네임의 사용자가 피자 두 판을 배달했다는 글이 올라왔다. 아래 도표는 라스즐로가 올린 인증샷과 비트코인 거래 기록이다. 비트코인 분산원장에 10,000 BTC의 거래 기록이 남았고 이는 지금도 누구나 확인 가능하다.

비트코인 이용자들은 이 날을 '피자데이'로 기념하고 있다. 25달러 정도의 라지 사이즈 피자 두 판과 교환한 1만 개의 비트코인은 현재 거래가격(2018년 5월 6일, 9600USD/BTC)으로 환산하면 96백만 달러, 한화로는 1천억원에 달한다. 비트코인 가격이 상승할 때마다 라스즐로의 글에는 당신이 먹은 피자가 10만 달러, 1백만 달러, 1천만 달러를 넘어섰다는 댓글이 기록되고 있다.

[그림33] 비트코인으로 피자를 구매한 거래 기록

트랜잭션 비트코인 거래에 대한 세부정보 보기

요약		입력 및 출력	
크기	23620 (bytes)	총 거래량	10,000.99 BTC
무게	94480	총 출력	10,000 BTC
수신 시각	2010-05-22 18:16:31	거래 수수료	0.99 BTC
블록에 포함됨	57043 (2010-05-22 18:16:31 + 0 분 전)	1 바이트 당 수수료	4,191.363 sat/B
승인	436676 승인	무게 단위당 요금	1,047.841 sat/WU
시각화	트리 차트 보기	예상 BTC거래량	10,000 BTC
		스크립트	스크립트 보기 & coinbase

자료: Blockchain.info, 한화투자증권

비트코인 1만개의 가치가 50달러였다가 1천달러, 1만달러, 1억달러, 그리고 지난 해 최고점에는 무려 2억달러까지 상승했다가 현재는 다시 1억달러 아래로 내려와 있다. 많은 경제학자들은 비트코인의 가격 변동이 지나치게 크다는 점이 화폐가 될 수 없는 이유라고 지적한다. 가격이 급등할 때는 지출하려 하지 않고 가격이 하락할 때는 얼마나 더 하락할 지 알 수 없으니 물건을 판매하는 쪽에서 받아주려 하지 않는다.

하지만 지금의 가격 변동폭만을 두고 비트코인이 화폐가 아니라고 단정할 수는 없을 것 같다. 어린아이들의 시장놀이를 떠올려 보자. 2010년 비트코인 1만개가 50달러 미만의 가치였던 것은 어린아이들의 시장놀이에서 쓰이는 종이동전처럼 비트코인 역시 아주 소수의 커뮤니티에서 쓰였기 때문이다. 비트코인이 화폐가 될 수 있다고 믿는 사람은 극히 소수였고 그들조차 비트코인의 미래를 알 수 없었기에 가격은 매우 낮았다. 비트코인을 화폐라고 믿고 거래하는 사람들의 경제 규모가 얼마나 커지느냐에 따라 비트코인의 가치는 변할 것이다.

아이들이 자라서 종이동전보다 한국은행권이 더 가치가 있다고 생각하면 종이동전의 가치는 사라진다. 비트코인도 마찬가지다. 새로운 암호화폐가 나타나 더 많은 사람들이 사용하게 되고 비트코인 사용자는 줄어든다면 그 가치는 낮아질 것이다.

최근 비트코인 시가총액은 약 150조원에서 200조원 사이를 오가고 있다. 이 가격이 적정한지 고평가, 저평가 되었는지 판단할 수는 없다. 비트코인이 미래의 화폐라고 생각해서 보유하고 있는 사람도 있을 테지만 가격이 올라갈 때 더 올라갈 것 같아서 구입한 투기적 수요도 많았을 것이다.

경제학적 관점에서 화폐수량설의 교환방정식에 빗대어 비트코인의 가치를 추론해보기도 한다. 비트코인을 화폐로 사용하는 사람들의 경제규모와 통화량, 그리고 화폐의 유통 속도에 따라 비트코인의 가치가 결정될 수 있다는 것이다. 화폐수량설이 이미 오래전부터 통하지 않는다는 논란 속에 이를 암호화폐 가치 산정에 적용한다는 것은 논란의 소지가 있다.

무엇보다 비트코인을 화폐로 믿고 사용하는 경제 규모가 얼마나 될 지, 하루아침에 사라져 버리지 않을런지 예측할 수 없다. 일본처럼 지급결제수단으로 인정하는 국가가 많아진다면 사용자가 늘어나고 가격도 상승할 수 있는 반면, 거래소 폐쇄와 같은 강한 규제가 나올 때에는 폭락해도 이상하지 않다. 따라서 당분간 비트코인 가격은 폭락할 수도 있고 폭등할 수도 있다.

[그림34] 화폐수량설과 교환방정식

19세기와 20세기 초 고전학파 경제학자들에 의해 발전된 이론이다. 1911년 어빙 피셔는 '화폐의 구매력(The Purchasing Power of Money)'에 화폐수량방정식을 제시했는데 이후 이것은 화폐수량설로 발전했다. 화폐의 유통속도가 단기에 일정하다는 피셔의 견해로부터 화폐수량설은 명목 GDP가 오직 통화량에 의해 결정된다고 설명했다.

$$MV=PY$$

M: 통화량

V: 화폐유통속도

PY: 명목GDP

자료: 한화투자증권

비트코인으로 물건도 살 수 있고 여행도 할 수 있다. 달러나 금만큼 세계적으로 통용되는 것은 아니나 비트코인 거래에 참여하는 사람들은 늘어났다. 비트코인이 빠르게 확산될수록 논쟁도 치열해진다. 기술에 열광하는 사람들과 보수적인 학자, 관료들 사이에 관점의 차이가 크다. 양측의 주장을 살펴보자.

경제학자들은 대체로 비트코인에 대해 부정적인 의견을 제시한다. 미국 연방준비제도 이사회의 이사를 역임한 미쉬킨 교수(Frederic S. Mishkin)는 그의 저서, 화폐와 금융(The Economics of Money, Banking, and Financial Markets - 제 11판)에서 비트코인이 미래의 화폐가 될 수 없는 이유를 다음과 같이 설명했다.

화폐의 3가지 기능은 교환의 매개, 계산단위, 가치의 저장이다. 비트코인은 확실히 교환의 매개수단으로 잘 기능한다. 비트코인을 통한 거래에 수반되는 수수료는 신용카드나 직불카드의 경우보다 상당히 낮다. 또한, 비트코인을 통한 거래는 익명으로 할 수 있어서 프라이버시를 지키고 싶은 사람들에게 매우 매력적이다.

그러나 비트코인은 계산단위와 가치의 저장이라는 2가지 화폐의 기능은 잘 수행하지 못한다. 비트코인의 가격은 매우 변동이 심하다. 높은 변동성은 비트코인이 가치의 저장수단으로서 잘 기능하지 못한다는 것을 의미한다. 즉 비트코인을 보유하는 것은 너무 위험성이 크다. 이러한 변동성 때문에 비트코인은 계산단위가 되지 않았다. 상품의 가격을 비트코인으로 표시하는 사람은 거의 없다.

이와 같이 미쉬킨 교수는 비트코인이 화폐의 3가지 기능 중 2가지를 충족시키지 못하기 때문에 미래의 화폐가 되지 않을 것이라고 설명했다. 다만 전자 거래를 저렴하게 사용하도록 하는 기술적 측면은 미래 전자결제 시스템의 하나의 특색이 될 것이라고 보았다.

비트코인에 대해 대표적인 회의론자로 폴 크루그먼(Krugman) 교수가 유명하다. 그는 2013년 뉴욕타임스에 ‘비트코인은 악이다(Bitcoin is Evil)’라는 글을 썼다. 비트코인은 정상적인 화폐가 아니라 중앙은행 시스템을 공격하려는 정치적 동기를 가지고 있고 금에 대한 물신주의(gold fetish)와 다를 바 없다고 비난했다. 비트코인이 탄생한 배경과 탈중앙화라는 개념을 생각해보면 이를 악이라고 비난하는 입장도 충분히 이해할 만하다. 현존하는 국가와 화폐 시스템을 부정하는 것으로 비춰질 수 있기 때문이다.

워런 버핏은 ‘비트코인은 진정한 버블 상태’라며 버블 붕괴 위험을 경고했다. 비트코인은 가치창출을 할 수 있는 자산이 아니기 때문에 가치를 평가할 수 없다며 가치 평가를 할 수 없는 상태에서 가격이 상승하고 있다는 점이 진정한 거품이라고 말했다. 전 연방준비제도(Fed) 의장 재닛 옐런(Janet Yellen) 역시 비트코인은 매우 투기적인 자산(highly speculative asset)이라고 말한 바 있다.

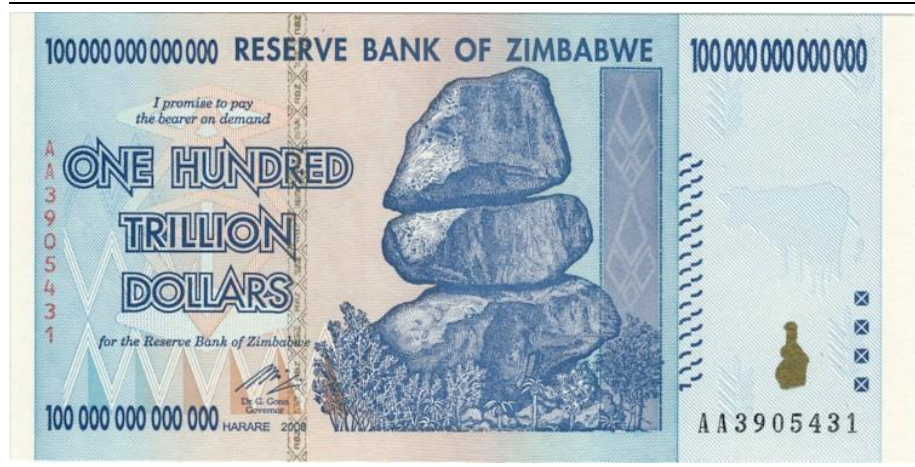
하지만 일각에서는 비트코인이 완전히 새로운 개념이 아니라 오랜 기간 동안 논의되어 온 민간 화폐라고 주장한다. 하이에크 등을 배출한 오스트리아학파의 철학과 비트코인의 지향점이 유사하다는 것이다. 오스트리아학파는 중앙은행의 통화정책을 비판했으며 일부 경제학자는 상품화폐, 즉 금본위제를 주장했다. 비트코인의 발행량은 총량이 21백만개로 제한되어 있어 채굴량이 한정되어 있는 금과 유사하다는 점에서 비트코인의 모태는 오스트리아학파의 화폐 이론일 것이라고 보는 사람들도 있다.

대한민국은 화폐가치가 상당히 안정적인 국가에 속한다. 외환위기를 겪었음에도 매우 빠른 속도로 위기를 극복했다. 환율 급등기에도 원달러 환율은 위기를 겪은 타국에 비해 상대적으로 덜 오른 편이었다. 대한민국을 포함해 자국의 통화가치가 안정적인 선진국에서는 비트코인 같은 암호화폐를 보유해야할 유인이 크지 않다.

흥미로운 점은 지난 몇 년간 자국의 통화가치가 급격하게 하락한 국가에서 비트코인 수요가 급격하게 상승했다는 것이다. 비트코인 거래량과 가격이 동시에 상승하기 시작한 시점은 2013년 키프로스 사태가 발생한 해였다. 세계 곳곳에 지정학적 위험이 도사리고 있고 정치적·경제적 갈등이 우려되는 국가들도 있다. 글로벌 금융시장에 불안한 이벤트가 발생할 때마다 암호화폐에 대한 수요는 강해질 가능성이 높다.

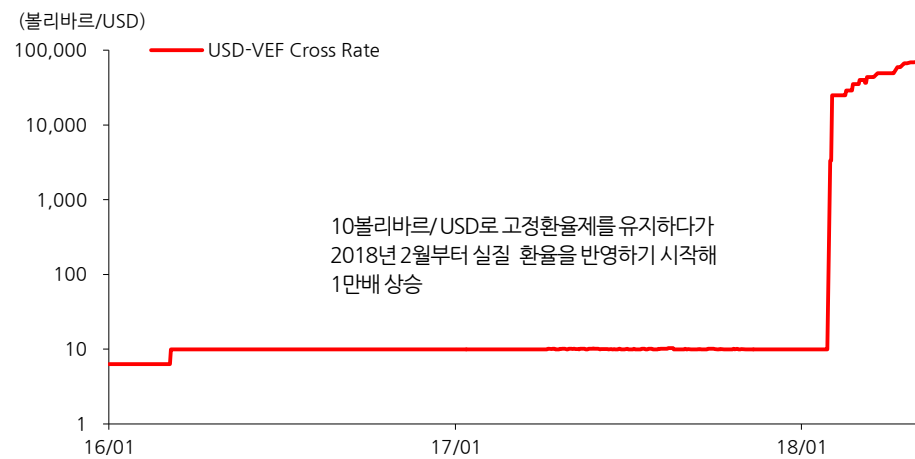
실제로 하이퍼인플레이션을 겪은 짐바브웨나 베네주엘라처럼 자국의 통화가치가 급락하거나 정치적 불확실성이 높은 국가에서 비트코인에 대한 선호도가 매우 높았다고 알려져 있다. 이들 국가의 상황을 보면 통화가치에 대한 헛징 차원에서 비트코인을 화폐가 아니라 디지털 금으로 봐야 한다는 주장도 일리가 있어 보인다.

[그림35] 짐바브웨 100 조 달러 지폐



자료: 한화투자증권

[그림36] 베네주엘라 환율 급등 (로그 스케일)



자료: Bloomberg, 한화투자증권

비트코인은 금과 마찬가지로 채굴량이 한정되어 있다. 특정 국가의 화폐가치가 크게 훼손되거나 은행에서 예금을 인출할 수 없을 때, 전쟁 같은 극단적인 상황이 벌어졌을 때 비트코인은 인터넷이 연결되는 세계 어느 곳에서도 접근 가능한 일종의 안전자산 기능을 할 수 있다. 물론 엄청난 가격변동성으로 인해 비트코인이 자산으로서 가치 저장 수단일 수 있는가에 대한 논란은 지속되고 있지만 안전하게 보관할 수 있다는 것만으로도 그 의미가 있다. 전쟁이 났을 때 금을 들고 피난하다 빼앗길 확률이 블록체인 장부에 기록된 비트코인을 빼앗길 가능성보다 높지 않을까?

사토시 나카모토가 비트코인 백서를 공개한 시점은 2008년 9월 리먼브라더스 파산 직후였다. 소수의 중앙은행이 통제하는 금융 시스템에 대한 불신으로 탈중앙화된 암호화폐를 만든 것으로 해석된다. 금융위기가 발생한 지 올해로 10년 차다. 전세계 통화량은 급증했고 경기는 회복되고 있다지만 세계 곳곳에서 빈부 격차는 심화되었다. 정부가 신뢰를 상실한 일부 국가에서는 법정화폐가 휴지보다 못하다.

경제가 안정되어 있는 국가일수록 비트코인을 불필요하다고 생각할 수 있는 반면에 경제가 불안정하고 환율 변동이 심한 국가, 정부 정책과 중앙은행의 신뢰가 낮은 국가에서는 비트코인을 선호하고 있다.

대다수의 주류 경제학자나 오랜 투자의 대가들이 대체로 비트코인에 회의적인 반면 엔지니어 출신 중에는 비트코인의 잠재력을 긍정적으로 평가하는 사람들이 많다. 지난해 10월, 애플의 공동창업자였던 스티브 워즈니악(Steve Gary Woz Wozniak)은 한 컨퍼런스에서 비트코인에 대해 긍정적 입장을 밝혔다. 워즈니악은 '비트코인이 금보다 가치 있다고 생각한다'며 비트코인이 극심한 가격 안정성 때문에 비판 받고 있지만 미국 달러와 같은 정부 발행 통화보다 안정적이라고 설명했다. 그는 또한 이더리움 같은 스마트 컨트랙트 플랫폼에 대해 깊은 관심을 표명하며 상상할 수 없었던 수많은 소프트웨어 프로그램의 발전이 이뤄질 것이라고 말했다.

페이팔의 창업자인 피터 틸도 비트코인에 대해 긍정적으로 언급했다. 그는 사우디아라비아에서 열린 한 포럼에서 비트코인이 사이버 금에 그친다고 할지라도 엄청난 잠재력이 있으며 사람들이 비트코인을 과소평가하고 있다고 강조했다. 빌게이츠는 비트코인에 대해 직접적으로 언급을 하지 않았지만 비트코인을 만들어낸 블록체인 기술에 대해 찬사를 보낸 바 있다.

수많은 저명 인사들이 비트코인에 대해 각기 다른 의견을 밝히고 있다. 자, 다시 질문으로 돌아와보자. 비트코인은 미래의 화폐가 될 수 있을까?

비트코인이 법정화폐를 대체할 가능성은 희박해 보인다. 비트코인은 중앙은행이나 금융회사의 개입 없이 발행과 거래가 이뤄져 거래시간과 비용을 획기적으로 낮출 수 있다는 점이 긍정적이다. 그러나 법정화폐를 대체하기에는 가격 변동성이 지나치게 높은데다 시간 당 처리할 수 있는 거래건수도 제한돼 화폐 거래를 대체할 수는 없다. 하지만 화폐가 될 수 없다고 해서 가치가 없는 것은 아니다. 필자는 화폐나 아니냐의 논란보다 비트코인을 비롯한 암호화폐가 경제적 가치를 가질 수 있다는 점에 주목해야 한다고 생각한다. 디지털 경제의 시대에 암호화폐는 새로운 자산으로 등장하고 있다.

3. 디지털 경제의 시대, 새로운 자산으로 등장하는 크립토 에셋

<p>밀레니얼 세대의 비트코인 선호</p>	<p>지난 해 미국의 벤처캐피탈 업체인 ‘블록체인캐피탈’이 18세 이상 미국인 2,000명을 대상으로 실시한 설문에서 18~34세 응답자의 30%는 국채 혹은 주식보다 비트코인에 투자하겠다고 답했다. 밀레니얼 세대 중 비트코인에 대해 알고 있다는 비중은 42%에 달했다. 반면 65세 이상 응답자 중에서 비트코인이 익숙하다고 답한 경우는 15%, 실제 비트코인을 보유하고 있다고 응답한 비중은 2%에 불과했다.</p>
<p>디지털 네이티브</p>	<p>최근 암호화폐에 대한 반응을 보면 젊은 층으로 내려갈수록 관심도가 높다. 이들은 기술에 대한 이해도 빠르다. ‘디지털 네이티브(Digital Natives)’라고도 불리는 밀레니얼 세대는 SNS와 게임, 쇼핑 등 인터넷을 사용하는 시간이 길고 용도가 다양하다. 이들은 현실 세계와 디지털 세계를 거의 동시에 살고 있다고 할 만큼 디지털에 친숙하다.</p> <p>디지털 네이티브는 미국의 교육학자인 마크 프렌스키(Marc Prensky)가 2001년 그의 논문 ‘Digital Native, Digital Immigrants’를 통해 처음 사용한 용어다. 프렌스키는 디지털 환경이 구축된 시대에 출생하여 각종 디지털 미디어를 접하면서 성장한 세대를 디지털 네이티브(Digital Natives)로, 기성세대를 디지털 이주민(Digital Immigrants)으로 분류했다. 그리고 이 두 집단은 사회, 환경의 전반에 걸친 급격한 변화를 수용하는 자세가 다른 만큼 서로 다른 성향을 보인다고 주장했다.</p> <p>디지털 네이티브는 각종 정보를 실시간으로 주고받으며, 병렬처리와 멀티 태스킹을 선호한다. 텍스트 정보보다는 그림, 영상, 소리 등의 복합적인 멀티정보를 좋아한다. 또 삶 전체에 네트워크가 자리 잡고 있어 상호작용적인 평가에 즉각적으로 반응한다.</p>
<p>스마트폰 사용시간</p>	<p>자녀들이 공부는 하지 않고 휴대폰만 붙들고 있거나 게임만 한다고 걱정하는 부모들이 많다. 와이즈 앱에 따르면 10대는 하루 평균 3시간 43분, 20대는 4시간 24분, 30대는 4시간 4분간 스마트폰을 사용하고 있다고 한다. 수면시간을 제외하고 하루의 1/4 이상을 스마트폰과 함께 보내고 있으니 걱정할 만도 하다. 그런데 우리 아이만 스마트폰에 빠져있는 것이 아니라 세대의 특성이라면 시대가 변했다고 봐야 하는 건 아닐까?</p>
<p>게임에 친숙한 세대</p>	<p>디지털 네이티브는 기성 세대가 생각하는 것보다 훨씬 더 게임에 친숙하다. 2017년 게임 이용자 실태조사 보고서에 따르면 10대의 87.9%, 20대의 85.2%가 게임을 이용하고 있다고 응답했다. 40대 이상과 상당한 차이가 있음을 알 수 있다. 10~30대는 평균 게임 시간도 길다. 20대는 주말 평균 184분, 3시간 이상 게임을 하는 것으로 나타났다.</p> <p>게임을 하고 SNS를 하는 데 시간만 많이 들이는 것이 아니다. 시간을 많이 들인다는 것은 그만큼 삶에서 차지하는 비중이 높다는 뜻이며 게임과 SNS에서의 내 존재가 중요해졌다는 뜻이기도 하다.</p>

2018년 2월, 블룸버그에 ‘의류의 죽음(The Death of Clothing)’이라는 기사가 보도됐다. H&M 같은 저가 패스트 의류 기업이 시장을 잠식하면서 옷 가격은 지속해서 하락했는데 이들과 성장 한계에 부딪혔다고 한다. 처음에는 아마존 등 온라인 커머스 영향이라고 해석했는데 실은 다른 요인도 가세하고 있다는 것이다. 바로 밀레니얼 세대의 선호도 변화다.

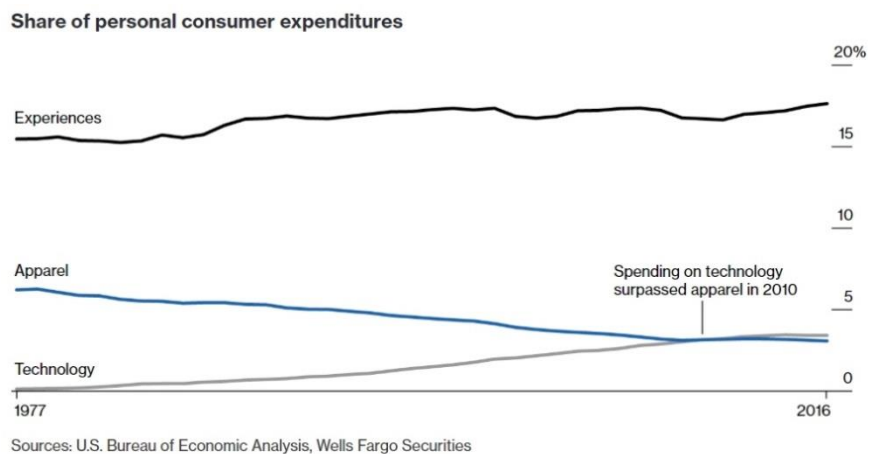
정체성을 표현하는
방식의 변화

밀레니얼 세대는 옷이나 운동화를 사는 것보다 데이터 요금이나 미디어 콘텐츠 같은 디지털을 더 선호하고 소유보다 경험에 소비하는 비중이 높아지고 있다는 것이다. 옷을 사더라도 유명인의 TV 광고를 보고 구매하기보다 인스타그램 스타가 입은 옷을 산다고 한다. 이전에는 아베크롬비, 나이키 같은 유명브랜드의 옷으로 정체성(Identity)를 표현했다면 지금은 브랜드나 가격보다 소셜 네트워크의 팔로워 숫자가 더 중요해진 것이다.

페이스북, 트위터, 인스타그램 같은 SNS를 많이 사용하지 않는 기성세대는 이해하기 어려울 것이다. 2018년 1월, 호주 오픈 테니스 대회에서 한국 선수 최초로 메이저 대회 4강이라는 신화를 보여준 정현의 인스타그램이 화제가 됐다. 정현 선수는 메달도 중요하지만 인스타그램 팔로워 10만명 달성이 마음속에 진짜 목표였다고 했다. 그리고 ‘진짜 목표’를 달성해서 ‘너무너무 행복하다’고 덧붙였다.

SNS와 친숙하지 않은 세대에게는 이해할 수 없는 일이었을테지만 젊은 세대는 정현 선수가 정말 기쁜 것 같으며 공감을 표현했다. 디지털 네이티브 세대에게 SNS 세상에서의 인기와 계급은 이미 새로운 욕망의 대상이 되어가고 있고, 디지털 세상은 비단 게임이나 SNS뿐 아니라 점점 영역을 확장해 가고 있다.

[그림37] 개인 소비 비중 변화: 테크 소비가 의류 소비를 앞질렀다



자료: Bloomberg, 2018년 2월, 'The Death of Clothing', 한화투자증권

4. 밀레니얼 세대는 게임같은 금융상품을 원한다

게이미피케이션	디지털 네이티브인 밀레니얼 세대의 등장과 함께 게이미피케이션(Gamification) 즉 게임화 라는 단어도 널리 퍼져가고 있다. 모든 것이 게임화 되고 있다는 얘기도 흔히 들을 수 있는데 게임에서의 경쟁심리나 보상심리를 활용해 교육이나 상업에 활용하는 비즈니스가 늘어나고 있다.
스타벅스 리워드 시스템	대표적으로 스타벅스 리워드 시스템이 있다. 스타벅스 카드로 음료를 구입하면 스타벅스 앱에 별을 적립 할 수 있는데 일정 갯수 이상을 모으면 무료 음료쿠폰뿐만 아니라 상위 레벨로 승격된다. 게임에서 아이템을 모아 레벨을 올리는 것과 유사하다. 별을 모아 골드회원이 되고자 일부러 스타벅스에 갈만큼 성공적인 마케팅으로 평가받는다. 스타벅스는 일찍이 디지털에 투자했다. 이미 2016년에 스타벅스 선불카드 잔액은 12억 달러를 넘어섰다고 보도된 바 있다. 이자도 주지 않는 선불카드에 12억 달러라는 현금이 보관되어 있는 것이다. 이 때문에 스타벅스 선불카드가 은행에 라이벌이 될 수 있다는 얘기도 나온 지 오래다.
금융에도 게임 같은 요소가 필요	세계 최대 자산 운용사 블랙록(BlackRock)의 창립자 롭 카피토는 밀레니얼 세대들이 대부분의 서비스에서 게임같은 요소를 찾는다며 금융업계도 이에 맞춘 투자 상품을 개발해야 할 것이라고 말했다. 카피토는 우버를 즐겨 쓰는 젊은층은 앱을 통해 본인이 선택한 차량이 실시간 이동하는 모습을 보는 것에서도 재미를 느낀다며 단순히 편리해서라기보다 게임적인 요소가 들어 있기 때문이라고 설명했다.
암호 자산(Crypto Asset)	인스타그램 팔로워수나 스타벅스의 골드회원, 게임에서의 아이템과 계급은 디지털 네이티브 세대에게 꽤 강력한 참여 동기를 유발한다. 동일한 목적을 공유하는 블록체인 네트워크 상에서 암호화폐는 마찬가지로 사용될 수 있다. 게임 아이템이 게임 이용자 사이에서 가치가 있고 스타벅스 별 모으기 역시 가치가 있듯 암호화폐는 블록체인 커뮤니티 내에서 사용하고 저장할 수 있는 암호자산(Crypto Asset)이 될 가능성이 있다.
디지털 콘텐츠 산업	게임 아이템은 법정화폐로 거래된 지 오래된 디지털 자산이다. 물론 아이템 거래를 불법으로 보는 국가도 있고 자산으로 볼 수 있는가에 대해서도 여전히 논란이 많다. 법적으로 또는 회계적으로 자산인가 아닌가의 논쟁의 결론을 내리자는 것은 아니다. 이를 자산으로 여기는 사람들이 디지털 네이티브 세대를 중심으로 늘어나고 있다. 게임 사용자는 시간과 노력을 들여 아이템을 획득할 것인지, 아니면 아이템을 구매해서 즐길 것인지 선택할 수 있다. 돈을 주고 아이템을 구매해본 젊은층이 암호화폐 거래에 거부감이 별로 없다. 디지털 네이티브 세대의 성장과 함께 게임 등 디지털콘텐츠 산업은 블록체인으로 인한 변화 가능성이 엿보이는 산업이다. 이와 함께 자산 시장에서도 크립토 에셋(Crypto Asset)이 새로운 자산으로 자리잡아 갈 가능성이 엿보인다.

5. 디지털 트랜스포메이션, 그리고 디지털 경제의 확장

인류는 농업 경제에서 산업 경제로, 그리고 이제는 디지털 경제로 넘어가고 있다. 정보 통신-인터넷 기술의 발달로 전 세계 사람들이 디지털 경제에서 소통한다.

데이터가 자원인 시대

몇 년 전부터 외신에서는 ‘Data is the new oil of the digital economy.’라는 문장이 심심치 않게 나왔다. 디지털 경제에서는 정보와 지적 산출물, 데이터의 가치가 중요하다. FANG(Facebook, Amazon, Netflix, Google)이나 BAT(Baidu, Alibaba, Tencent)같은 거대 공룡기업들은 우리가 끊임없이 입력하는 데이터를 먹고 자랐다. 많은 사용자 데이터를 확보해 잘 해석하는 기업들이 산업의 경계를 넘어 시장을 정복해가고 있다.

소수의 기업이 수혜를 독식

디지털 경제가 빠르게 커지고 있는데 그 수혜를 누리는 기업은 소수의 공룡 기업이다. 석유가 발견되었을 때, 에너지 기업들이 독과점화되어 성장하던 것과 유사하다. 데이터라는 자원을 소수의 기업이 빠르게 흡수하면서 독보적인 성장세를 보이고 있는 것이다.

그런데 이들을 강하게 만들고 있는 데이터는 다름 아닌 우리가 제공한다. 사용자가 데이터를 입력해주고 공유해주지 않았더라면 이토록 빠르게 시장을 잠식할 수 없었을 것이다. 데이터가 새로운 자원임에도 불구하고 그들은 땀가름 지拂하지 않는다. 24시간 휴대하는 스마트폰을 통해 얼마나 많은 개인 정보들을 가져가고 있는지, 어떤 용도로 활용되고 있는지 불안감은 사용자 몫이다.

디지털 경제의 확장

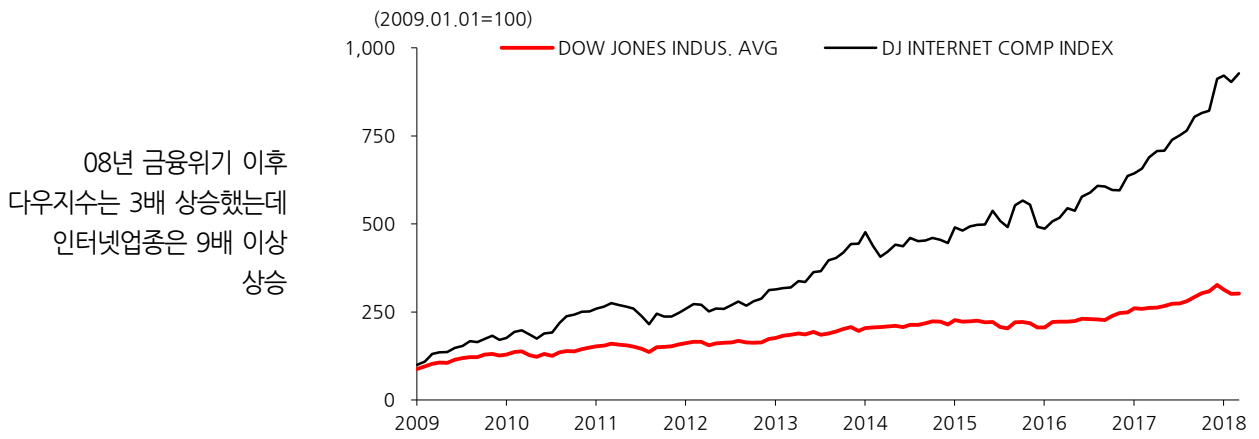
밀레니얼 세대가 아니더라도 오늘날 사람들은 점점 더 많이 디지털로 생산하고 소비한다. 개인, 기업, 정부 할 것 없이 거의 모든 영역에서 디지털 트랜스포메이션을 외치고 있다. 이대로라면 인터넷 공룡기업의 데이터 독과점은 심화될 것이다. 이미 수많은 기업들이 아마존 AWS클라우드 서비스에 정보를 저장하고 있다.

지난 수백년간 실물경제에서 쌓인 정보가 디지털화 될수록 디지털 경제의 규모는 어마어마하게 커질 것이다. 지금은 인터넷 검색이나 SNS, 게임 정도를 디지털 경제로 본다면 앞으로는 실물경제의 산업들이 디지털화 되면서 실물경제와 디지털 경제의 경계가 무너질 것이다. 과도한 상상이라고 생각하는가? 이미 사무직 업무의 대부분은 디지털로 바뀌었다. 대부분의 업무가 데이터로 남는다. 앞으로 더 많은 영역이 디지털 경제로 흡수될 것임은 자명하다.

블록체인 기술은 데이터 독과점에 대항하는데 유용하게 쓰일 수 있다. 데이터라는 자원을 생산자가 직접 관리하고 그 가치를 교환할 수 있게 할 때 비로소 인터넷 초기부터 추구했던 정보의 민주화를 이룰 수 있을 것이다.

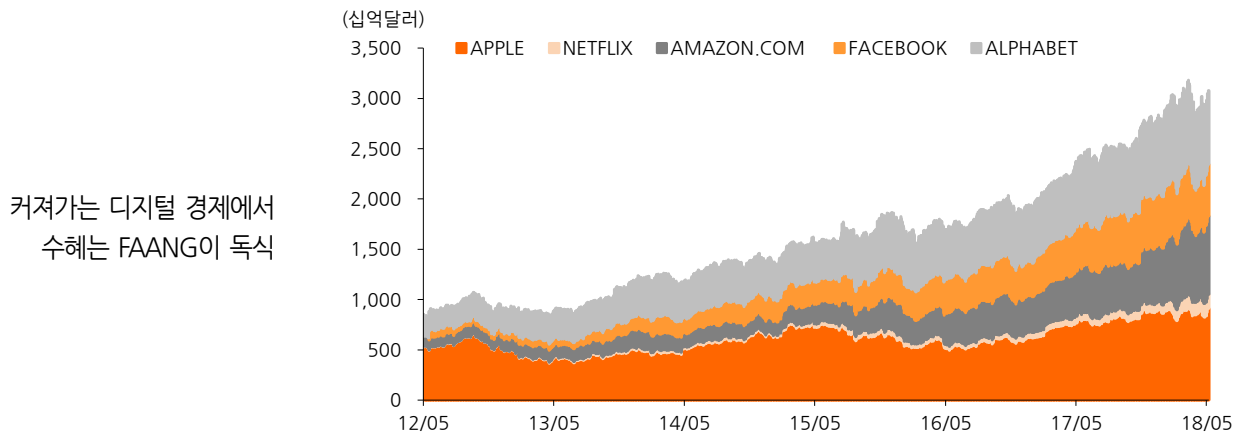
정부의 규제로 암호화폐를 법정화폐와 교환하거나 실물을 구매하는 것이 불가능해질 수 있다. 하지만 암호화폐는 디지털 경제 내에서만 가치를 갖게 된다 해도 디지털 자산으로 존재할 가능성이 충분해 보인다.

[그림38] 다우지수와 다우인터넷 업종지수 추이



자료: Bloomberg, 한화투자증권

[그림39] FAANG 시가총액 합산 추이



자료: Bloomberg, 한화투자증권

6. 비트코인 선물거래 개시, 디지털 금(Gold)이 될 가능성

제도권으로 진입한 비트코인

2017년 12월 10일, 시카고옵션거래소(CBOE: Chicago Board Options Exchange)가 그 리고 18일에는 세계 최대 파생상품 거래소인 미국 시카고 상업거래소(CME: Chicago Mercantile Exchange)가 비트코인을 기초로 하는 선물거래를 개시했다. 비트코인을 기초자산으로 하는 선물 출시를 먼저 발표한 것은 시카고 상업거래소였는데 실제 상품은 시카고옵션거래소가 먼저 출시했다.

CME 그룹에 따르면, 비트코인 선물은 'CME CF 비트코인 레퍼런스 레이트(BRR)'를 기준으로 결정된다. 비트코인 지수인 BRR은 2016년 11월 CME와 영국 런던의 디지털 화폐 거래소인 크립토퍼실리티즈가 공동으로 만든 지수다.

CME 그룹은 디지털 자산을 거래하고자 하는 수요가 꾸준히 증가함에 따라 비트코인 선물 출시를 결정했다고 밝혔다. 비트코인 선물거래는 비트코인이 비로소 제도권 금융 시장에 진입한다는 의미에서 기념비적 이벤트라고 볼 수 있다. 당시 CME는 홈페이지에 비트코인을 금, 법정화폐와 비교해 설명하는 글을 게시했다. (이 글을 쓰고 있는 현재, CME 홈페이지에서는 해당 글을 찾을 수 없다.)

[표3] CME 그룹의 비트코인 선물상품 개요

계약 단위	CME CF 비트코인 레퍼런스 레이트(BRR)의 정의에 따른 5 비트코인
최소호가변동폭	아웃라이트: 비트코인 당 \$5.00 = 계약 당 \$25.00 캘린더 스프레드 거래 및 BTIC 거래: 비트코인 당 \$1.00 = 계약 당 \$5.00
거래 시간	CME Globex 및 CME ClearPort: 일요일 - 금요일 오후 5:00 - 오후 4:00 * 미국 중부시간 기준
상품 코드	아웃라이트: BTC
상장 주기	3월 주기 분기월물(3, 6, 9, 12 월) 중 최근물 2개 및 분기월물이 아닌 연속월물 중 최근물 2개
거래 종료	최종거래일은 계약월의 마지막 금요일임. 만료되는 선물의 거래는 최종 거래일의 런던시간 오후 4:00에 종료됨.
포지션 한도	현물 포지션 한도는 1,000 계약임. 전체월물 합산 포지션 또는 현물월이 아닌 어느 단일 월물에의 포지션이 5,000 계약 이상시 포지션설명의무가 적용됨. 보고 대상 기준은 25 계약임.
대량매매 최소수량요건	5계약.
가격제한폭	영업일 당 가격제한폭은 매 영업일의 런던시간 오후 4:00에 결제되는 가장 최근의 비트코인 선물 결제가격을 기준으로 설정됨. 특별 가격변동폭 제한은 직전 결제가격의 상하 7%, 직전 결제가격의 상하 13%, 직전 결제가격의 상하 20%임. 직전결제가격의 상하 20%를 벗어나는 가격에의 거래는 허용되지 않음.
최종결제	최종 거래일의 CME CF 비트코인 레퍼런스 레이트(BRR)과 같은 가격인 최종결제가격에 의거하여 현금결제됨.

자료: CME, 한화투자증권

몇 가지 인상적이었던 부분을 정리해보면 다음과 같다. 금과 비트코인은 총량이 한정되어 있고 가격이 올라갈수록 채굴경쟁이 심화된다. 경쟁이 심화되면 원가인하 시도가 강해지는데 이것이 선형으로 나타나는 것이 아니라 정체를 겪는다. CME는 이를 천연가스 공급에 비유했다. 천연가스 가격이 상승하면 투자가 증가하지만 천연가스의 실질적인 공급이 증가하기까지는 시간이 필요하기 때문에 공급 부족 기간을 겪는다는 것이다. 시차를 두고 공급을 증가시키는데 성공하면 한동안 가격은 정체된다.

비트코인의 가격 변동성이 높기는 하지만 투자자들은 과거에 유사한 수준의 변동성을 보였던 자산에 여전히 투자하고 있다. 미국 주식시장은 1929년에서 1933년 사이에 89%의 하락을 경험했고 1954년에야 회복했다. 이후에도 1973년과 1974년 사이 47% 하락, 2000년부터 2002년 사이 50% 하락, 2007년 10월부터 2009년 3월까지 약 60%의 하락을 경험한 바 있다. 원유 가격은 2008년 최고치 대비 67% 하락한 바 있다. 단, 비트코인과 주가지수, 원유 가격 사이에는 중요한 차이가 있는데 주가지수와 원유는 모두 위험자산임을 투자자들이 충분히 인지하고 있다는 점이다.

법정화폐는 가치의 저장보다는 교환의 매개 수단으로서 금보다 실용적이다. 재화나 서비스 구매로 소비하지 않으면 법정화폐의 가치는 인플레이션만큼 하락하기 때문에 소비할 유인이 있다. 반면 금이나 비트코인은 교환의 매개 수단보다는 가치의 저장으로서의 기능이 좀더 우수하고 가치의 척도나 지불 용도로는 미흡하다고 볼 수 있다.

필자의 주관적인 견해를 밝히자면 비트코인은 화폐라고 볼 수 없으며 가격이 안정적인 안전자산이라고 보기는 어렵지만 변동성이 큰 투자자산으로서 가치가 있다고 생각한다.

[그림40] 통화가치 저하의 역사적 사례

Country, Currency	Period Covered	Cumulative Decline in Silver Content	Largest Debasement	Year
Austria, kreuzer	1371-1499	-69.7%	-11.1%	1463
	1500-1799	-59.7%	-12.5%	1694
Belgium, hoet	1349-1499	-83.8%	-34.7%	1498
	1500-1789	-56.3%	-15.0%	1561
France, livre tournois	1258-1499	-74.1%	-56.8%	1303
	1500-1789	-78.4%	-36.2%	1718
Germany				
Bavaria, pfennig	1417-1499	-32.2%	-21.5%	1424
	1500-1799	-70.9%	-26.0%	1685
Frankfurt, pfennig	1350-1499	-14.4%	-10.5%	1404
	1500-1789	-12.8%	-16.4%	1500
Italy, lira fiorentina	1280-1499	-72.4%	-21.0%	1320
	1500-1799	-35.6%	-10.0%	1550
Netherlands, guilder	1450-1499	-42.0%	-34.7%	1496
	1500-1799	-48.9%	-15.0%	1560
Russia, ruble	1761-1799	-42.3%	-14.3%	1798
Spain, maravedis	1501-1799	-62.5%	-25.3%	1642
Sweden, mark ortug	1523-1573	-91.0%	-41.4%	1572
United Kingdom, pence	1260-1499	-46.8%	-20.0%	1464
	1500-1799	-35.5%	-50.0%	1551

Source: *This Time Is Different*, Rienhart and Rogoff, page 176, Princeton University Press, 2009

자료: NASDAQ, 한화투자증권

VIII. 크립토 버블에 대한 생각

1. 톨립버블, 닷컴버블과 비교한 암호화폐 버블

- 버블과 폭락

자산 가격이 펀더멘털 가치(fundamental value)를 초과할 때 우리는 버블이라고 말한다. 로버트 실러 교수는 불합리한 기대가 증만할 때, 자산 가격은 합리적으로 추정한 펀더멘털 가치를 넘어서 수 있는데 이는 중국에 급격한 가격 폭락을 초래할 수 밖에 없다고 주장했다. 버블이란 어느 누구도 버블이라고 선형적으로 규명할 수 없는 것을 의미한다고도 말했다.
- 크립토 버블은 닷컴버블과 유사

지난해 암호화폐 가격 폭등은 가히 ‘크립토 버블’이라 부를 만 했다. 필자는 크립토 버블이 톨립버블보다는 닷컴버블에 가깝다고 생각한다. 톨립은 인류 삶에 변화를 불러오지 못했지만 닷컴버블 이후 생존한 기업들은 실제 세상을 바꾸고 있다.
- 17세기 톨립버블

17세기 네덜란드에서 일어난 톨립버블은 역사적으로 손꼽히는 버블이다. 당시 경기 호황과 동인도회사 투자 열기가 불면서 톨립 투기가 발생했다. 톨립 구근 가격이 오를수록 더 희귀한 최고급 톨립 품종을 개량하려는 사람들이 늘어났고 아직 꽃이 피기도 전에 미래 어느 시점에 매매한다는 계약을 사고파는 선물거래까지 등장했다. 톨립 가격은 폭등했다가 어느 순간 급락했다. 더 높은 가격에 톨립을 사겠다는 사람이 사라지는 순간 가격은 빠르게 제자리로 돌아갔고 돌이킬 수 없는 손실을 남겼다.
- 1990년대 닷컴버블

1990년대 후반 닷컴버블 역시 매우 뜨거웠다. 당시 인터넷 사업을 정관에 넣으면 실제 아무런 사업을 시작하지도 않았는데 주가만 올랐다는 얘기가 있을 정도다. 1996년 상장한 야후 주가는 2000년 초 주당 240 달러까지 상승했다가 1년만에 30달러로 하락했다. 기업의 내재 가치를 크게 초과한 버블은 결국 터지고야 말았다.

[그림41] 역사적인 자산 버블



자료: The Economist, 한화투자증권

사명 변경 지난해에는 블록체인과 관련해 유사한 현상이 일어났다. 미국 나스닥(NASDAQ)에 상장된 무알콜 음료 회사 ‘롱 아일랜드 아이스 티 (Long Island Iced Tea Corporation)’사가 사명을 ‘Long Blockchain Corporation’으로 변경하자 주가가 세배로 뛰었다. ‘바이오틱스’라는 이름의 바이오테크 회사도 ‘라이엇 블록체인(Riot Blockchain)’으로 사명을 바꾸고 블록체인 산업 진출을 발표했다. 라이엇 주가는 네다섯배 가량 올랐다가 다시 제자리로 돌아갔다.

미국 증권거래위원회(SEC)는 롱 블록체인에게 상장폐지 처분을 내렸다. 롱 블록체인사가 블록체인 기술에 대한 일반 투자자들의 관심을 이용해 이익을 취한 것으로 보인다는 것이다. 라이엇 블록체인에 대해서도 소환조사를 했다. 두 회사 모두 블록체인과는 전혀 관련없는 사업을 영위하던 중 블록체인이 인기를 얻자 시류에 편승해 사명 변경으로 주가를 띄웠다는 의혹을 샀다.

그렇다면 블록체인은 새로운 버블의 역사로 사라지게 될 것인가? 판단하기 이르지만 그렇지 않을 가능성이 높다고 생각한다. 1994년 설립된 아마존은 90년대 후반 닷컴 버블 당시 주목받던 회사였다. 닷컴 버블 붕괴 후 고전했으나 이후 꾸준히 성장해 20년이 지난 오늘 날 공룡 기업이 되어 세계를 먹여 삼키고 있다.

버블은 지나고 가야 버블인지 판단할 수 있을테니 블록체인도 버블인지 아닌지 알 수 없다. 하지만 기술은 발전하고 있고 새로운 비즈니스가 나타나고 있다. 문제는 우리에게 새로운 아마존을 찾을 수 있는 안목이 있느냐다. 아마존도 닷컴버블 당시 무수히 많은 주식 중 하나였고 온라인 서점의 벨류에이션이 지나치게 비싸다는 평가를 받았다.

지난 해 한창 암호화폐 투자 열기가 뜨거울 때, 국내 증시에서도 블록체인 신사업에 진출한다거나 ICO를 추진한다는 보도로 주가가 움직이는 일이 종종 발생했다. 어떤 주식에 투자해야 하느냐는 질문도 많이 받았다. 하지만 지금은 블록체인 산업의 도입기다. 누가 진정한 승자가 될 지 예측하기에 앞서 기술의 변화 방향과 이를 통해 변화할 세상에 대한 고민이 필요한 시점이다. 변화 방향을 따라가다보면 전혀 의외의 곳에서 비즈니스 아이디어나 투자 기회를 찾을 수 있을 것이다. 지금 우리에게 필요한 것은 상상력과 열린 토론이다.

[그림42] Riot Blockchain 주가 추이



자료: Yahoo Finance, 한화투자증권

[그림43] 1999년 닷컴 버블 당시 아마존 주가



자료: Yahoo Finance, 한화투자증권

[그림44] 지난 20년간 아마존 주가



자료: Yahoo Finance, 한화투자증권

2. ICO 참여 전 생각해볼 질문들

지난 해 암호화폐 투자 열기는 뜨거웠다. 누가 코인에 투자해서 강남 아파트를 샀더라 또는 회사를 그만뒀다더라는 얘기가 떠돌았다. 정부는 코스닥 벤처기업 활성화를 외쳤지만 열매, 스무배의 수익률을 구경한 사람들에게 상장 주식의 기대수익률은 너무 낮게 느껴졌을 것이다. 사촌이 돈을 벌었다 하니 너도나도 암호화폐에 뛰어든 것이 바로 작년 하반기였다.

정부는 거래소 폐쇄라는 업포를 놓았지만 거래소 감사와 실명제 도입으로 신규자금 유입을 한동안 차단했다. 우연인지 한국 정부의 규제 강화와 함께 암호화폐 시장은 매우 빠른 속도로 하락했다. 정부를 탓하는 사람들도 있었지만 어찌보면 한국정부의 경고 덕에 큰 손실을 피할 수 있었다며 안도하는 사람들도 많았다. 폭락의 근본 원인은 그만큼 비이성적인 과열이 존재 했다는 뜻이기도 하다.

암호화폐 투자 열풍과 함께 2017년은 ICO의 해였다. 이더리움 같은 플랫폼 프로토콜에서 쓰이는 암호화폐를 코인이라고 한다면 특정 용도의 스마트 계약에 쓰이는 암호화폐를 토큰이라 구분한다. 작년에는 이더리움 이외에 새로운 프로토콜 코인들이 나오면서 각 프로토콜 안에 구현하겠다는 다양한 종류의 토큰 ICO가 인기를 끌었다.

이미 크게 상승한 비트코인과 이더리움을 새로운 토큰으로 교환해 추가 수익을 꿈꾸는 사람들이 ICO 시장에 몰려들었다. ICO 시장이 과열되는 양상을 보이자 사기성 코인도 늘어났다. 블록체인 기술과 무관한 토큰 발행이 이어졌고 실현 가능성이 희박해 보이는 프로젝트도 많아졌다.

올해 초 암호화폐 시장이 폭락한 후, 올해 ICO 시장이 다소 위축될 것이라고 예상했다. 그런데 이 글을 쓰고 있는 5월 현재에도 ICO 시장의 열기는 식지 않고 있다. 물론 새로운 종류의 코인이 워낙 많아지다 보니 ICO라고 해서 무조건 성공하는 것은 아니며 실패하는 프로젝트도 그만큼 많다. 하지만 여전히 ICO 시장으로 유입되는 자금 규모는 전년 못지 않다.

[그림45] 2017년 1월부터 2018년 3월까지 월별 ICO 추이

Disclosed funding of completed ICOs. January 2017 - March 2018



자료: CBInsights, 한화투자증권

ICO에 참여하기 전, 먼저 토큰의 정체에 대해 고민해보자.

미국 증권거래위원회(SEC)와 스위스 금융위원회(FINMA)는 토큰 중 증권, 즉 주식의 성격을 가진 토큰에 대해 증권과 유사한 수준의 규제 및 감독 대상이라고 밝혔다. 개념적으로 비유하자면 토큰은 일반적으로 유통되는 화폐와는 다르다. 증권형 토큰(Security Token)의 경우 주식과 유사하고 유틸리티 토큰은 이용권, 상품권에 가깝다. 주식과 상품권의 기능이 섞인 회원권 같은 토큰도 있다.

토큰은 토큰으로 자리잡게 될 것	암호화폐, 크립토에셋은 역사가 짧고 블록체인 업계에서조차 아직 명확하게 정의하지 못한 상태다. 필자는 이것이 주식이 처음 발행되었던 시기의 상황과 유사하다고 생각한다. 크립토에셋의 종류가 다양해지고 성격이 좀더 명확해지면 토큰은 토큰으로 자리잡게 될 것이다. 주식도 처음에는 화폐도 아니고 증서도 아닌 장부 거래였다.
최초의 주식거래와 유사한 암호화폐 거래	최초의 주식회사는 1602년 네덜란드에 설립된 네덜란드동인도회사(VOC)였는데 당시에는 주식 증권이란 개념이 없었다. 주주들의 이름과 지분을 기록한 장부가 있었을 뿐이다. 주식의 소유권을 이전할 때도 종이로 된 증서를 주고받는 게 아니라 회계 담당자가 가지고 있는 장부를 고치는 식으로 이뤄졌다고 한다.

블록체인 장부에 잔액을 고쳐쓰며 거래하는 암호화폐 거래와 유사하지 않은가? 최초의 주식 거래는 물리적인 장부에 사람이 수기로 기록했다면 암호화폐 거래는 디지털 장부에 컴퓨터로 기록한다. 네덜란드동인도회사의 주가가 폭등하자 17세기 네덜란드에서는 여기저기서 유사한 회사가 설립되고 묻지마 투자가 일어나 버블을 겪었다고 하는데 지난 해 암호화폐 시장의 상황도 비슷했던 것 같다. 이후 주식이란 무엇인지, 가치는 어떻게 평가해야 하는지 본격적인 연구 결과가 나온 건 한참 후였다. 암호화폐란 무엇인지, 토큰의 가치 평가는 어떻게 해야 하는지 본격적인 연구 결과가 나오려면 시간이 필요할 것이다.

지금까지의 논의를 기초로 주관적인 견해를 밝히자면, 현재까지 발행된 토큰들은 프로젝트에 참여할 수 있는 투표(Voting) 권한이자 회원권, 사용권이다. ICO 토큰의 가치는 해당 프로젝트 또는 커뮤니티를 사용하는 가치에 수렴할 것이다. 프로젝트가 성공한다면 고급 골프장이나 리조트 회원권처럼 가격이 예상보다 상승할 수 있고 만족스럽게 이용할 수도 있을 것이다. 하지만 아직 구현되지 않은 상태에서 투자했다가 프로젝트가 실패하거나 결과물이 미흡할 경우에는 사용하는 만족도가 낮아지는 것은 물론이며 회원권으로서 토큰의 가치도 하락할 것이다.

투자를 결정하기 전에 해당 코인이 고가의 회원권이나 우량 기업의 비상장 주식인지, 싸이월드의 도토리가 되어 사라질 것인지, 프로젝트의 성공가능성과 사용가치에 대한 판단이 필요하다. 싸이월드의 도토리를 폼하하는 것은 아니다. 싸이월드가 한창 인기를 끌던 시기에 도토리는 생일 선물로도 주고받을 만큼 가치가 있었다. 지금 ICO 시장에서 발행되는 토큰들 역시 마찬가지다. 나중에 가치가 올라갈 지 내려갈 지 알 수 없지만 구매해서 사용해 보는 것으로도 만족할 수 있다면 최소한의 값어치가 있다고 할 수 있다.

ICO 투자 주의사항 지난해부터 대폭 증가한 ICO 프로젝트를 보면서 필자가 했던 고민들과 투자자들이 ICO에 참여하기 전에 생각해보면 좋을 질문들을 정리해 보았다.

첫째, 해당 프로젝트의 비즈니스 모델을 이해해야 한다. 오프라인 비즈니스의 예를 들거나 듣도보도 못한 비즈니스 모델을 설명하며 토큰을 발행하는 경우가 많은데 정작 토큰을 어디에 어떻게 쓴다는 것인지 설명이 부족한 경우가 태반이다. 토큰에 투자한다면 최소한 그 토큰을 사서 어디에 쓸 수 있는지, ICO 단계가 지나가고 실제 프로젝트가 구현되었을 때 토큰이 왜 필요한지에 대해 충분히 이해하고 접근해야 한다.

둘째, 고수익을 보장한다면 무조건 의심하자. 고위험을 동반하지 않은 고수익은 세상에 거의 존재하지 않는다고 봐도 좋다. 모든 투자는 위험과 수익이 비례하거나 위험은 높고 수익은 높지 않는 경우가 흔하다. 게다가 암호화폐 생태계에 ‘보장된 이익’은 어디에도 있을 수 없다. 이익을 보장한다는 프로젝트는 무조건 의심해야 한다.

셋째, 왜 블록체인이어야 하는가에 답을 할 수 있어야 한다. 이미 주식회사로 비즈니스를 영위하고 있는 회사들이 ICO를 하는 것을 ‘리버스 ICO(Reverse ICO)’라고 하는데 이미 보여줄 수 있는 사업이 존재하니 아무 것도 보여주지 못한 ICO보다 안정적이라고 설명하는 것을 보았다. 주식회사가 ICO를 하는 것은 과연 안정적이냐? 반드시 그런 것은 아니다. 왜 ICO를 해야 하는지, 왜 블록체인으로 구현하려 하는지 답할 수 있어야 한다. 게다가 주식회사가 코인을 발행할 경우, 기존 주주와 이해관계 문제가 발생할 수 있으며 주식과 코인이 어떤 차이가 있고 권한과 책임 관계는 어떻게 되는지 구분이 필요하다.

넷째, 모집된 자금을 어디에 어떻게 쓸 것인지 계획을 살펴봐야 한다. 통상 ICO는 법정 화폐가 아닌 비트코인이나 이더리움으로 받고 있는데 모집된 암호화폐를 어디에 어떻게 보관할 지 개발자와 어드바이저에게 언제 어떻게 배분되는지 계획과 절차가 투명해야 한다.

다섯째, ICO의 주체는 누구인지, 재단이라면 어느 나라에 설립되어 있는지 살펴보자. 그리고 프로젝트의 설립자와 개발자, 어드바이저를 구분해서 살펴보자. 최근 ICO 중에는 유명인을 어드바이저로 내세워 홍보를 하는 프로젝트가 많다. 어드바이저는 그 대가로 코인을 받고 홍보활동에 참여한다. 프로젝트를 추진하고 있는 진짜 멤버가 누구인지, 그들의 이력과 과거 평판을 꼼꼼히 살펴볼 필요가 있다. 물론 살펴본다고 해서 다 알 수 있는 것도 아니니 더욱 신중할 필요가 있다.

ICO는 대부분의 국가에서 제도화되어 있지 않은 만큼 모든 책임은 투자자 본인에게 있다. 어느 누구도 수익을 보장해주거나 자산을 지켜줄 수 없다는 것을 명심하고 크라우드펀딩이나 비상장주식의 선별보다 더욱 신중해야 할 것이다.

IX. 블록체인, 과연 세상을 바꿀 기술인가?

1. 잘 돌아가고 있는 기존 인프라를 바꿀 필요는 없다

지난 해 암호화폐 투자 열풍이 불면서 블록체인에 대한 관심도 함께 높아졌다. 스타트업뿐 아니라 상장사와 대기업 그리고 공공기관들도 블록체인 사업을 추진한다는 보도가 심심치 않게 흘러나오고 있다. 블록체인은 잠재력이 엄청난 기술이라고 생각하지만 당장 모두가 뛰어들어야 할 기술인지에 대해서는 냉정하게 되짚어봐야 할 것이다.

이상과 현실 사이	블록체인의 잠재력과 현재 기술 수준 사이에 간극이 크다. 블록체인 관련 컨퍼런스나 포럼에서 자주 듣는 어구는 ‘infancy’, ‘at the early stage’, ‘too young’ 같은 것이다. 비탈릭 부테린조차 2015년에 만들어진 이더리움이 아직 30% 정도밖에 구현되지 않았다고 말했다. 기술 개발 초기에 아무리 잠재력이 뛰어난 기술이라고 해도 당장 효용을 발휘할 수 있는 분야를 찾는다는 것은 쉬운 일이 아니다. 블록체인이 만병통치약이 될 수도 없을 테지만 대단한 잠재력을 가지고 있다고 해도 아직은 개발 초기 단계에 불과하다.
클라우드 컴퓨팅	블록체인이 상용화되기 위해서는 아직 기술적으로 해결해야 할 과제가 많다. 초당 거래 승인 건수를 높여야 하고 거래 수수료는 낮춰야 하며 IPFS(Inter Planetary File System) 등 데이터를 분산해 저장하는 기술도 아직 완벽하지 않다. 인터넷 TCP/IP 프로토콜 같은 표준화가 이뤄지려면 한참 멀었다. 현재의 기술 수준만 놓고 보자면 블록체인보다 클라우드 컴퓨팅이 훨씬 편리한 경우가 많고 클라우드 컴퓨팅도 나날이 발전하고 있다.
기존 인프라를 바꿀 필요는 없다.	우리는 민주주의, 자본주의가 발달한 OECD 선진국에 살고 있다. 대한민국에서는 충분히 신뢰할만한 기관들이 효율적으로 업무를 수행하고 있다. 또한 대한민국은 이미 세계 최고 수준의 정보통신·IT 강국이다. 전자정부 서비스가 잘 갖춰져 있고 모바일 뱅킹, 모바일 쇼핑, 메신저 서비스 등 삶에 필요한 대부분의 서비스가 이미 잘 구현되어 있다.
기존 인프라를 바꿀 필요는 없다.	불편함이 없다면 블록체인 기술을 굳이 도입할 필요가 없다. 중계자나 중앙 집권형 기관을 신뢰할 수 있고 중계자의 역할이 필요하다면 탈중앙화를 위한 블록체인 도입은 더욱 불필요하다. 당연한 얘기임에도 굳이 언급하는 이유는 최근 필자가 만나본 수많은 팀들이 이미 잘 구현된 인프라를 두고도 블록체인으로 개발하겠다고 조언을 구해왔기 때문이다. 블록체인이 없어도 잘 돌아가고 있다면 기존 인프라를 바꿀 필요는 없다.
기존 시스템이 체계적이지 않은 분야	현재 웹 서버/클라이언트 방식과 클라우드 컴퓨팅으로 대부분의 시스템은 아주 효율적으로 구현돼 있다. ‘블록체인을 위한 블록체인 프로젝트’를 추진해서 더 나은 시스템을 구축하기 어렵다.
기존 시스템이 체계적이지 않은 분야	기존 시스템이 이미 잘 돌아가고 있는 분야가 아니라 기존 시스템으로 구현하지 못했던 부분 중에 블록체인을 통해 새로운 가치를 창출할 수 있는지를 고민해 보는 편이 낫다. 예를 들자면 무료로 배포되던 디지털 자산 거래나 사회적 투자, 기부 사업처럼 비용이 발생하고 거래관계가 존재하나 시스템이 체계화 되지 않았던 분야를 먼저 검토해보면 어떨까?

2. 신흥국을 움직일 블록체인

모바일 기기 확산	세계은행에 따르면 세계 약 17억명의 사람들이 은행 계좌를 보유하고 있지 않다. 최근 수년 간 모바일 폰 보급 덕분에 빠른 속도로 줄어든 숫자다. 2011년에는 27억명이 은행 계좌를 보유하고 있지 않았으나 중국, 인도, 그리고 아프리카 신흥국에 모바일 기기가 확산되면서 빠른 속도로 계좌도 개설됐다.
여전히 은행계좌가 없는 신흥국 사람들	저개발 신흥국에서 은행 지점이나 ATM 기계를 설치하려면 물리적으로 시간이 많이 필요하다. 아프리카처럼 도시 인프라가 잘 갖춰지지 않은 지역에서는 더욱 오랜 시간이 걸린다. 그런데 이렇게 오프라인 banking 시스템이 갖춰지지 않은 지역에서 모바일 머니는 빠르게 확산되고 있다. 케냐, 가봉, 수단 등 아프리카 빈국에서는 은행 계좌를 만들기 전에 모바일 머니를 사용하는 사람들이 늘어나는 중이다. 세계은행은 사하라 이남 국가들을 중심으로 모바일 머니의 성장 가능성이 높다고 전망했다. 이 지역에 은행 계좌가 없는 성인 3억 5천만 명 중 1억 5천만 명 이상이 모바일 폰을 보유하고 있다고 한다.
모바일 머니의 확산	모바일 머니가 빠르게 확산된 대표적인 국가는 케냐다. 케냐에는 엠페사(M-Pesa)라는 모바일 결제 시스템이 있다. 엠페사는 현지 통신사인 사파리콤(Safaricom)과 보다폰(Vodafone)의 자회사 보다콤(Vodacom)이 함께 만들어 2007년 서비스를 개시한 후 케냐 전역으로 확산됐다. 현재 알바니아, 콩고, 이집트, 가나, 모잠비크, 탄자니아 등 아프리카에서 약 3천만명 가까이 사용하고 있다.
엠페사	엠페사의 사용 방법은 간단하다. 엠페사 로고가 부착된 동네 상점에 가서 휴대전화 번호와 연결된 계좌를 만들 수 있으며 송금 시에는 상대방 전화번호와 송금액을 누르고 전송하면 된다. 메시지를 받은 사람은 엠페사 로고가 부착된 상점에 가서 해당 메시지와 비밀번호를 제시하면 현금을 받을 수 있다. 은행 시스템이 갖춰지기까지 상당한 시간이 걸릴 것으로 예상됐던 아프리카에서 선진국보다 먼저 모바일 머니가 확산됐다.

[그림46] 2017년 엠페사 10주년 기록



자료: Vodafone, M-Pesa, 한화투자증권

모바일 머니에 익숙해진 아프리카 사람들은 블록체인을 활용한 송금 시스템이나 암호화폐에 대해서도 대체로 거부감이 없다고 한다. 자국 화폐의 가치가 안정적이지 않고 국경을 넘는 금융 거래 시 송금 수수료도 높아 블록체인 암호화폐 거래 시 장점이 많다.

비트페사 2014년 비트페사(BitPesa)는 케냐에서 비트코인을 기반으로 한 송금 결제 서비스를 개시했다. 케냐는 웨스턴유니언이나 시중은행을 통한 송금 수수료가 약 7%에 달하고 은행간 청산 결제에도 이틀 이상이 소요된다. 국경을 넘는 거래, 특히 선진국과 송금 결제 시에는 은행거래보다 비트코인의 장점이 많다.

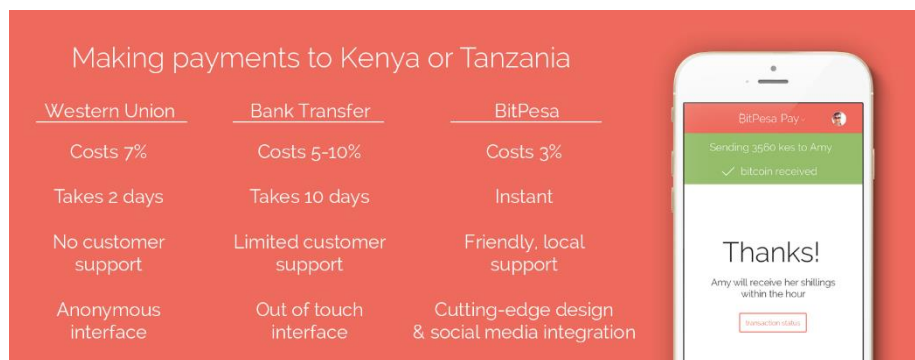
블록체인은 선진국의 기존 बैं킹 시스템에 비하면 아직 느리고 비효율적이지만 케냐와 같은 저개발 신흥국에서는 상당히 유용하게 쓰일 수 있다. 모든 것은 상대적이다. 아무 것도 갖춰지지 않은 곳에서 모바일 폰으로 बैं킹 서비스를 이용할 수 있게 한다는 것은 현재 블록체인 기술로도 충분히 혁신이라고 할 수 있다.

온두라스 정부 블록체인은 부패한 정부나 기관이 오명을 씻고 신뢰를 회복하고자 할 때 유용하게 쓰일 수 있다. 중앙아메리카 최빈국 중 하나인 온두라스는 오랜 기간 군부 독재 체제 하에 있었다. 온두라스는 가장 부패한 국가 상위권에서 오랫동안 빠지지 않았다. 군벌이나 토호 세력, 관료조차 시민의 토지를 권력으로 빼앗거나 불공정한 거래가 빈번했다고 한다.

온두라스 정부는 미국 블록체인 스타트업 팩팀의 기술을 도입해 국가 토지 대장을 블록체인 방식으로 전환하는 프로젝트를 추진하고 있다. 그 밖에도 공공부문에 블록체인을 도입해 신뢰도를 높이려는 것으로 알려져 있다.

한국에서는 엠페사 모바일 머니나 블록체인 등기부 등본 같은 서비스의 필요성을 느낄 수 없다. 은행 시스템이 잘 갖춰져 있고 환율은 안정적인 편이며 등기부 등본을 의심해야 할 일도 거의 없다. 하지만 전 세계 모든 국가가 대한민국만큼 신뢰할 만 하고 효율적인 것은 아니다. 비효율적이고 원칙없이 의사결정을 바꾸는 부패한 권력은 너무나 많다. 이런 국가나 기관들은 블록체인을 도입함으로써 잃어버린 신뢰를 다시 구축하고자 할 유인이 존재한다.

[그림47] 아프리카에서 확산되고 있는 비트페사 송금 서비스



자료: Bitpesa, 한화투자증권

3. 부패한 중개자를 배제한, 신속하고 투명한 원조

국제 원조 사업 역시 신뢰가 필요한 분야 중 하나다. UN(United Nations)과 UNICEF(United Nations International Childrens Emergency Fund) 등 국제 원조기구들은 블록체인 기술에 투자하고 있으며 투명하고 신속한 원조가 이뤄지길 기대하고 있다.

세계 식량 원조에 쓰인
이더리움

세계 최대의 구호 단체로서 식량 원조를 담당하고 있는 WFP(World Food Programme, 유엔세계식량계획)는 2017년 5월, 요르단에 있는 시리아 난민 약 1만명에게 암호화된 140만 달러 상당의 음식 쿠폰을 전달했다. 난민 원조에 이더리움 기반의 블록체인 기술을 활용한 것이다. 상점 계산원들은 스캐너로 쿠폰을 식별하고 데이터를 확인함으로써 모든 거래 기록은 이더리움 분산원장에 남았다.

블록체인 기술을 적용함으로써 금융 수수료를 크게 줄일 수 있었을 뿐 아니라 인건비와 소요시간도 줄일 수 있었다. 회계적인 측면에서도 식품 지급 즉시 분산원장에 기록되는 것을 확인할 수 있어 정산이 끝날 때까지 기다릴 필요가 없다.

이 프로젝트의 리더인 하다드는 지난 해 멕시코에서 열린 이더리움 개발자 회의에서 이 프로젝트를 통해 2018년까지 50만명 이상의 난민을 지원하겠다고 밝혔다. 블록체인 기술을 확장할수록 난민들에게 빠르고 신속하면서도 다양한 원조가 가능해질 전망이다. 하다드는 세계 보건 기구의 의료 기록, 유니세프의 교육 인증서 및 WFP의 영양 데이터를 포함해 현재 다양한 원조 기관마다 따로 관리하고 있는 데이터를 난민들에게 개인키 하나로 접근할 수 있게 하기를 희망한다고 말했다.

기술의 진보는 빠르고 관료화된 조직은 느리다. WFP의 프로젝트가 성공하기 위해서는 관료주의를 없애고 세계 각 기구가 협력해야 한다. 긍정적인 점은 블록체인 기술로 신뢰가 높아지면, 더 많은 지원을 이끌어 낼 수 있을 것이라는 사실이다. 원조가 필요한 사람들에게 합당한 자원 배분이 이뤄지는 것을 세계 어디서든 확인할 수 있게 된다면 더 많은 사람들이 참여하고자 하는 동기 부여 효과도 기대된다.

[그림48] WFP의 이더리움을 활용한 시리아 난민 원조 프로젝트



자료: WFP, 한화투자증권

4. 블록체인이 바꾸는 사회, 탈중앙화와 검열저항성

탈중앙화와 검열저항성

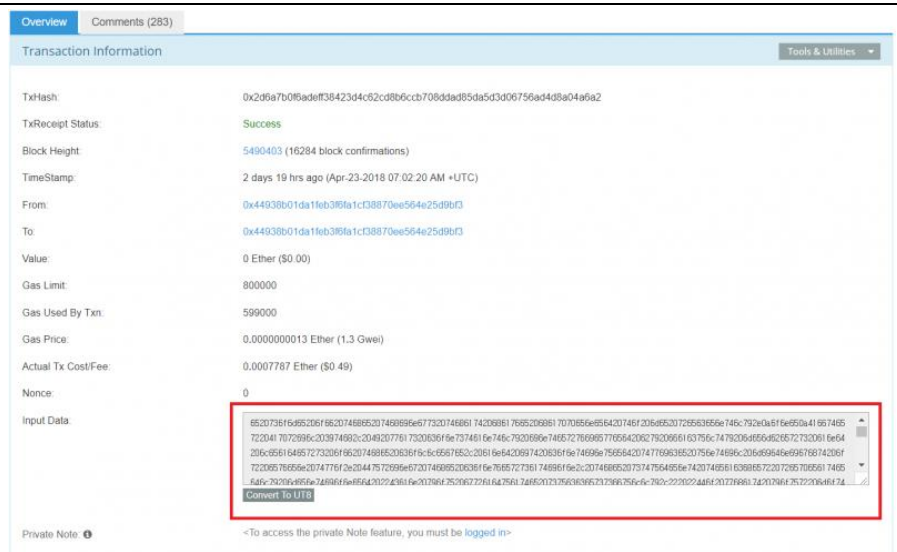
블록체인은 디지털 시대의 미디어로서 탈중앙화와 검열저항성을 가진다. 중앙 서버나 특정 관리 기구가 존재하지 않기 때문에 블록체인에 기록할 때 사전 검열이 어렵고 블록체인에 한번 기록되면 누군가가 임의로 삭제할 수 없다. 이것은 블록체인이 미디어에 불러온 큰 변화다. 이미 세상은 인터넷 상에서 자유롭게 의견을 개진하는 듯 변화해 왔지만 중앙 서버 관리 조직이 검열하고 임의로 삭제하거나 편집할 수 있었다. 블록체인은 분산화된 노드에 암호화돼 기록되며 한번 기록되고 나면 특정 시점의 기록을 임의로 변경할 수 없다.

2018년 4월, 이더리움 블록체인에 중국의 미투(Me Too) 운동 글이 올라와 화제가 됐다. 중국 북경대의 한 학생이 온라인 검열을 피해 성폭행 사건을 이더리움 블록체인에 기록한 것이다. 웨신(Yue Xin)이라는 이름의 학생은 이더리움에 이더(ETH)를 전송하면서 16진법으로 된 메모를 입력했다. 이 메모를 UTF-8으로 전환하면 ‘북경대의 선생과 학우들에게’로 시작하는 글이 나온다.

1998년, 북경대는 21살 대학생을 성폭행한 혐의를 받은 남성 교수를 사임케 했다. 피해 학생이 자살로 생을 마감하면서다. 학교 측은 단지 ‘사임’으로 죽음으로 이어진 성폭력 사건을 종결지었다. 이에 8명의 학생이 과거 사건에 대한 정보공개를 학교측에 요청했으나 학교측은 사임 사실 이외의 정보를 공개하지 않았고 정보공개청구서를 제출한 학생들을 압박했다고 한다. 이러한 상황에 대해 웨신은 이더리움 전송 메모에 기록했고 전세계 네트워크를 타고 퍼져 이더리움 블록체인에 저장됐다.

중국 정부가 이더리움 블록체인 관련 사이트를 차단할 수는 있겠지만 블록체인의 특성상 한번 올라간 기록을 삭제하는 것은 거의 불가능하다. 검열저항성이라는 블록체인의 강점을 보여준 사건이라 할 수 있다.

[그림49] 이더리움 블록체인에 기록된 중국 미투 운동 사건



자료: 블로터, <https://www.bloter.net/archives/308832>, 한화투자증권

이더리움 블록체인에
판문점 선언이 기록됨

2018년 4월 27일, 남과 북의 정상이 만나 한반도에 더 이상 전쟁은 없을 것이라며 판문점 선언을 발표했다. 한국인 개발자에 의해 판문점 선언도 이더리움 블록체인에 기록됐다. 그는 언론사와 인터뷰에서 중국 미투 운동 기록 사건에서 아이디어를 얻어 한국에 역사적인 판문점 선언을 이더리움에 기록하게 됐다고 말했다. 판문점 선언은 이더리움 551만 7596번째 블록에 기록되었으며 이더리움 네트워크 노드 전체가 파괴되지 않는 한 이 기록은 사라지지 않게 됐다. 기록을 찾아보고 싶다면 이더스캔 사이트에 접속해 검색창에 해당 거래값(Txhash)을 입력하면 확인할 수 있다.

이더리움 블록체인은 아마존 AWS같은 클라우드 컴퓨팅보다 느리고 더 비싸지만 탈중앙화, 검열저항성을 유지하는 것이 우선이라고 이더리움의 창시자 비탈릭 부테린은 주장한다. 한국에서도 언론의 자유가 없었던 시절이 있었고 지금도 세계 많은 나라에서 힘없는 개인은 보호받지 못한다. 탈중앙화된 블록체인 상에서는 검열을 피할 수 있고 개인 간에 자유롭게 무엇이든 거래할 수 있다. 블록체인은 사회적인 기술이다.

검열에 저항할 수 있는
미디어의 탄생

한편, 아무도 검열하지 않는다는 것이 반드시 이로운가에 대해서는 논란이 많다. 거짓 정보를 기록해도 삭제가 불가능하며 대중은 거짓된 정보에도 때때로 휩쓸린다. 어쨌거나 지금까지 언론 통제가 강했던 정부일수록 블록체인의 탈중앙화 철학에 불편해지는 것은 사실이다. 블록체인은 검열에 저항할 수 있는 미디어의 탄생이라는 의미가 있다.

[그림50] 이더리움에 기록된 판문점 선언

TxHash:	0xe4ee15d3f63db8464a649e3237ed83e930f9b3e40e842537a626745d1c96553c
TxReceipt Status:	Success
Block Height:	5517596 (86467 block confirmations)
TimeStamp:	15 days 2 hrs ago (Apr-28-2018 12:00:37 AM +UTC)
From:	0xe484c512c156c7f30c85cf432b8e2e70fd499058
To:	0xe456064545f872b311ae7432689a0fece90c9a29
Value:	0 Ether (\$0.00)
Gas Limit:	800000
Gas Used By Txn:	434032
Gas Price:	0.000000012 Ether (12 Gwei)
Actual Tx Cost/Fee:	0.005208384 Ether (\$3.51)
Nonce & {Position}:	0 {95}
Input Data:	<div style="border: 1px solid #ccc; padding: 5px;"> <p>0x2018년 4월 27일 한반도 판문점 선언</p> <p>1. 남과 북은 남북 관계의 전면적이며 획기적인 개선과 발전을 이룩함으로써 끊어진 민족의 혈맥을 잇고 공동번영과 자주통일의 미래를 앞당겨 나갈 것이다.</p> </div>

자료: etherscan.io, 한화투자증권

5. 초연결사회, 4차 산업혁명의 핵심이 될 블록체인

초연결사회 블록체인은 자율주행과 사물인터넷(IoT) 등 4차 산업혁명이라고 일컬어지는 혁신을 가능하게 할 전망이다. 4차 산업혁명이라는 용어에는 논란이 많은데 필자는 핵심은 초연결사회(Hyper Connected Society)라고 생각한다. 인터넷·통신 기술의 발전으로 사람과 사람이 연결되었다면 앞으로의 사회는 사람과 사물, 사물과 사물 간에 끊임없이 연결되며 자동적·지능적으로 컨트롤 되는 사회가 될 것이다.

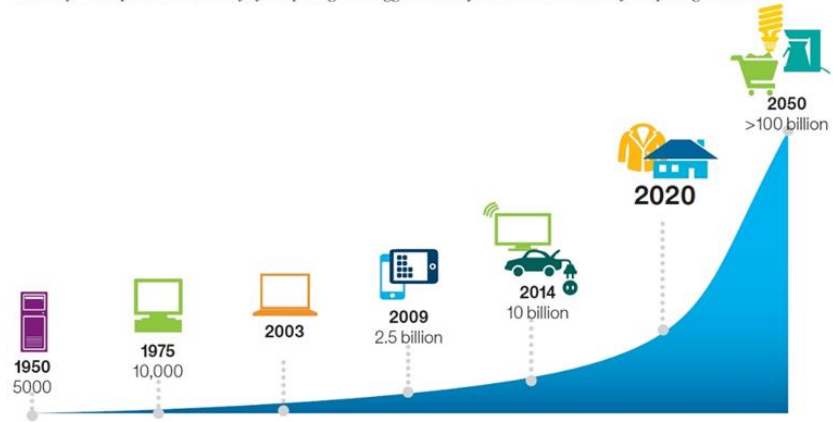
IT기업뿐 아니라 자동차, 물류, 서비스에 이르기까지 많은 기업과 정부기관들이 협력해 M2M(Machine to Machine), IoT(Internet of Things)에서 IoE(Internet of Everything)로 초연결사회가 되는 스마트 시티를 연구하고 있다.

기반기술이 될 블록체인 IBM에 따르면, 컴퓨팅 장치는 2014년 약 100억 개에서 2020년에는 약 250억 개로 증가할 전망이다. 현재까지 사물인터넷은 클라우드 컴퓨팅에 기반을 두고 발전해 왔다. 이 방식은 중앙 서버로서 집중된 대규모 데이터 센터를 필요로 하는데 구축 비용이 많이 들고 확장성과 보안에 대한 우려가 존재한다. 그런데 사물인터넷 기기들에 블록체인 기술을 적용하게 되면 기기 장치 스스로가 블록체인의 노드가 됨으로써 중앙 서버가 불필요해진다. 물론 보안성도 높아진다.

블록체인은 중개기관(Middleman)을 없애는 것뿐 아니라 사람이 배제된 기계간(Machine to Machine) 거래가 가능하게 할 전망이다. ‘비즈니스 블록체인’의 저자 윌리엄 무가야는 블록체인 기술이 월드와이드웹 이후 가장 혁신적인 인터넷 기술이라고 말한다. 웹이 IT 생태계를 뒤흔들었듯 블록체인 역시 현재의 중앙집중형 시스템 체제에 변화를 예고한다.

[그림51] 사물 인터넷 장치는 2014년 100억개에서 2050년 1천억개로 증가할 전망

Each inflection point in the history of computing has triggered an explosion in the number of computing devices



자료: IBM, 한화투자증권

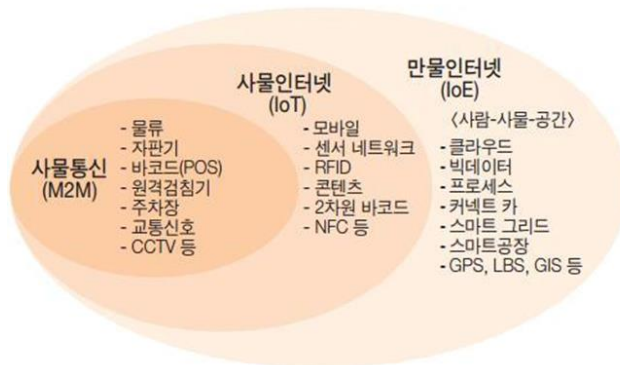
[그림52] 2025년 이후 사물인터넷은 분산 네트워크로 연결



자료: IBM, 한화투자증권

[그림53] 초연결사회 M2M, IoT, IoE의 포괄적 개념

M2M, IoT, IoE의 포괄적 개념



자료: 산업연구원, 한화투자증권

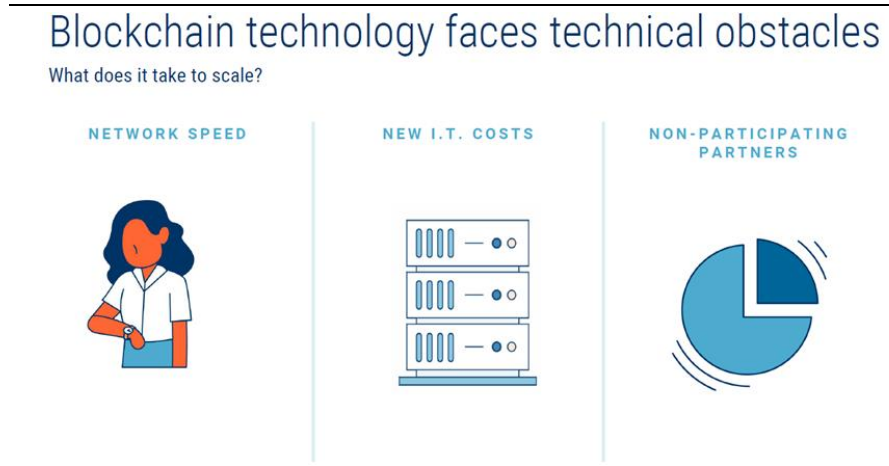
6. 블록체인이 해결해야 할 과제: 기술은 번영을 보장해주지 않는다

블록체인 기술이 상용화되기 위해서는 해결해야 할 과제가 많다. 비탈릭 부테린은 3년 차에 접어든 이더리움의 완성도가 아직 30% 수준이라고 말했다. 3세대 블록체인이라고 홍보하고 있는 대부분의 블록체인은 아직 개념 설계 단계 이거나 테스트넷을 구동하는 수준이다.

기술적 난제

CBInsights는 블록체인의 3가지 기술적 난점으로 네트워크 속도, 투자 비용, 참여자 확보를 위한 인센티브 부여 방법을 꼽았다. 이 밖에도 수많은 기술적 난점을 해결하는 데 최소한 몇 년의 시간이 걸릴 것으로 예상된다.

[그림54] 블록체인의 기술적 난제



자료: CB Insights, 한화투자증권

사회적, 법률적 문제

그런데 기술적 문제보다 더 큰 난관은 사회적, 법률적 문제다.

국내 한 보험사에서는 스마트 계약을 통해 고객이 의료기록을 별도로 제출하지 않아도 의료기관에서 진료를 받으면 자동으로 보험금을 지급하는 프로젝트를 추진하고 있다. 그런데 이러한 스마트 계약을 구동했을 때 문제의 소지가 있다. ‘개인정보보호법 제 21조(개인정보의 파기)’에 의하면 ‘개인정보 처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.’라고 되어 있는데 블록체인에 한번 기록된 데이터는 파기할 수 없다.

물론 블록체인에는 개인의 실명이나 의료기록 원본이 기록되는 것이 아니라 암호화된 문자로만 남게 된다. 현재의 기술로 본인이 아니면 해석이 불가능한 기록이라 해도 개인으로부터 발생한 기록은 법률 상 개인정보로 보기 때문에 이를 블록체인으로 상용화하려면 법 개정이 필요한 상황이다.

스마트 계약은 현재 법적 강제성이 없고 알고리즘에 의한 계약이기 때문에 계약 불이행 시 피해 보상에 대해 법적인 보호를 받기 힘들다. 따라서 전력 시장에 블록체인을 적용한다면, 마이크로그리드 상 개인 간 직접 전력 거래 시, 계약이나 결제 불이행 등의 문제 발생한다 해도 대처할 법적인 보호 장치가 없는 셈이다. 부동산 등기부 등본이나 유언장 서비스 같은 것도 마찬가지다.

영국의 적기조례

비단 블록체인만의 문제가 아니라 기술이 급변하는 시대에는 연관된 산업의 전통적 규율과 제도적 장벽을 뛰어넘는 개방된 논의가 필요하다. 1865년 영국의 '적기조례(Red Flag Act)'는 산업혁명의 중심이었던 영국이 자동차 산업의 주도권을 독일, 미국 등에 빼앗긴 이유를 보여주는 대표적인 사례다.

마차와 마부를 보호하겠다고 만든 법은 결국 마차와 마부뿐 아니라 자동차 산업도 망쳐 버렸다. 압호화폐 투자 열풍과 사기에 대한 소비자 보호 장치도 물론 필요하지만 블록체인을 적용해 사회적 효용을 높일 수 있는 분야에 대해서는 적극적인 제도 개혁이 필요하다.

[그림55] The Locomotive Act 1865 (적기조례)

- 1) 최고 속도는 교외에서는 시속 4마일(6km/h), 시가지에서는 시속 2마일(3 km/h)로 제한한다.
- 2) 1대의 자동차에는 세 사람의 운전수(운전수, 기관원, 기수)가 필요하고, 그 중 기수는 붉은 깃발(낮)이나 붉은 등(밤)을 갖고 55m 앞을 마차로 달리면서 자동차를 선도해야 한다. 기수(旗手)는 보속을 유지하며 기수(騎手)나 말에게 자동차의 접근을 예고한다.

자료: 나무위키, 한화투자증권

[그림56] The Locomotive Act 1865 (적기조례)

The Locomotive Act 1865 | Red Flag Act

XS2



© 2013/12. Photo by [Lukas Pauka](#). All rights reserved.

자료: Lukas Pauka, 한화투자증권

낮은 생존 확률

딜로이트는 2017년 10월, GitHub에 올라와 있는 블록체인 프로젝트 86천여 개 중 약 8%만이 관리되고 있는 것이며 5% 정도만이 생존할 것이라고 전망했다. 블록체인 기술은 발전하겠지만 기술이 발전한다고 해서 모두 성공할 수는 없다. 기술을 통해 혁신을 이루고 비즈니스를 성공시키는 것은 결국 사람이며 조직이다.

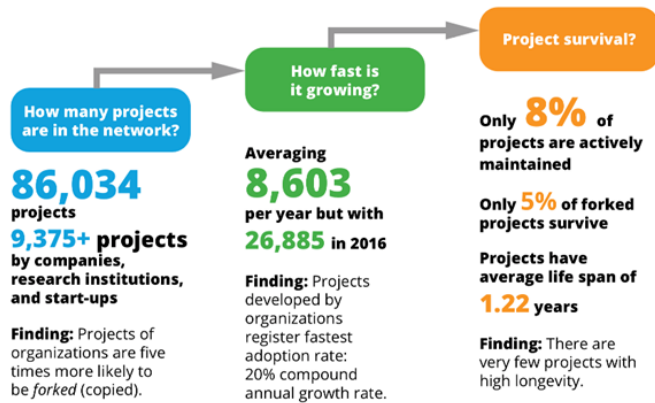
기업 운영방식의 변화

이더리움 재단 창립자이자 컨센시스(ConsenSys)의 CEO 조셉 루빈은 자본주의가 살아남으려면 우리 힘으로 체제를 바꿀 필요가 있다고 말했다. 특히 네트워크 세상에 부합하지 않는 지시나 통제 기반의 위계질서로부터 벗어나야 한다는 것이다. 컨센시스 멤버들은 자신이 일할 것을 알아서 선택하며 하향식 업무 할당이란 존재하지 않는다. 해야 할 작업을 공유, 확인하고 하고 업무를 배분하고 각자의 역할과 책임, 보상 수준을 합의하며 이 과정을 블록체인 네트워크 상에서 구현한다. 앞으로 블록체인 기반의 가상 기업이 이런 방식으로 운영되는 사례가 많아질 것이다. 특히 코딩같은 컴퓨터 기반의 업무가 대부분인 산업에서 이러한 비즈니스 모델은 상당히 유용할 것으로 기대된다.

거대 기업일수록 조직 체계는 고위 임원진을 시장의 신호로부터 떨어뜨리고 새로운 아이디어와 시도를 밀어내는데 파괴적 혁신은 변방에서 일어나고 결국 기업은 작은 혁신으로부터 위협받게 된다. 90년대 인터넷 확산기에 태동한 기업들이 세상을 움직이는 거대 공룡 기업이 되어있다. 아마존도 구글도 모두 한 때는 스타트업이었다. 많은 인터넷 기업들이 닷컴버블 이후 사라졌듯 수많은 블록체인 기업들도 험난한 생존 경쟁을 해야 할 것이다. 막연한 낙관이나 비관은 불필요하다. 변화가 무섭도록 빠르기는 하지만 변화의 흐름을 따라잡기 위해 노력해야 할 때다.

[그림57] 블록체인 프로젝트의 5%만 살아남을 수 있을 것이라는 딜로이트의 전망

Figure 3. Blockchain on GitHub



Source: Deloitte analysis of GH Torrent data and GitHub API data, as of October 12, 2017.

Deloitte Insights | deloitte.com/insights

자료: Deloitte, 한화투자증권



X. 불임

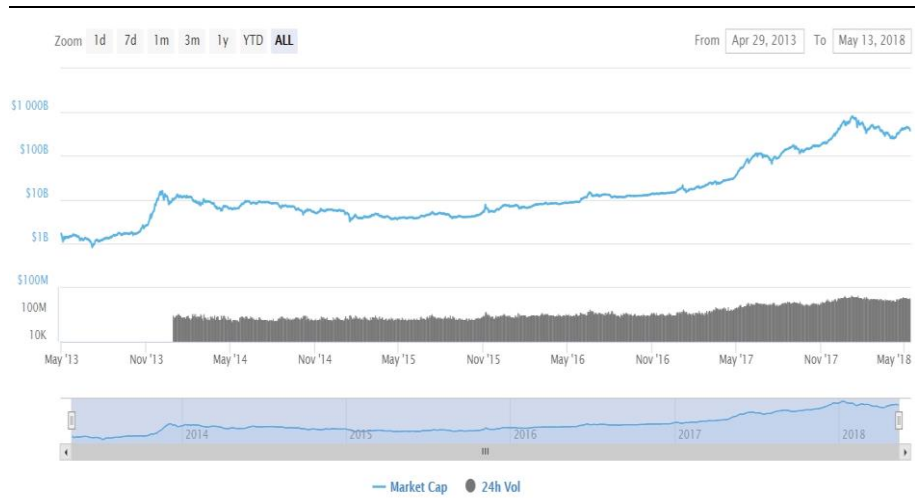
1. 암호화폐 시가총액과 시장점유율
2. 비트코인 주요차트
3. 이더리움 주요차트

1. 암호화폐 시가총액과 시장점유율

단락제목 필요 시 2018년 5월 13일 현재 암호화폐 전체 시가총액은 약 3,882억 달러(약 415조원) 규모로 비트코인이 1,443억 달러, 이더리움이 681억 달러를 기록하고 있다.

시장 점유율을 살펴보면, 비트코인 37.4%, 이더리움 17.5%, 리플 7.0%, 비트코인 캐시 6.4%, 라이트코인 2.1% 순이다. 다양한 종류의 토큰 발행이 지속되면서 상위 10개를 제외한 기타코인 합산 비중이 약 25%로 상승했다.

[그림58] 암호화폐 전체 시가총액 (로그 스케일)



자료: coinmarketcap, 한화투자증권

[그림59] 암호화폐 시장 점유율 추이



자료: coinmarketcap, 한화투자증권

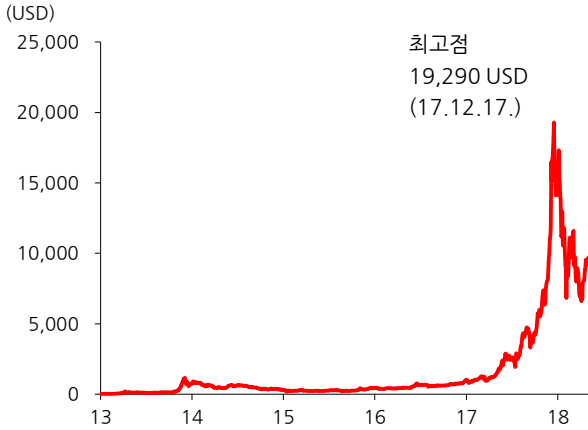
[표4] 암호화폐 시가총액 상위 30 개

No.	이름	단위	시가총액 (BnUSD)	가격 (USD)	발행량 (천개)	24시간 거래금액 (BnUSD)	%24h
1	Bitcoin	BTC	143.9	8,452.0	17,031	6.65	-0.24%
2	Ethereum	ETH	67.6	679.9	99,401	2.60	-0.65%
3	Ripple	XRP	26.9	0.7	39,189,968	0.58	-1.07%
4	Bitcoin Cash	BCH	24.6	1,437.0	17,125	1.40	3.00%
5	EOS	EOS	11.9	14.0	85,269	3.06	-6.82%
6	Litecoin	LTC	7.9	140.3	56,507	0.40	1.58%
7	Cardano	ADA	6.9	0.3	25,927,071	0.26	0.07%
8	Stellar	XLM	6.7	0.4	18,576,314	0.11	11.12%
9	IOTA	MIOTA	5.2	1.9	2,779,530	0.11	0.12%
10	TRON	TRX	4.5	0.1	65,748,112	0.63	2.47%
11	NEO	NEO	4.2	64.0	65,000	0.12	0.36%
12	Monero	XMR	3.3	205.1	16,025	0.03	2.39%
13	Dash	DASH	3.2	399.6	8,068	0.08	0.83%
14	NEM	XEM	2.9	0.3	9,000,000	0.02	1.70%
15	VeChain	VEN	2.4	4.5	526,019	0.07	0.13%
16	Tether	USDT	2.2	1.0	2,207,141	4.47	0.26%
17	Ethereum Classic	ETC	1.8	18.1	101,656	0.26	1.68%
18	Bytecoin	BCN	1.7	0.0	183,886,850	0.04	-7.44%
19	ICON	ICX	1.5	3.9	387,231	0.08	-3.95%
20	Binance Coin	BNB	1.5	12.8	114,041	0.04	0.05%
21	Qtum	QTUM	1.4	16.2	88,591	0.15	-0.25%
22	OmiseGO	OMG	1.4	13.7	102,043	0.04	0.42%
23	Zilliqa	ZIL	1.3	0.2	7,286,962	0.19	2.37%
24	Lisk	LSK	1.1	10.1	105,830	0.02	0.33%
25	Zcash	ZEC	1.0	247.1	3,904	0.04	2.47%
26	Bitcoin Gold	BTG	1.0	56.2	17,001	0.02	-2.18%
27	Aeternity	AE	0.9	3.8	233,020	0.03	-2.67%
28	Verge	XVG	0.9	0.1	14,983,058	0.03	-2.22%
29	Ox	ZRX	0.9	1.6	528,667	0.03	-5.56%
30	Nano	NANO	0.8	6.2	133,248	0.01	1.00%

자료: Coinmarketcap, 한화투자증권

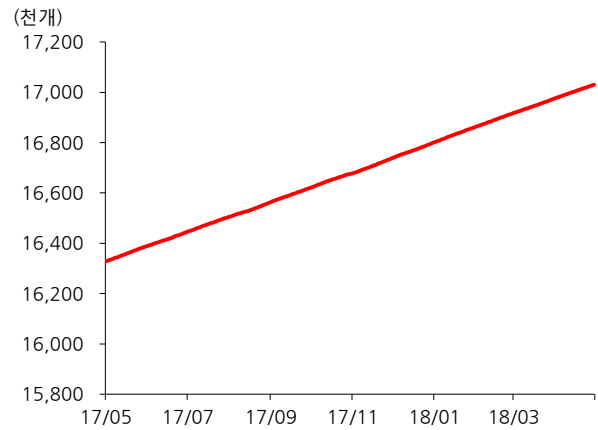
2. 비트코인 주요차트

[그림60] 비트코인 가격: 8,401 USD (18.05.13.)



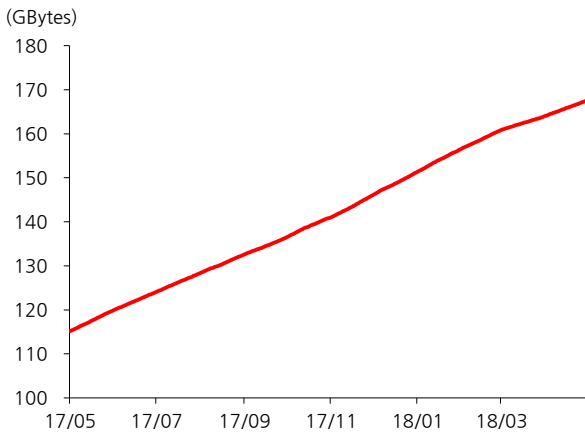
자료: Blockchain.info, 한화투자증권

[그림61] 비트코인 누적 채굴량: 1,703 만개 (18.05.13.)



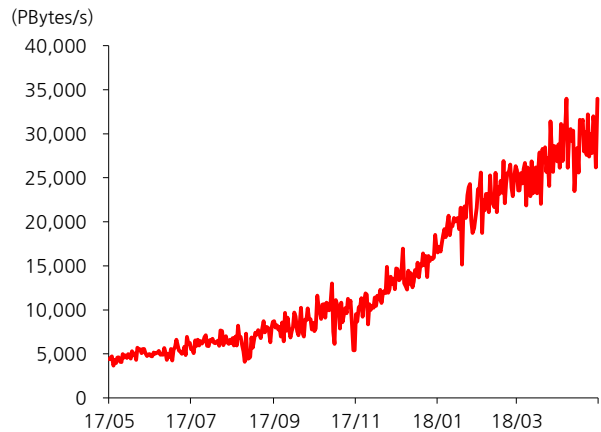
자료: Blockchain.info, 한화투자증권

[그림62] 비트코인 블록 전체 사이즈: 약 167 기가바이트



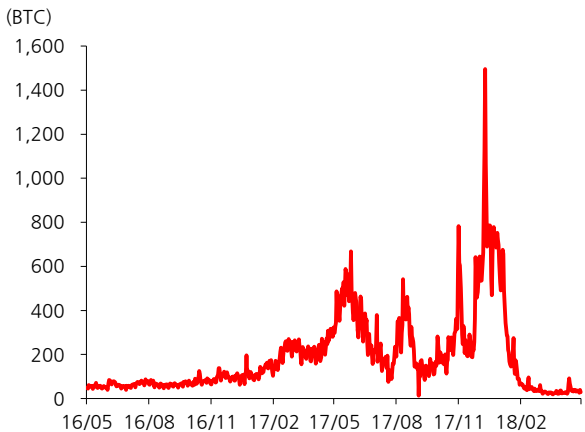
자료: Blockchain.info, 한화투자증권

[그림63] 비트코인 해시 레이트: 약 3,399 페타바이트/초



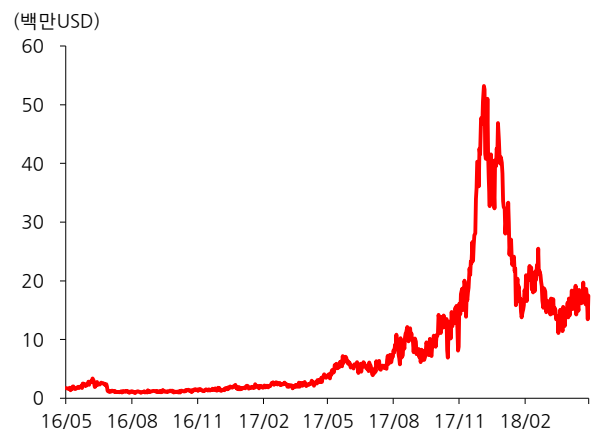
자료: Blockchain.info, 한화투자증권

[그림64] 블록보상을 제외한 전체 수수료: 약 28 BTC/일



자료: Blockchain.info, 한화투자증권

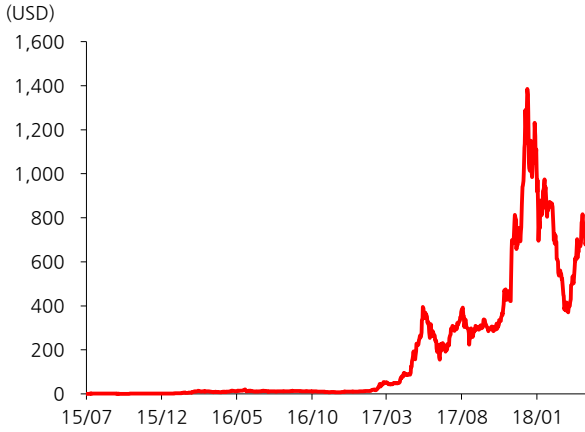
[그림65] 블록보상을 포함한 마이닝 수익: 약 1,750 만 달러/일



자료: Blockchain.info, 한화투자증권

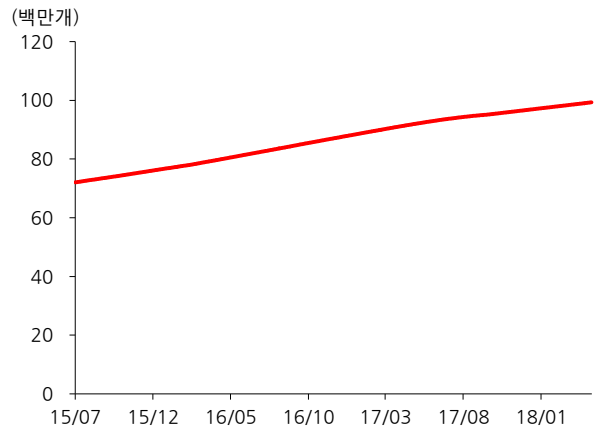
3. 이더리움 주요차트

[그림66] 이더리움 가격: 685 USD (18.05.13)



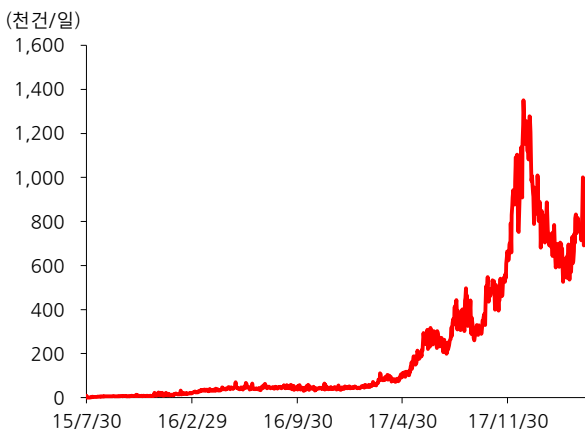
자료: etherscan.io, 한화투자증권

[그림67] 이더리움 누적 채굴량: 약 9,940 만개 (18.05.13)



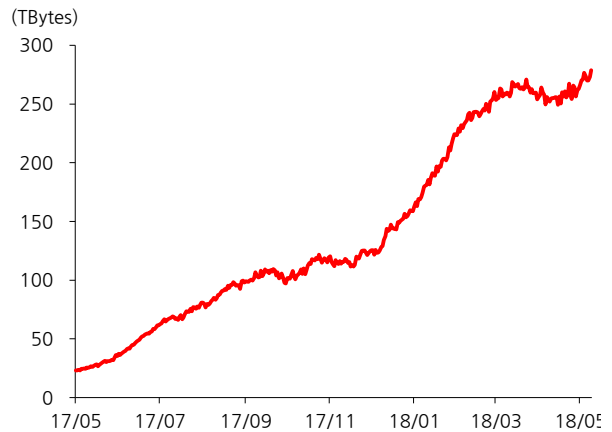
자료: etherscan.io, 한화투자증권

[그림68] 1 일 트랜잭션 건수: 788 만건 (18.05.09)



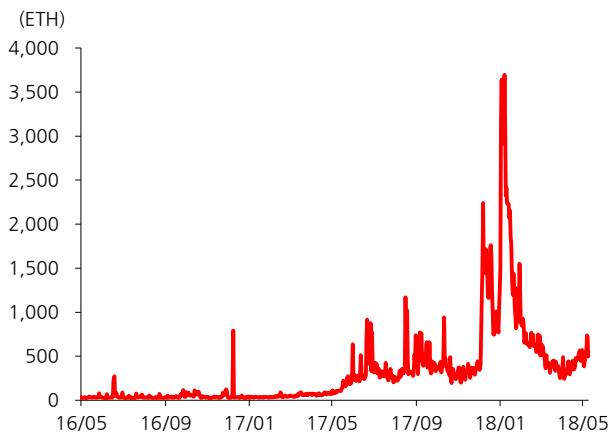
자료: etherscan.io, 한화투자증권

[그림69] 이더리움 해시 레이트: 약 279 테라바이트/초



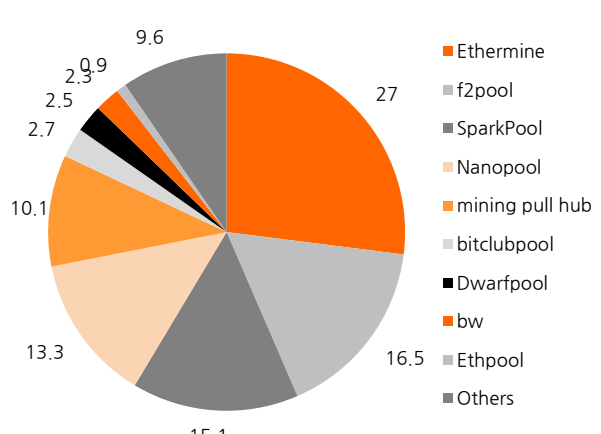
자료: etherscan.io, 한화투자증권

[그림70] 블록보상을 제외한 전체 수수료: 약 498 ETH/일











자료: etherscan.io, 한화투자증권

[그림71] 이더리움 채굴 순위



자료: etherscan.io, 한화투자증권

[그림72] ERC20 로 발행된 토큰 시가총액 순위

	Token	Price	%Change	Volume (24h)	~ MarketCap
1	 EOS (EOS) Infrastructure for Decentralized Applications	\$14.0793 0.00167301 Btc 0.020821 Eth	▲ 2.92%	\$2,764,430,000	\$12,005,644,027
2	 Tronix (TRX) TRON is a blockchain-based decentralized protocol that aims to construct a worldwide free content entertainment system with the blockchain and distributed storage technology.	\$0.0691 0.00000821 Btc 0.000102 Eth	▲ 8.58%	\$613,620,000	\$4,541,143,174
3	 VeChain (VEN) VeChain aims to connect blockchain technology to the real world by providing a comprehensive governance structure, a robust economic model as well as advanced IoT integration.	\$4.5059 0.00053543 Btc 0.006664 Eth	▲ 3.86%	\$56,863,300	\$2,370,210,718
4	 ICON (ICX) The ICON Network is comprised of various institutions ranging from: financial institutions, insurance companies, hospitals, universities and more.	\$3.8694 0.0004598 Btc 0.005722 Eth	▲ 0.94%	\$68,421,000	\$1,498,364,597
5	 BNB (BNB) Binance aims to build a world-class crypto exchange, powering the future of crypto finance.	\$12.8608 0.00152822 Btc 0.019019 Eth	▲ 2.65%	\$40,067,200	\$1,466,662,224
6	 OmiseGO (OMG) OmiseGO (OMG) is a public Ethereum-based financial technology for use in mainstream digital wallets	\$13.5400 0.00180894 Btc 0.020024 Eth	▲ 3.15%	\$38,274,600	\$1,381,656,151
7	 Zilliqa (ZIL) Zilliqa is a high-throughput public blockchain platform - designed to scale to thousands of transactions per second.	\$0.1740 0.00002067 Btc 0.000257 Eth	▲ 9.39%	\$180,398,000	\$1,267,639,901
8	 Aeternity (AE) Scalable smart contracts interfacing with real world data.	\$3.7741 0.00044847 Btc 0.005581 Eth	▲ 4.21%	\$33,268,700	\$879,442,564

자료: etherscan, 한화투자증권

[Compliance Notice]

본 자료는 투자자의 증권투자를 돕기 위하여 당사 고객에 한하여 배포되는 자료로서 어떠한 경우에도 복사되거나 대여될 수 없습니다. 본 조사자료에 수록된 내용은 당사 리서치센터가 신뢰할 만한 자료 및 정보로부터 얻어진 것이나, 당사는 그 정확성이나 안전성을 보장할 수 없습니다. 따라서, 어떠한 경우에도 본 자료는 고객의 증권투자의 결과에 대한 법적 책임소재에 대한 증빙자료로 사용할 수 없습니다.