

# 비트코인의 현황 및 시사점

이동규<sup>■</sup>

금융결제국 결제연구팀

---

■ 결제연구팀 조사역(Tel : 02-750-6629, E-mail : ldg11@bok.or.kr)

◆ 이 자료의 내용은 집필자의 개인의견으로서 한국은행의 공식견해를 나타내는 것은 아닙니다. 본 조사연구를 진행하는 과정에서 유익한 조언을 해주신 김종욱 결제연구팀장, 이상형 통화연구팀장, 오영주 외환심사팀장께 감사드립니다.



## < 차례 >

### <요 약>

<b>I. 검토 배경 .....</b>	<b>1</b>
<b>II. 비트코인의 개념 및 현황 .....</b>	<b>2</b>
1. 비트코인의 개념	
2. 비트코인 시스템의 구성	
3. 비트코인의 거래 규모	
<b>III. 주요 제약점 .....</b>	<b>13</b>
<b>IV. 해외 논의 및 대응 사례 .....</b>	<b>17</b>
<b>V. 시사점 .....</b>	<b>22</b>

<부록> 비트코인 거래 절차



## 비트코인의 현황 및 시사점

### I

#### 비트코인의 개요

- 비트코인(Bitcoin)은 사토시 나카모토(Satoshi Nakamoto)란 가명의 프로그래머 (또는 집단)에 의해 2009년 처음으로 도입
  - 디지털 파일의 형태로 구매력이 저장되고 구매력을 자체단위<sup>■</sup>로 표시한다는 점에서 가상화폐(virtual currency)와 유사한 면이 있으나 발행기관이 없다는 점에서는 구별
    - 비트코인의 기본단위로 BTC(비트코인)를 사용하며 보조단위로 mBTC(=0.001BTC, 밀리코인), μBTC(=0.000001BTC, 마이크로코인) 및 satoshi(=0.00000001, 사토시)가 있음
- 비트코인은 P2P 네트워크상에서 암호화 알고리즘에 따라 채굴(mining)되며 채굴자들을 포함한 다수의 네트워크 참가자들은 계좌이체 방법으로 비트코인을 거래
  - 채굴이란 계좌이체 거래기록들을 이용하여 일종의 수학문제를 푸는 작업을 말하며 채굴에 성공하는 자에게는 시스템 운영에 기여한 대가로 일정한 비트코인이 새로 발행되어 주어짐
  - 채굴(약 10분 정도 소요)이 성공하면 채굴과정에서 이용된 거래기록들이 승인되며 채굴이 성공하기 전까지의 거래는 미확정 상태<sup>■</sup>를 지속
    - 거래 미확정 상태에서 수취자는 계좌이체로 받은 비트코인을 사용할 수 없음
  - 채굴자들의 성공보수(현재 25BTC)가 약 4년마다 절반으로 줄어들도록 설계되어 있어 총 발행량은 2,100만BTC로 제한됨(현재 1,200만BTC 발행)
  - 전체 채굴량이 2,100만BTC에 근접하여 비트코인이 추가로 발행되지 않는 경우 채굴자들은 계좌이체 거래자들로부터 수수료<sup>■</sup>만을 수취
    - 거래기록이 승인되면 거래자들은 거래금액과 상관없이 건당 0.0001BTC 정도의 수수료를 채굴자에게 지급
- 비트코인 거래자들은 은행계좌에 해당하는 공개주소(public address)를 활용하여 비트코인을 이체
  - 기존의 인터넷 뱅킹 등과 달리 이체시 청산 및 결제 기능을 담당하는 금융기관 및 중앙은행을 필요로 하지 않음

## II

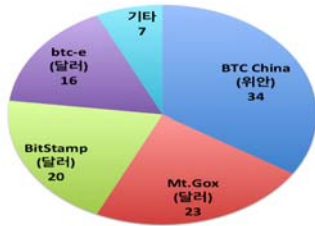
### 비트코인의 거래 현황

□ 비트코인 거래자들은 채굴 방법 이외에도 유가증권 또는 외환의 경우와 같이 거래소 구매 방법으로 비트코인을 획득할 수 있음

— BTC China(중국), Mt.Gox(일본), bitcoin.de(독일) 등이 위안, 달러, 유로화 등과 비트코인간 거래를 중개하고 있으며 한국에서는 Korbit이 2013.7월부터 내국인 대상 원화거래를 중개하기 시작

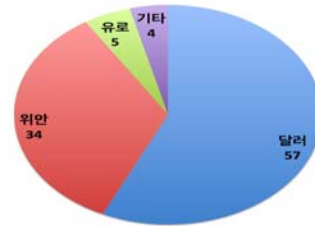
거래소 시장점유율<sup>1)</sup>

(단위: %)



통화별 거래비중<sup>1)</sup>

(단위: %)



주: 1) 2013.12.2일 기준

자료: www.bitcoincharts.com

— 달러 대비 환율은 각국 정부의 비트코인 규제 등에 대한 부분적 견해 표명에 따라 급등락을 반복

○ 2013.4월 키프로스 정부가 규제금융의 전제조건으로 은행예금에 대한 일괄적 과세방안을 확정하자 대체 투자자산으로서 비트코인에 대한 인기가 높아지면서 1BTC당 가격이 266달러까지 상승

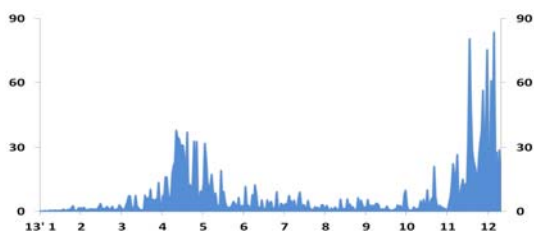
○ 최근에는 11.18일 열린 미국 의회 청문회에서 버냉키 연준의장이 비트코인의 장래성을 인정하는 취지의 서한<sup>■</sup>을 보낸 것으로 알려지면서 가격이 다시 사상 최고 수준인 1,200달러를 기록

■ 당시 버냉키 연준의장의 서한 내용은 다소 왜곡되어 알려졌는데 이에 관한 내용은 5쪽 참조

○ 이후 12월초 중국 인민은행이 투기성과 가격변동성을 우려하여 금융기관의 비트코인 업무취급을 금지시킴에 따라 일시 600달러대까지 급락하였다가 재차 반등

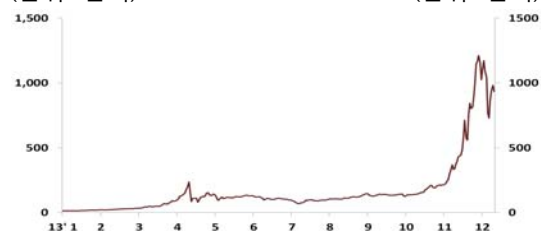
비트코인 거래량

(단위: 백만달러)



비트코인 달러 가격<sup>1)</sup>

(단위: 달러)



주: 1) Mt.Gox 기준

자료: www.blockchain.info, www.bitcoincharts.com

□ 비트코인을 지급수단으로 인정하는 가맹점은 아직 많지 않으나 그 수는 점차 증가하는 추세

— 주로 **WordPress, Wikileaks, The Pirate Bay**와 같은 온라인 사이트들이 비트코인을 받아들이고 있으며 미국과 유럽을 중심으로 오프라인 가맹점도 늘어나고 있음

○ 높은 익명성, 편리한 자금이체, 낮은 수수료 및 비트코인 가격 상승기 대 등 경제적인 이유와 비트코인에 관심을 가진 사람들에게 홍보할 수 있다는 점이 가맹점 증가의 원인으로 지적

#### 비트코인을 지급수단으로 인정하는 주요 온라인 서비스

명 칭	서비스 내용	비트코인 수납 시기
WordPress	블로그 서비스	2012.11월
The Pirate Bay	P2P 파일공유 서비스	2013. 4월
Reddit	소셜 뉴스 서비스	2013. 2월
The Internet Archive	웹사이트 라이브러리 서비스	2013. 2월
OkCupid	소셜 네트워크 서비스	2013. 4월

자료: Forbes

— 또한 선불카드 판매 서비스인 **Gyft** 등이 지급수단으로 비트코인을 인정함에 따라 비트코인을 보유한 소비자가 **Amazon, Groupon**(온라인 쇼핑몰) 등의 선불카드 가맹점도 이용할 수 있게 됨

### III 비트코인 논의 동향

#### (주요 규제 논의)

□ 비트코인은 거래의 익명성을 보장하고 별다른 규제가 적용되지 않는다는 점에서 자금세탁, 탈세, 마약 및 무기 밀매 등 불법적인 거래에 활용될 수 있다는 우려가 제기

▪ 마약 및 무기 밀거래 사이트인 실크로드(Silk Road)는 지급수단으로 비트코인만을 허용

— 이로 인해 비트코인 사용이 비교적 활성화된 미국 및 유럽을 중심으로 비트코인의 법적 성격을 규정하는 한편 비트코인 관련 서비스를 규제하고자 하는 움직임이 나타남

□ 그러나 비트코인의 법적 성격이나 서비스 규제에 관한 각국 정부의 입장은 다소 차이를 보이고 있음

— 우선 미국은 법원 판례와 규제 가이드라인을 통해 비트코인이 부분적으로는 화폐(money)의 성격을 갖는다고 해석

- 2013.3월 미국 재무부 산하 금융정보분석기구인 FinCEN(Financial Crime Enforcement Network)은 가상화폐 거래소를 자금이체기관(money transmitter)으로 파악▪하였으며 이에 따라 비트코인 거래소 Mt.Gox는 계좌주의 신원 확인 등 자금세탁 방지 의무를 이행하면서 6월 FinCEN 으로부터 자금이체업 허가를 받음
  - *A user of virtual currency is not an MSB(Money Services Business) under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and record keeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter. (FinCEN Guidance 2013.3.18)*
- 2013.8월 텍사스 연방 판사는 SEC(Securities and Exchange Commission)가 Bitcoin Savings & Trust를 금융사기 혐의로 기소한 사건에서 비트코인 투자를 화폐 형태(form of money)의 투자로 판단
  - *It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money. (U.S. Eastern District of Texas Court, Memorandum Opinion 2013.8.6.)*
- 2013.7월 독일 연방금융감독기구(BaFin)는 규제 가이드라인에서 비트코인을 일종의 금융상품(financial instruments)으로 판단
  - 이에 따라 2013.8월부터 독일 소재의 비트코인 거래소 bitcoin.de는 BaFin으로부터 금융중개기관(financial intermediary) 허가를 받았으며 Fidor Bank와 파트너쉽▪을 체결
    - 파트너쉽 체결로 고객들은 Fidor Bank가 제공하는 계좌를 이용해 실시간으로 bitcoin.de에서 비트코인 매매를 할 수 있게 됨
  - 비트코인이 금융상품으로 인정됨에 따라 비트코인을 1년 미만 보유하면서 자본 이득을 실현한 사람에게는 자본이득세가 부과
    - *This means that, like stocks or shares, any profit from them(Bitcoin) is subject to Germany's capital gains tax, at 25pc - unless they are held for more than a year, according to German newspaper Frankfurter Allgemeine Zeitung.(The Telegraph 2013.8.19.)*
- 한편 금년 7월 태국 중앙은행은 비트코인이 환차익을 위한 투기수단일 수 있다는 이유로 비트코인 거래소(Bitcoin Co. Ltd.)의 등록을 거부
  - *For now we(Bank of Thailand) asked they(Bitcoin Co. Ltd.) not involve themselves with the baht because what they do may be a way to speculate on the exchange rate. (Bank of Thailand, Governor Prasarn Trairatvorakul, Asian Correspondent, 2013.7.31.)*



- 또한 중국 인민은행 등 정책당국은 비트코인이 투기성과 가격변동성이 높은 점을 들어 금융기관의 비트코인 업무취급을 금지시키는 등 부정적인 입장
  - 12.5일 인민은행 등은 「비트코인 관련 리스크 방지 통지(關於防范比特幣風險的通知)」를 통해 금융기관의 비트코인 관련 업무 취급을 금지
  - 동 통지문에 따르면 비트코인은 화폐 대용물(monetary equivalent)로서의 법적인 지위를 가지지 않으며 현재 중국 금융시스템을 위협하고 있는 않으나 정책당국은 위험요소를 예의 주시하고 있음을 적시

(미 의회, 연준 등의 논의)

□ 미 상원은 지난 11.18일 법무부, 국토안전부, 재무부 관계자 등을 대상으로 청문회를 개최하였으며, 동 청문회는 비트코인에 대한 사실 확인 (fact-finding)에 주안점을 두고 진행

— Tom Carper 상원의원은 비트코인을 초기 인터넷 및 1980년대 신용카드 붐(boom)과 비교하는 등 비트코인의 혁신성을 강조하면서 정책당국이 새로운 규제체계를 확립하거나 뚜렷한 정책적 견해를 제시함으로써 비트코인과 관련한 불확실성을 해소할 필요가 있다고 주장

— 대부분의 정부 관계자는 비트코인이 합법적인 금융서비스(financial service)이며, 현재로서는 비트코인을 이용한 범죄를 우려하여 추가적인 규제책을 마련하고 있지 않다고 증언

— 비트코인 재단(Bitcoin Foundation) 관계자는 은행산업이 취약한 국가에서 비트코인에 대한 수요가 크게 증가하고 있으며, 미국 내에서는 캘리포니아, 조지아 주가 비트코인의 상용화를 주도하고 있다고 주장

□ 또한 버냉키 의장은 의회 청문회에 제출한 서한에서 가상화폐는 전자화폐(electronic money)의 한 형태로서 이와 같은 지급수단 혁신이 법 집행 및 감독 업무에 리스크를 초래할 수 있지만 효율적이고 안전한 지급결제시스템으로의 발전을 촉진한다면 장기적으로는 성공할 가능성이 있다고(may hold long-term promise) 언급

— 미 연준은 가상화폐의 발전 및 지급결제시스템의 혁신 등에 대해 모니터링하고 있으나 지급수단 혁신이나 발행주체에 대해 전반적인 규제 및 감독 권한을 가지고 있는 것은 아님

— 연준은 감독대상 은행 기관이 발행, 청산 및 결제한 가상화폐에 국한하여 규제 및 감독을 할 수 있으며 필요한 경우 가상화폐 등 전자현금(electronic cash) 이슈에 대해 정부와 공조할 방침

□ **Bloomberg**는 청문회 직후 기사에서 비트코인이 일종의 금융서비스로서 인정받게 되었지만 실패한 혁신으로 끝날 수 있다고 전망

- 버냉키 의장이 비트코인을 특정하여 “장기적인 성공” 가능성을 이야기 한 것이 아니라 **financial inclusion** 관점에서 소비자, 특히 취약계층에 도움이 될 수 있는 가상화폐 전반에 대해서 긍정적인 입장을 나타낸 것임
- 아직까지 비트코인은 현금 또는 신용카드와 비교하여 지급수단으로서의 우월성이 명확하게 드러나지 않고 있을 뿐만 아니라, 보안 취약성, 디플레이션 유발 가능성, 불안정한 인프라 등 많은 문제점을 가지고 있음

#### IV

#### 비트코인 전망 및 시사점

□ **성장 요인** : 비트코인은 물리적 공간의 제약 없이 자금이체가 가능하고 거래수수료가 낮으며 다양한 방식의 거래가 가능하다는 점에서 이론적으로는 지급거래수단으로 발전할 가능성

□ **주요 한계** : 그러나 여러 가지 한계로 인해 이론적 성장 가능성이 실현되기는 어려울 것으로 판단

- **(취약한 보안성)** 비트코인 개인사용자 또는 거래소에 대한 해킹 사례가 늘어나고 있는 가운데 별다른 보안 대책은 마련되고 있지 않음
- **(가격 변동성)** 투기적 거래로 인해 비트코인 가치가 급격하게 변동하고 있어 비트코인이 가까운 장래에 보편적인 교환의 매개로 활용될 가능성은 낮음
  - 비트코인은 내재적 가치(intrinsic value)가 없기 때문에 17세기 네덜란드에서 발생한 튜립버블과 같은 투기적 수요에 쉽게 노출될 우려
- **(제한적 수용성)** 최근 비트코인 가맹점이 늘어나고 있으나 거래규모는 다른 지급수단 또는 금융상품에 비해 극히 미미한 수준이며 가치를 보증하는 발행기관이 없어 가맹점 확산은 제한적일 것으로 예상
- **(채굴유인 감소)** 채굴자들에게 보상으로 지급되는 비트코인의 양이 계속 줄어들도록 설계되어 있어 시간이 지날수록 채산성이 감소하면서 거래가 지연될 가능성
- **(높은 사회적 비용)** 비트코인이 개별 사용자의 거래 비용은 낮출 수 있지만 채굴 과정에는 엄청난 양의 전기를 사용하는 컴퓨터 연산이 필요하므로 사회적인 거래비용은 낮지 않음

- 채굴자들의 일평균 전기사용량, 거래건수 등을 고려하면 현재 건당 평균 거래비용은 약 2.57달러 수준
- 소액지급수단의 사회적 비용에 관한 ECB의 연구와 비교하면, 비트코인 거래비용은 수표, 신용카드보다 낮으나 현금보다는 4배, 직불카드보다는 2.5배 이상 높은 수준

#### 지급수단별 건당 거래비용<sup>1)</sup>

(단위: 달러)	현금	수표	카드	(직불카드)	(신용카드)	자동이체	계좌이체	비트코인
건당 거래비용	0.57	4.79	1.34	0.95	3.22	1.71	2.59	<b>2.57</b>

주: 1) 비트코인의 1유로당 1.35달러의 환율 적용  
 자료: European System of Central Banks, www.blockchain.info

- 비트코인은 지급거래의 효율성과 편의성을 제고할 수 있는 장점이 있으나 보안의 취약성, 가격의 급변성, 제한적 수용성 등으로 인해 앞으로 대안적인 지급수단으로 성장할지는 매우 불투명
  - 다만 국가간 거래, 소액 거래 등 제한된 영역에서 활용되면서 해킹, 자금세탁 등 불법 행위가 시도될 수 있는 만큼 정부는 비트코인에 대한 규제 방안을 마련할 필요
  - 비트코인은 발행기관이나 중앙서버가 없는 분권화된(decentralized) 체계로서 네트워크 참가자들도 익명성을 보호받기 때문에 비트코인 발행을 금지하거나 채굴자들을 직접 규제하는 것은 어려움
  - 조직화·기업화된 형태의 비트코인 서비스 또는 대규모의 상업적인 사용은 소비자 보호, 과세 및 불법행위 방지 등을 위해 적절한 규제체계 하에서 이루어지도록 하는 것이 바람직
  - 또한 모든 거래는 네트워크를 통해 모두에게 공개되는 만큼 대규모 네트워크 데이터에 대한 분석능력을 확충
- 한편 비트코인은 종전과 크게 다른 형태의 시도라는 점에서 새로운 패러다임의 확산이 경제에 미칠 영향에 대해 지속적인 관심을 기울일 필요
  - 현재의 비트코인이 실패한 시도로 끝난다 하더라도 비트코인의 한계점 및 문제점을 개선한 새로운 방식의 가상화폐가 등장할 개연성이 있음



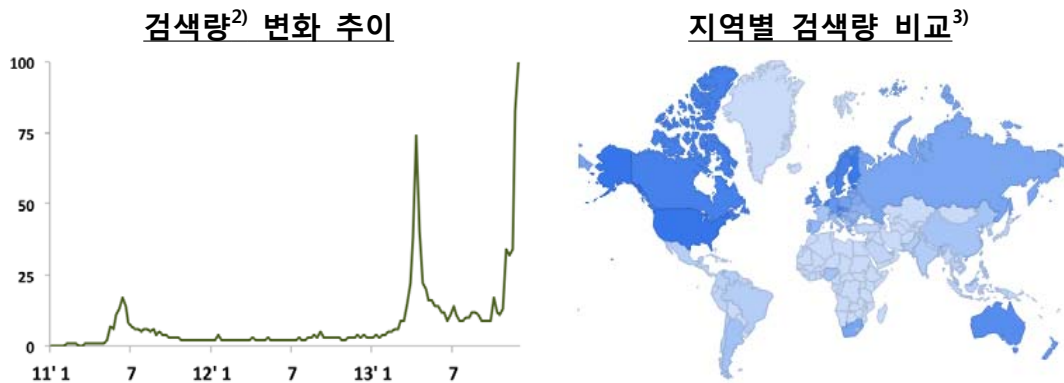




## I 검토 배경

- 인터넷의 대중화, 통신속도의 향상 등 기술혁신을 배경으로 2009년부터 등장한 비트코인(bitcoin)이 빠른 속도로 확산
  - 지난 2013.11월에는 비트코인에 대한 미국 의회 청문회가 열리면서 전세계적으로 비트코인에 대한 관심이 집중
  - 국내에도 비트코인 거래소가 설립되고 비트코인 보도가 늘어남에 따라 일반의 비트코인에 대한 인지도가 높아지고 있음
- 한편 각국에서는 발행기관을 특정하기 어려운 비트코인의 성격을 두고 정부 및 학계를 중심으로 활발한 논의를 진행

### 비트코인 구글 트렌드 검색 결과<sup>1)</sup>



주: 1) 검색어: Bitcoin, 검색기간: 2011.1월초 ~ 2013.11월말  
2) 검색량이 가장 많았던 때를 100으로 한 상대적인 비율  
3) 파란색이 진할수록 검색량이 많음  
자료: [www.google.com/trends](http://www.google.com/trends)

- 그러나 국내에서는 아직까지 비트코인에 대한 체계적 설명이나 분석을 담은 연구가 많지 않은 상황
  - 이에 본고는 비트코인의 개념 및 현황을 살펴보고 주요 논의를 정리함으로써 향후 성장 가능성을 점검하고자 함

## II 비트코인의 개념 및 현황

### 1 비트코인의 개념

#### 가. 비트코인의 개념

□ 비트코인(Bitcoin)은 사토시 나카모토(Satoshi Nakamoto)란 가명의 프로그래머(또는 집단)에 의해 2009년 처음으로 도입

— 1998년 프로그래머 Wei Dai가 제안했던 암호화화폐(cryptocurrency)의 개념을 처음으로 실현

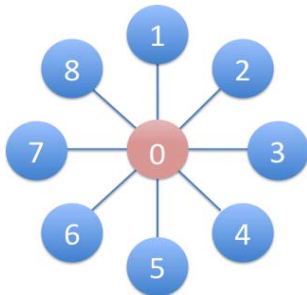
- 암호화화폐란 화폐의 발행 및 거래 승인 과정에서 암호화기술(cryptography)을 사용하는 화폐시스템을 말하며 비트코인 이외에도 Litecoin, PPcoin 및 Namecoin 등을 포함

— 중앙기관의 개입을 배제하기 위해 클라이언트·서버 모델 대신 P2P(Peer-To-Peer) 네트워크 기술을 이용하여 거래 기록의 보관, 거래의 최종 승인 등을 네트워크 참여자들이 공동으로 수행

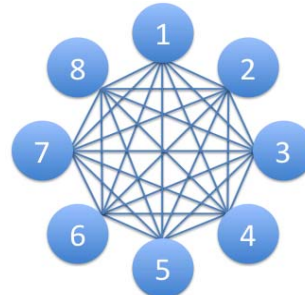
- 네트워크 구성 방식의 일종으로 정보나 자원을 일괄적으로 관리하고 필요한 서비스를 제공하는 서버(컴퓨터 또는 프로그램)와 서버에 자원 및 서비스를 요청하는 클라이언트로 이루어지며 인터넷뱅킹 등의 서비스에서 널리 사용됨
- 클라이언트나 서버의 개념 없이 동등한 참가자(peer nodes)들이 클라이언트와 서버의 역할을 동시에 수행하며, 데이터나 주변 장치 등을 공유하는 방식으로 주로 파일 공유 등의 서비스에 활용됨

#### 네트워크 개념도

(클라이언트·서버 모델)



(P2P 네트워크 모델)





— 자체적인 화폐단위로 비트코인(BTC로 표시)을 사용하며 보조단위로 는 밀리코인(0.001BTC, mBTC로 표시), 마이크로코인(0.000001BTC,  $\mu$ BTC로 표시) 및 사토시(0.00000001BTC, satoshi로 표시, 최소단위)가 있음

□ 비트코인 거래자들은 은행계좌에 해당하는 공개주소(public address)를 활용하여 비트코인을 이체

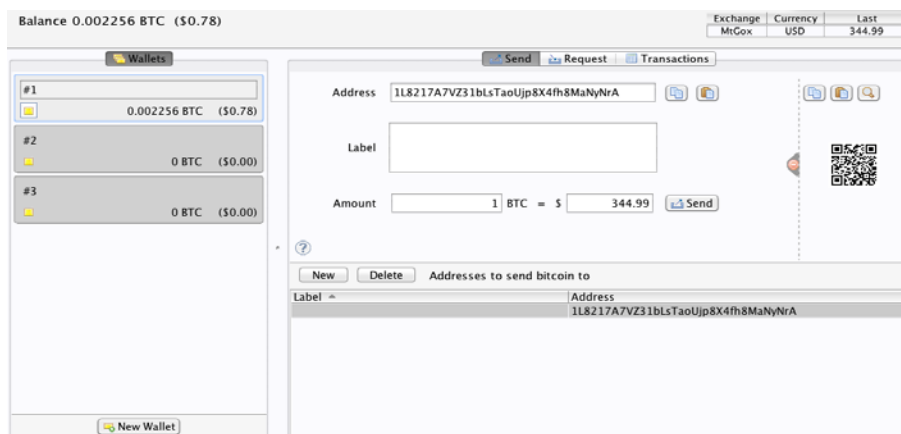
— 이용자는 지갑프로그램을 통해 무수히 많은 공개주소를 만들 수 있으며 공개주소와 함께 비밀키(private key)도 동시에 생성

■ 비트코인 지갑(wallet)은 사용자가 보유 비트코인을 확인하고 이체거래를 실시할 수 있도록 고안된 프로그램으로 MultiBit, Bitcoin-Qt 등 PC용 지갑 및 Coinbase 등 모바일 지갑 등이 사용됨

○ 공개주소는 임의로 생성되는 문자와 숫자의 조합으로 계좌번호와 같은 기능을 수행하며 비트코인 잔액을 표시

○ 비밀키는 일종의 비밀번호로서 이용자의 지갑프로그램에 저장되며 비트코인 이체거래시 입력되어야 함

### 비트코인 지갑 프로그램 화면



— 한편 비트코인은 인터넷뱅킹 등과 달리 계좌정보를 확인하여 거래를 승인하고 기록을 보관하는 중앙 처리기관이 존재하지 않음

○ 대신 네트워크 참가자들이 거래를 승인하고 기록을 모두에게 공개

## 나. 현금, 전자화폐 및 유가증권과의 비교

□ **(현금과의 비교)** 현금의 지급·청산·결제의 전 과정을 거쳐야 거래가 완결되는 비현금 지급수단과 달리 지급만으로 거래가 종료

- 비트코인은 최종적인 가치를 지니며 지급거래 후 더 이상의 채권·채무관계가 남아있지 않다는 점에서 현금과 비슷
- 그러나 비트코인은 현금과 달리 물리적 실체 없이 전자화된 파일의 형태를 가지며 정부 또는 발행기관에 의해 가치가 보장되지 않고 비트코인 네트워크를 구성하는 사용자들에 의해서만 가치가 인정됨

□ **(전자화폐와의 비교)** 유럽연합(2009)은 전자화폐를 발행인에 대한 청구권으로 ① 화폐적 가치가 전자화된 형태로 저장되고 ② 발행금액에 상응하는 법정통화를 수취한 대가로 발행되며 ③ 발행기관 이외의 가맹점에서 사용할 수 있는 지급수단으로 정의

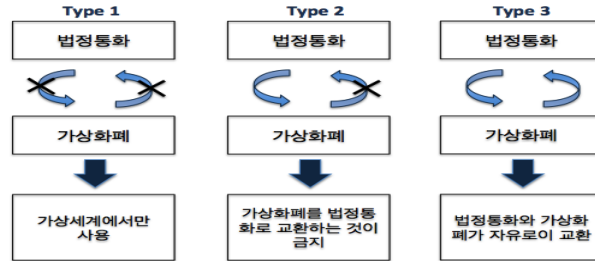
- 비트코인은 특정한 가치가 전자화된 형태로 저장되어 있고 온·오프라인 상점에서 사용될 수 있다는 점에서는 전자화폐와 유사
- 그러나 발행기관이 존재하지 않으며 법정통화를 수취한 대가가 아니라 미리 정해진 알고리즘에 따라 발행된다는 점에서 전자화폐와 다름
  - 또한 전자화폐와 달리 관련법의 규제를 받지 않으며 법정통화 단위(달러, 유로 등)로 표시되지 않고 자체적인 화폐 단위로 표시

□ **(가상화폐와의 비교)** ECB(2012)는 가상화폐를 ① 가상공간의 개발자에 의해 발행되고 ② 가상공간의 회원 사이에 지급수단으로 수수되며 ③ 법규에 의해 통제되지 않는 화폐로 정의

- 실제 법정통화와의 교환성을 기준으로 **Type 1**(폐쇄형), **Type 2**(일방형), **Type 3**(양방향)로 구분
  - **Type 1** : 가상세계의 활동을 통해서만 가상화폐를 획득할 수 있고 발행된 가상화폐는 가상세계에서만 사용 가능
  - **Type 2** : 법정통화로 가상화폐를 구매할 수는 있으나 가상화폐를 법정통화로 교환할 수는 없음

- Type 3 : 법정통화와 가상화폐간 교환이 자유롭게 이루어짐

### 가상화폐의 종류



자료: ECB(2012)

- 비트코인은 Linden Dollar\* 등 법정통화와 상호 교환되는 Type 3의 가상화폐와 비슷\*\*하지만 발행 및 거래승인을 담당하는 중앙기관이 없다는 점에서 큰 차이를 보임

- Linden Lab에서 개발한 가상세계 Second Life에서 사용되는 가상화폐
- ECB(2012)는 비트코인을 Type 3의 가상화폐로 간주

### 현금, 전자화폐, 가상화폐 및 비트코인 비교

	현금(법정통화)	전자화폐	가상화폐(Type1,2)	비트코인
화폐 형태	주화(금속) 또는 지폐(종이)	디지털	디지털	디지털
화폐 단위	법정통화	법정통화	가상화폐	가상화폐
적용 법규	○	○	x	x
사용처	모든 거래	가맹점	가상공간	가맹점
발행기관	중앙은행	금융기관	비금융기관	x
법정통화와의 교환성	-	법정통화로 충전, 잔액은 법정통화로 환급가능	가상화폐를 법정통화로 교환할 수 없음	법정통화와 자유로이 교환됨

- (유가증권과의 비교) 유가증권은 권리의 거래를 편리하게 하기 위해 무형의 권리를 증권에 결합한 증서를 의미

- 비트코인은 주식, 채권 등과 같이 거래소를 통해 매매되고 있어 유가증권의 성격도 포함
- 그러나 유가증권은 지분증권 및 채무증권으로 구분되며 권리의 존재를 전제로 하는 만큼 권리관계가 없는 비트코인은 유가증권으로 해석되기 어려움
- 더욱이 유가증권은 유가증권법정주의에 의해 법으로 그 종류와 내용을 제한하기 때문에 비트코인이 유가증권으로 인정되기 위해서는 명시적인 법률 규정이 필요

- 비트코인 시스템을 구성하는 주요 부문으로는 채굴자, 거래소, 비트코인을 받는 온·오프라인 가맹점, 비트코인과 관련된 금융서비스 제공기관 등이 있음

### 가. 채굴자

- 비트코인은 P2P 네트워크상에서 암호화 알고리즘에 따라 채굴(mining)될 수 있음

- 채굴이란 비트코인의 계좌이체 거래기록 집합인 블록(block)을 승인하는 작업을 말하며 채굴에 성공하는 참가자에게는 시스템 운영에 기여한 대가로 비트코인이 새로 발행되어 주어짐

- 채굴이 성공(평균적으로 매번 약 10분 정도 소요)하면 채굴과정에서 이용된 거래기록들이 승인되며 채굴이 성공하기 전까지의 거래는 미확정 상태를 지속

- 거래 미확정 상태에서 수취자는 계좌이체로 받은 비트코인을 사용할 수 없음

- 채굴자들은 새로운 블록을 형성하기 위해 비트코인 시스템이 요구하는 특정한 작업을 수행

- 채굴자들은 직전 블록의 해시값<sup>■</sup>, 미승인 거래기록(암호화된 메시지) 및 논스(nonce)라 불리는 임의의 숫자를 입력하여 새로운 블록의 해시값을 계산

- 해시값(hash value)이란 해시함수를 이용해 임의의 데이터로부터 고정된 길이의 난수(일종의 짧은 전자지문)를 만들어 내는 방법을 말함

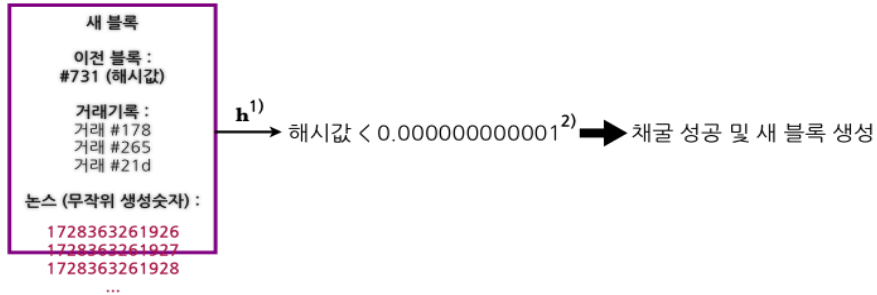
- 논스를 다르게 입력하면서 계산된 해시값이 시스템의 요구조건, 즉 설정된 임계치보다 낮아야 한다는 조건을 충족하는지 확인

- 시스템의 임계치는 채굴자들이 많아질수록 난이도가 높게 조정됨

- 채굴자중 한명이 조건을 충족하는 해시값을 구하면 거래 블록이 형성되고 보상으로 비트코인(현재 25BTC) 이 지급됨

- 현재 초당 7천조번의 해시값을 계산할 수 있는 기기(또는 집단)로 약 10분 정도에 한 개의 블록을 승인할 수 있으며 일반적인 PC CPU(20Mh/s 미만)의 경우 10년 이상 소요

## 채굴



- 주: 1) 해시함수  
2) 네트워크의 컴퓨팅 파워를 고려하여 자동 조정

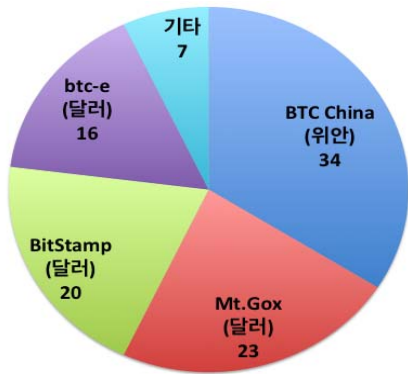
- 채굴자들의 성공보수가 약 4년마다 절반으로 줄어들도록 설계되어 있어 총 발행량은 2,100만BTC로 제한됨
- 전체 채굴량이 2,100만BTC에 근접하여 비트코인이 추가로 발행되지 않는 경우 채굴자들은 계좌이체 거래자들로부터 수수료만을 수취
  - 거래기록이 승인되면 거래자들은 거래금액과 상관없이 건당 0.0001BTC 정도의 수수료를 채굴자에게 지급

## 나. 거래소

- 비트코인 이용자들은 채굴 방법 이외에도 유가증권 또는 외환의 경우와 같이 거래소 구매 방법으로 비트코인을 획득할 수 있음
  - 거래소는 비트코인 구매자와 판매자를 중개하는 업무를 수행하는데 수요와 공급의 상대적인 규모에 의해 달러, 유로, 위안화 등 법정통화와의 교환비율이 정해짐
- 대표적인 거래소로 BTC China(중국), Mt.Gox(일본), bitcoin.de(독일) 등이 있으며 국내에서는 Korbit이 2013.7월부터 비트코인 원화거래를 중개하기 시작

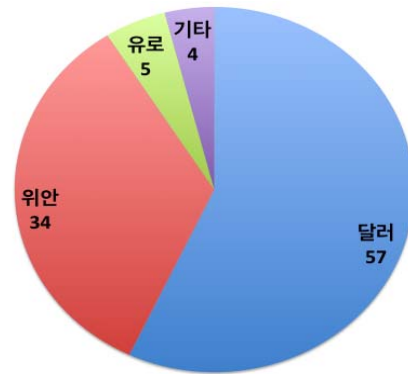
거래소 시장점유율<sup>1)</sup>

(단위: %)



통화별 거래비중<sup>1)</sup>

(단위: %)



주: 1) 2013.12.2일 기준

자료: www.bitcoincharts.com

□ 국내 비트코인 거래소 **Korbit**은 2013.7월 설립되어 비트코인 원화 거래 중개서비스를 제공

— **Korbit**은 회원에게 비트코인 및 원화 두 가지 계좌를 개설하도록 하고 비트코인 또는 원화의 예치 금액 범위 내에서 매매주문을 중개

○ 호가가 일치하는 매수 및 매도 주문이 나오면 거래를 성립시키고 회원 계좌간 대체 방식으로 비트코인 및 원화를 이체

○ **Korbit**은 거래수수료로 매수자 및 매도자에 대해 각각 1%를 징구 (비트코인 매수자에 대해서는 비트코인으로 수수료 징구)

— 한편 **Korbit**은 고객이 비트코인의 도난·분실 등에 대비할 수 있도록 비트코인 보관 서비스도 제공

#### 다. 가맹점

□ 비트코인을 지급수단으로 활용할 수 있는 가맹점은 아직 많지 않으나 점차 증가하는 추세

— 주로 **WordPress, Wikileaks, The Pirate Bay**와 같은 온라인 사이트들이 지불수단으로 비트코인을 수취하고 있으며 미국과 유럽을 중심으로 오프라인 가맹점도 점차 늘어나고 있음

- 높은 익명성, 편리한 자금이체, 낮은 수수료 및 상승중인 비트코인 가격 등 경제적인 이유와 비트코인에 관심을 가진 사람들에게 홍보 효과를 낼 수 있다는 점이 가맹점 증가의 원인으로 지적
- Bitpay와 같이 상점들이 비트코인을 지급수단으로 수취할 수 있도록 지급결제 솔루션을 제공하는 업체도 등장

**비트코인을 지급수단으로 인정하는 주요 온라인 서비스**

명 칭	서비스 내용	비트코인 수납 시기
WordPress	블로그 서비스	2012.11월
The Pirate Bay	P2P 파일공유 서비스	2013. 4월
Reddit	소셜 뉴스 서비스	2013. 2월
The Internet Archive	웹사이트 라이브러리 서비스	2013. 2월
OkCupid	소셜 네트워크 서비스	2013. 4월

자료: Forbes

- 또한 선불카드 판매 서비스인 Gyft 등이 지급수단으로 비트코인을 인정함에 따라 비트코인을 보유한 소비자가 Amazon, Groupon 등의 선불카드 가맹점을 이용할 수 있게 됨

**라. 비트코인 관련 금융상품**

□ 비트코인 예금·대출, 옵션, 선물 등 기존의 금융서비스와 유사한 상품도 출시

- 다만 대부분 사업 초기단계로 거래가 많지 않은 상황이며 향후 활성화 여부도 불확실

**비트코인 관련 금융상품**

유 형	서비스명	내 용
예금	Bitdeposit, flexcoin	비트코인 예금 이자 지급
대출	Bitbond.net, BTCJam, Bitdeposit.net	P2P 방식 비트코인 대출
옵션	BTClevels, BTCOracle, MPOE	비트코인 옵션
선물	ICBIT, MPEX	비트코인, 금, 석유 등 선물 거래

자료: Wikipedia

**비트코인 예금**

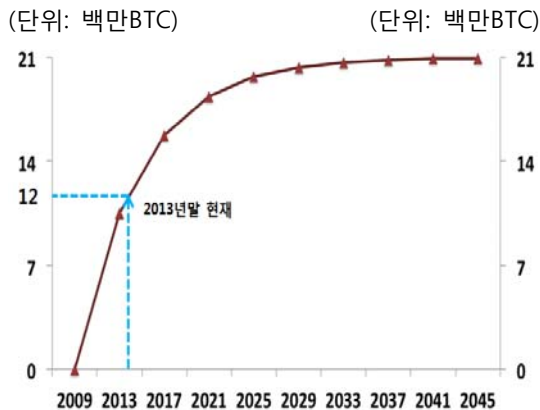
The screenshot shows the Bit Deposit website interface. At the top, there is a navigation menu with links for Home, Products, Startup funding, About, Contact, and Login. The main heading reads "Bitcoins grow Here!" followed by the text "We pay extremely high interest rates: 19.3% on 1 year deposits!". A prominent green button says "Make a deposit today". Below this, it states "35108.243 BTC currently in deposits." There are three columns of text: "Bitcoin friendly" (We only invest in bitcoin related things...), "Premature withdrawal possible" (You may withdraw Bitcoins from your deposit before the deposit term ended...), and "Secure" (Your bitcoins are fully safe against hackers or data loss...).

## 가. 비트코인 발행

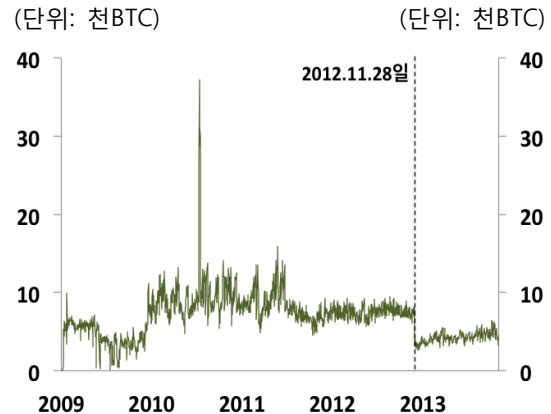
□ 비트코인은 2009.1.3일 개발자인 사토시 나카모토에 의해 처음으로 채굴이 이루어짐

— 최초의 채굴 이후 약 4년간 블록당 50BTC가 지급되었으나 2012.11.28일부터 25BTC가 지급

— 2013.11월말 현재 총 발행량은 약 1,200만BTC 정도이며 일평균 발행량은 2012.11.28일 전후로 나누어 각각 7,367BTC 및 4,241BTC 수준

비트코인 발행잔액<sup>1)</sup>

비트코인 일평균 발행량



주: 1) 10분당 1블록이 생성된다는 가정하에 계산된 발행잔액  
자료: www.blockchain.info

□ 비트코인 도입 초기에는 일반적인 개인용 컴퓨터의 연산능력으로도 채굴이 가능하였으나 네트워크의 규모가 커지고 채굴의 난이도가 상승함에 따라 전문적인 채굴용 장비가 개발되어 활용

- 채굴용 장비 판매업체는 Avalon, Butterfly Labs 등이 대표적이며 몇만원에 살 수 있는 USB 채굴기부터 수억원에 달하는 고가 장비 등 다양한 장비가 이용되고 있음



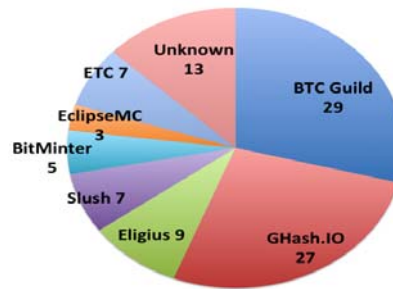
- 현재 여러 사람들이 네트워크를 구성하여 공동으로 채굴을 한 뒤 보상을 나누어 가지는 마이닝 풀(mining pool)이 보편적인 채굴 방법으로 채택되고 있음

### 국가별 비트코인 마이닝 풀

국가	마이닝 풀
미 국	Bitcoin Miner, Eclipse Mining Consortium, Ozcoin, BitClockers, BTC Guild, Multipool, Bitcoin Mining.Co 등
유 럽	Eclipse Mining Consortium, Ozcoin, BitClocker, BTC Guild, BTC Oxygen, BTCmow 등
독 일	50BTC, btcmp.com, Deepbit 등
네덜란드	GHash.IO 등
프 랑 스	Slush 등
캐 나 다	BTC Guild 등
러 시 아	50BTC, pool.itzod.ru 등

### 비트코인 마이닝 풀 점유율<sup>1)</sup>

(단위: %)



주: 1) 2013.11.29일~12.2일 동안의 채굴 비중  
 자료: www.blockchain.info

자료: Wikipedia

## 나. 비트코인 유통

□ 비트코인의 이체거래(발굴 포함)는 일평균 기준으로 2011년초 약 52,000BTC에서 2013.11월 약 266,000BTC로 급증

- 이 중 거래소를 통한 비트코인 달러매매(일평균 기준)는 2011년초 10,000BTC 정도에서 2013.11월 37,000BTC로 증가

□ 달러대비 환율은 2011년 1월중 1BTC당 약 0.05달러 수준에서 2013.11월말 1,200달러까지 상승하였으나 최근 각국의 규제 움직임이 본격화하면서 높은 변동성을 시현

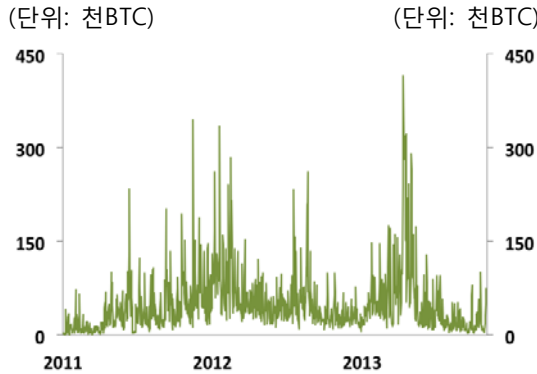
- 2013.4월 키프로스 정부가 구제금융의 전제조건으로 은행예금에 대한 일괄적 과세방안을 확정하자 대체 투자자산으로서 비트코인에 대한 인기가 높아지며 1BTC당 가격이 266달러까지 상승

- 11월에는 미국 의회 청문회에서 버냉키 연준의장이 비트코인의 장래성을 인정하는 취지의 서한<sup>■</sup>을 보낸 것으로 알려짐에 따라 가격이 사상 최고 수준을 기록

■ 당시 버냉키 연준의장의 서한 내용은 다소 왜곡되어 알려졌는데 상세 내용은 IV장 해외 논의 및 대응 사례 참조

- 12월초 중국인민은행이 투기성과 가격변동성을 우려하여 금융기관의 비트코인 업무취급을 금지시키고 프랑스, 네덜란드, 노르웨이 정책당국의 부정적 언급이 이어지면서 600달러대까지 급락하기도 하였으나 12.16일 현재 900달러 수준을 기록

**비트코인 거래량<sup>1)</sup>**



주: 1) 달러 거래량 기준  
자료: www.blockchain.info,

**비트코인의 달러 가격<sup>2)</sup>**



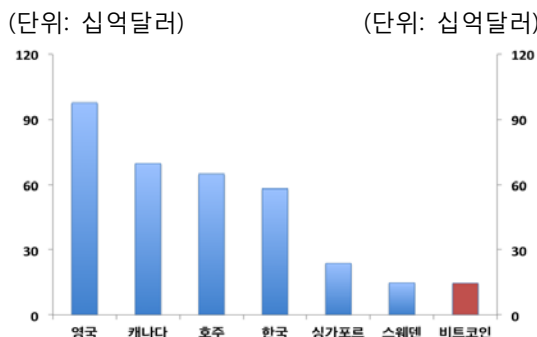
주: 1) Mt.Gox 오후 6시 기준  
자료: www.bitcoincharts.com

□ 비트코인 발행잔액의 총 시장가치는 크게 늘고 있으나 아직 주요국 법정통화에 비해 작은 수준

- 2013.1.1일부터 11.30일까지 총 시장가치는 약 1.4억달러에서 145억 달러로 100배 이상 증가

- 2013.11월말 현재 비트코인의 발행잔액은 약 145억달러로 우리나라의 화폐발행잔액의 약 25% 수준

**주요국<sup>1)</sup> 화폐발행잔액과 비트코인 발행잔액**



주: 1) 2012년말 기준(한국은 2013.10월말)  
자료: CPSS(2013), www.blockchain.info

**비트코인 총 시장가치**



### Ⅲ 주요 제약점

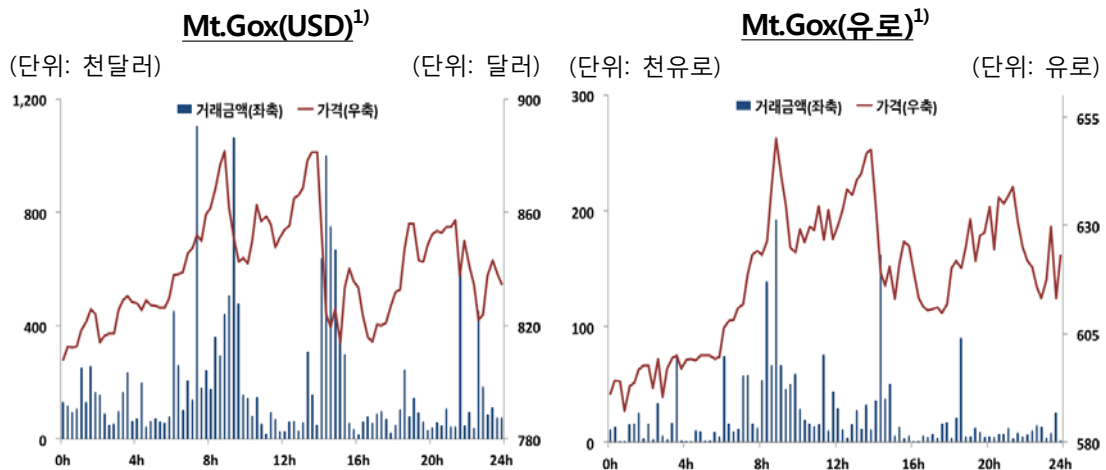
- 일부에서는 비트코인이 이론적으로는 물리적 공간의 제약 없이 자금이체가 가능하고 거래수수료가 낮으며 다양한 방식의 거래가 가능하다는 점에서 지급거래수단으로 발전할 가능성이 있다고 주장
  - 그러나 현실적으로 비트코인이 앞으로도 계속 성장하는 데는 많은 한계가 있는 만큼 아래에서 주요 제약점을 점검하기로 함
- **(취약한 보안성)** 비트코인 시스템은 블록체인 등을 통해 보안성을 확보하고 있지만 비트코인을 사용하는 개인을 보호할 수 있는 특별한 보안 체계를 보유하고 있지 않음
  - <부록> 비트코인 거래 절차 참조
  - 인터넷뱅킹 등 금융서비스가 공인인증서 등의 보안수단을 구비하고 있는 것과 달리 비트코인은 사용자 보호장치가 없어 해킹 공격에 취약할 수 있으며 중앙관리기관의 부재로 해킹 피해 발생시 복원할 방법이 없음
  - 실제 고객 계좌를 집중 보관하고 있는 거래소 및 온라인 지갑서비스업체에 대한 해킹 공격으로 다수의 피해 사례가 발생

#### 비트코인 관련 해킹 피해 사례

시기	서비스명	서비스 종류	피해금액
2011. 6월	Mt.Gox	거래소	875만달러
2011. 8월	MyBitcoin	거래소	80만달러
2012. 9월	Bitfloor	거래소	25만달러
2013. 4월	Instawallet	지갑서비스	460만달러
2013.10월	Inputs.io	지갑서비스	100만달러
2013.10월	Global Bond Limited	거래소	500만달러

자료: Wikipedia

- **(가격 변동성)** 비트코인이 교환의 매개로서 활용되기 위해서는 안정적인 가격 유지가 전제되어야 하지만 최근 투기적 거래로 인해 비트코인 가격이 일중에도 급격하게 변동
  - 2013.11월중에는 교환통화대비 가격이 일평균 10% 내외의 변동폭을 기록

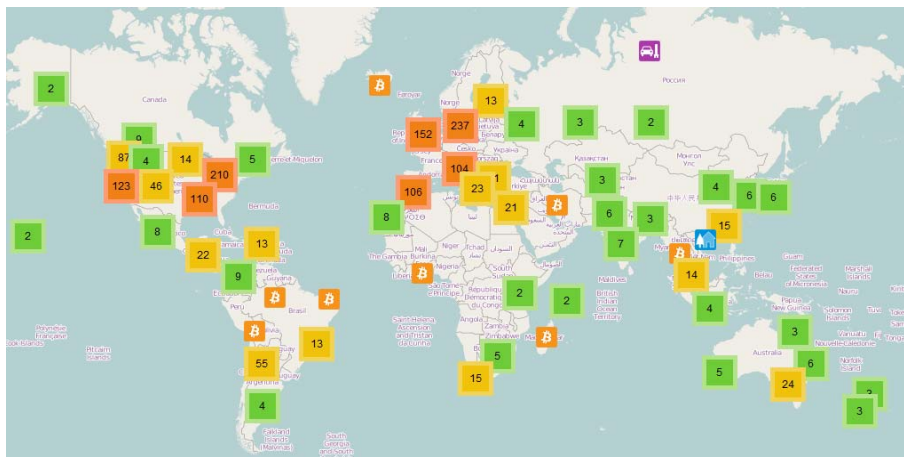


주: 1) 2013.11.23일 기준  
 자료: www.bitcoincharts.com

□ **(제한적 수용성)** 최근 비트코인 가맹점이 늘어나고 있으나 거래규모는 다른 지급수단 또는 금융상품에 비해 극히 미미한 수준이며 가치를 보증하는 발행기관이 없어 가맹점 확산은 제한적일 것으로 예상

— 비트코인 가맹점은 전세계적으로 1,300여곳으로 알려져 있으나 대부분 거래규모가 확인되지 않고 있으며 이중 다수가 홍보 목적으로 거래를 허용

**비트코인 가맹점 분포<sup>1)</sup>**



주: 1) 2013.11월말 기준  
 자료: coinmap.org

□ **(긴 거래 승인시간)** 비트코인을 이용한 지급거래는 채굴 과정을 거쳐 승인되므로 최종 결제까지 10분 내외의 시간이 소요

- 대중교통과 같이 빠른 거래 승인이 요구되는 오프라인 거래에서 사용되기 어려우며, 빠른 거래를 위해 최종 승인 이전에 재화 또는 용역을 제공할 경우 가맹점은 신용리스크에 노출

□ **(채굴 유인의 감소)** 채굴자들의 수가 증가함에 따라 채굴의 난이도는 지속적으로 상승하는 반면 채굴자들에게 보상으로 지급되는 비트코인의 양은 계속 줄어들도록 설계되어 있어 시간이 지날수록 채산성이 감소

- 새로 발행되는 비트코인이 채굴자들에게 충분한 보상이 되지 못하는 수준에 이르면 비트코인 거래 수수료가 크게 상승하거나 거래승인이 지연될 가능성
  - 시스템이 제공하는 건당 기본수수료는 0.0001BTC의 정도이지만 사용자는 수수료 수준을 조정할 수 있으며 채굴자들도 블록에 포함되는 거래를 선택할 수 있음

□ **(지급거래의 높은 사회적 비용)** 비트코인이 개별 사용자의 거래 비용은 낮출 수 있다고 하지만 채굴 과정에는 엄청난 양의 전기를 사용하는 컴퓨터 연산이 필요하므로 사회적인 거래비용은 낮지 않음

- 채굴자들의 일평균 전기사용량, 일평균 거래건수 등을 고려하면 건당 평균 거래비용은 2013.11월중 일평균 약 2.57달러 수준이며 채굴 난이도가 상승할수록 거래비용은 더욱 증가
  - Blockahin.info에 따르면 2013.11월중 채굴자들의 일평균 해시 계산량은 약 464만Gh/s이며 1Gh/s를 계산하는 데 시간당 10w의 전기를 소모하고 1kwh당 15센트의 전기요금이 부과된다고 가정하면 일평균 전기사용금액은 16.7만 달러로 추산. 11월중 일평균 비트코인 거래건수는 약 6.5만건이므로 건당 평균 거래비용은 2.57달러(=167,000/65,000) 수준
- 소액지급수단의 사회적 비용에 관한 ECB의 연구와 비교하면, 비트코인 거래비용은 수표, 신용카드보다 낮으나 현금보다는 4배, 직불카드보다는 2.5배 이상 높은 수준

지급수단별 건당 거래비용<sup>1)</sup>

(단위: 달러)	현금	수표	카드	(직불카드)	(신용카드)	자동이체	계좌이체	비트코인
건당 거래비용	0.57	4.79	1.34	0.95	3.22	1.71	2.59	2.57

주: 1) 비트코인외 1유로당 1.35달러의 환율 적용  
 자료: ECB(2012), www.blockchain.info

□ (정보격차의 심화) 일부에서는 비트코인이 은행계좌 등이 없는 금융 소외계층에게 금융서비스를 제공하는 **financial inclusion**의 의미가 있다고 주장하지만 금융소외계층이 일반적으로 정보기술에 대한 접근성 및 이해가 높지 않다는 점을 고려하면 비트코인이 오히려 정보격차(digital divide)를 심화시킬 우려

— 비트코인을 사용하기 위해서는 컴퓨터를 이용한 인터넷 접속이 필수적이므로 컴퓨터 활용능력이 부족하거나 인터넷 접속이 어려운 취약계층은 비트코인을 사용하기 어려움

## IV 해외 논의 및 대응 사례

- 비트코인은 거래의 익명성을 보장하고 별다른 규제가 적용되지 않는다는 점에서 자금세탁, 탈세, 마약 및 무기 밀매 등 불법적인 거래에 활용될 수 있다는 우려가 제기
  - 마약 및 무기 밀거래 사이트인 실크로드<sup>1)</sup>는 지급수단으로 비트코인만을 허용
- 또한 비트코인을 이용한 투기성 금융상품의 등장으로 소비자 피해가 발생하면서 소비자 보호차원에서 비트코인 관련 서비스를 규제할 필요성도 대두
- 이러한 상황에서 비트코인 사용이 비교적 활성화된 미국 및 유럽을 중심으로 비트코인의 법적 성격을 규정하는 한편 비트코인 관련 서비스를 규제하고자 하는 움직임이 나타남
  - 다만, 비트코인의 법적 성격이나 서비스 규제에 관한 각국 정부의 입장은 다소 차이를 보이고 있음

### (미국 Silk Road 사건)

- 2011.6월 미국 민주당 상원의원 **Charles Schumer** 등은 사법당국에 비트코인을 지급수단으로 사용하는 마약 및 무기 밀거래 사이트 실크로드(Silk Road)<sup>2)</sup>에 대한 규제를 촉구
  - 2013.10월 미국 사법당국은 실크로드 운영자를 체포하고 사이트를 폐쇄하는 한편 운영자가 보유하고 있던 360만달러 상당의 비트코인도 압수
- **Schumer** 의원은 비트코인을 자금의 원천 및 마약 구매자와 판매자를 숨기기 위한 온라인 형태의 자금세탁(an online form of money laundering)으로 묘사
- 이와 관련하여 2013.3월 미국 재무부 산하 금융정보분석기구인 FinCEN(Financial Crime Enforcement Network)은 가상화폐 거래소를 자금이체기관(money transmitter)으로 파악하고 자금세탁 방지 의무를 부과할 것이라고 발표<sup>3)</sup>

- *A user of virtual currency is not an MSB(Money Services Business) under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and record keeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter. (FinCEN Guidance 2013.3.18.)*

— 비트코인 거래소 Mt.Gox는 2013.5월부터 사진이 부착된 신분증, 거주증명서 등을 이용해 계좌주의 신원을 확인하는 등 자금세탁 방지 의무를 이행하였으며 6월에는 FinCEN으로부터 자금이체업 허가를 받음

### (미국 금융사기 소송)

□ SEC(Securities Exchanges Commision)는 2013.7월 Bitcoin Savings & Trust (BTCST)의 설립자인 Trenton Shavers를 Ponzi Scheme<sup>■</sup> 운영 혐의로 기소

- 신규 투자자가 지불한 돈으로 기존 투자자에게 투자 수익을 제공하는 다단계 금융사기 유형을 말함. Trenton Shavers는 비트코인 거래소간 차익 거래를 통해 투자자들에게 하루 1%의 이자를 지급하겠다고 약속하고 약 700,000BTC를 유치

— Shavers는 변론과정에서 SEC는 화폐를 통한 투자계약(investment of money)에 대해서만 규제할 수 있으며 비트코인은 국가가 인정 한 화폐(money)가 아니기 때문에 기소권이 없다고 주장

— 2013.8월 텍사스 연방판사 Amos Mazzat는 이 사건에 대해 비트코인을 통화(currency) 또는 화폐 형태(form of money)로 보는 것이 타당하며 SEC의 기소는 유효하다고 판단

- *It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money”(U.S. Eastern District of Texas Court, Memorandum Opinion 2013.8.6.)*

— 일부에서는 이번 판결을 미국 정부가 비트코인을 일종의 화폐로 인정한 사례로 파악하기도 하지만 텍사스 연방판사의 판단은 항소심 또는 새로운 사건에서 바뀔 수 있다는 견해도 공존



## (독일 정부의 규제)

- 2013.7월 독일 연방금융감독기구(BaFin)는 규제 가이드라인을 수정하면서 비트코인을 일종의 금융상품(financial instruments)으로 판단
  - 이에 따라 2013.8월부터 독일 소재 비트코인 거래소 bitcoin.de는 BaFIN으로부터 금융중개기관(financial intermediary) 허가를 받았으며 Fidor Bank와 파트너십<sup>▪</sup>을 체결
    - 파트너십 체결로 고객들은 Fidor Bank가 제공하는 계좌를 이용해 실시간으로 bitcoin.de에서 비트코인 매매를 할 수 있게 됨
  - 비트코인이 금융상품으로 인정됨에 따라 비트코인을 1년 미만 보유하면서 자본 이득을 실현한 사람에게는 자본이득세가 부과
    - *This means that, like stocks or shares, any profit from them(Bitcoin) is subject to Germany's capital gains tax, at 25pc - unless they are held for more than a year, according to German newspaper Frankfurter Allgemeine Zeitung.(The Telegraph 2013.8.19.)*

## (태국 및 중국의 대응)

- 금년 7월 태국 중앙은행은 비트코인이 환차익을 위한 투기수단일 수 있다는 이유로 비트코인 거래소(Bitcoin Co. Ltd.)의 등록을 거부
  - *For now we(Bank of Thailand) asked they(Bitcoin Co. Ltd.) not involve themselves with the baht because what they do may be a way to speculate on the exchange rate. (Bank of Thailand, Governor Prasarn Trairatvorakul, Asian Correspondent, 2013.7.31.)*
- 한편 중국 인민은행 등 정책당국은 비트코인이 투기성과 가치변동성이 높은 점을 들어 금융기관의 비트코인 업무취급을 금지시키는 등 부정적인 입장
  - 12.5일 인민은행 등<sup>▪</sup>은 「비트코인 관련 리스크 방지 통지(關於防范比特幣風險的通知)」를 통해 금융기관의 비트코인 관련 업무 취급을 금지
    - 인민은행, 공업정보화부, 은감회, 증감회, 보감회
  - 통지문에 따르면 비트코인은 화폐 대용물(monetary equivalent)로서의 법적인 지위를 가지지 않으며 현재 중국 금융시스템을 위협하고 있지는 않으나 정책당국은 위험요소를 예의 주시하고 있음

- 홍콩특구 정부재정국 **Ceng Junhua** 국장은 비트코인은 투기성향이 높으므로 투자하는 개인이나 비트코인을 받는 상점은 모두 주의가 필요하다고 주장(중신사, 12.1)
  - **Ceng** 국장은 거래기록, 결제잔액 등 모든 자료가 공개되지만 동일인 개설 계좌수가 무한하고 계좌소유주에 대한 신분확인이 불가능한 데다 동일인이 사고 파는 투기적 불법행위(自買自賣)를 막을 수 없는 한계가 있다고 언급

### (미국 비트코인 청문회)

- 미 상원은 지난 **11.18**일 법무부, 국토안전부, 재무부 관계자 등을 대상으로 청문회를 개최하였으며, 동 청문회는 비트코인에 대한 사실 확인(fact-finding)에 주안점을 두고 진행
  - **Tom Carper** 상원의원은 비트코인을 초기 인터넷 및 **1980**년대 신용카드 붐(boom)과 비교하는 등 비트코인의 혁신성을 강조하면서 정책당국이 새로운 규제체계를 확립하거나 뚜렷한 정책적 견해를 제시함으로써 비트코인과 관련한 불확실성을 해소할 필요가 있다고 주장
  - 대부분의 정부 관계자는 비트코인이 합법적인 금융서비스(financial service)이며, 현재로서는 비트코인을 이용한 범죄를 우려하여 추가적인 규제책을 마련하고 있지 않다고 증언
  - 비트코인 재단(Bitcoin Foundation) 관계자는 은행산업이 취약한 국가에서 비트코인에 대한 수요가 크게 증가하고 있으며, 미국 내에서는 캘리포니아, 조지아 주가 비트코인의 상용화를 주도하고 있다고 주장
- 또한 버냉키 의장은 의회 청문회에 제출한 서한에서 가상화폐는 전자화폐(electronic money)의 한 형태로서 이와 같은 지급수단 혁신이 법 집행 및 감독 업무에 리스크를 초래할 수 있지만 효율적이고 안전한 지급결제시스템으로의 발전을 촉진한다면 장기적으로는 성공할 가능성이 있다고(may hold long-term promise) 언급

- 미 연준은 가상화폐의 발전 및 지급결제시스템의 혁신 등에 대해 모니터링하고 있으나 지급수단 혁신이나 발행주체에 대해 전반적인 규제 및 감독 권한을 가지고 있는 것은 아님
- 연준은 감독대상 은행 기관이 발행, 청산 및 결제한 가상화폐에 국한하여 규제 및 감독을 할 수 있으며 필요한 경우 가상화폐 등 전자현금(electronic cash) 이슈에 대해 정부와 공조할 방침

□ **Bloomberg**는 청문회 직후 기사에서 비트코인이 일종의 금융서비스로서 인정받게 되었지만 실패한 혁신으로 끝날 수 있다고 전망

- 버냉키 의장이 비트코인을 특징하여 “장기적인 성공” 가능성을 이야기 한 것이 아니라 **financial inclusion** 관점에서 소비자, 특히 취약계층에 도움이 될 수 있는 가상화폐 전반에 대해서 긍정적인 입장을 나타낸 것임
- 아직까지 비트코인은 현금 또는 신용카드와 비교하여 지급수단으로서의 우월성이 명확하게 드러나지 않고 있을 뿐만 아니라, 보안 취약성, 디플레이션 유발 가능성, 불안정한 인프라 등 많은 문제점을 가지고 있음

## V 시사점

---

- **성장 요인** : 비트코인은 물리적 공간의 제약 없이 자금이체가 가능하고 거래수수료가 낮으며 다양한 방식의 거래가 가능하다는 점에서 이론적으로는 지급거래수단으로 발전할 가능성
- **주요 한계** : 그러나 여러 가지 한계로 인해 이론적 성장 가능성이 실현되기는 어려울 것으로 판단
  - **(취약한 보안성)** 비트코인 개인사용자 또는 거래소에 대한 해킹 사례가 늘어나고 있는 가운데 별다른 보안 대책은 마련되고 있지 않음
  - **(가격 변동성)** 투기적 거래로 인해 비트코인 가치가 급격하게 변동하고 있어 비트코인이 가까운 장래에 보편적인 교환의 매개로 활용될 가능성은 낮음
    - 비트코인은 내재적 가치(**intrinsic value**)가 없기 때문에 17세기 네덜란드에서 발생한 튜립버블과 같은 투기적 수요에 쉽게 노출될 우려
  - **(제한적 수용성)** 최근 비트코인 가맹점이 늘어나고 있으나 거래규모는 다른 지급수단 또는 금융상품에 비해 극히 미미한 수준이며 가치를 보증하는 발행기관이 없어 가맹점 확산은 제한적일 것으로 예상
  - **(채굴유인 감소)** 채굴자들에게 보상으로 지급되는 비트코인의 양이 계속 줄어들도록 설계되어 있어 시간이 지날수록 채산성이 감소하면서 거래승인이 지연될 가능성
  - **(높은 사회적 비용)** 비트코인이 개별 사용자의 거래 비용은 낮출 수 있지만 채굴 과정에는 엄청난 양의 전기를 사용하는 컴퓨터 연산이 필요하므로 사회적인 거래비용은 낮지 않음
    - 채굴자들의 일평균 전기사용량, 거래건수 등을 고려하면 현재 전당 평균 거래비용은 약 2.57달러 수준

□ 비트코인은 지급거래의 효율성과 편의성을 제고할 수 있는 장점이 있으나 보안의 취약성, 가격의 급변성, 제한적 수용성 등으로 인해 앞으로 대안적인 지급수단으로 성장할지는 매우 불투명

— 다만 국가간 거래, 소액 거래 등 제한된 영역에서 활용되면서 해킹, 자금세탁 등 불법 행위가 시도될 수 있는 만큼 정부는 비트코인에 대한 규제 방안을 마련할 필요

○ 비트코인은 발행기관이나 중앙서버가 없는 분권화된(decentralized) 체계로서 네트워크 참가자들도 익명성을 보호받기 때문에 비트코인 발행을 금지하거나 채굴자들을 직접 규제하는 것은 어려움

○ 조직화·기업화된 형태의 비트코인 서비스 또는 대규모의 상업적인 사용은 소비자 보호, 과세 및 불법행위 방지 등을 위해 적절한 규제체계 하에서 이루어지도록 하는 것이 바람직

— 또한 모든 거래는 네트워크를 통해 모두에게 공개되는 만큼 대규모 네트워크 데이터에 대한 분석능력을 확충

□ 한편 비트코인은 종전과 크게 다른 형태의 시도라는 점에서 새로운 패러다임의 확산이 경제에 미칠 영향에 대해 지속적인 관심을 기울일 필요

— 현재의 비트코인이 실패한 시도로 끝난다 하더라도 비트코인의 한계점 및 문제점을 개선한 새로운 방식의 가상화폐가 등장할 개연성이 있음

<부록>

비트코인 거래 절차

□ 비트코인 이용자는 상대방의 공개주소(public address)만 알면 손쉽게 자금을 이체할 수 있음

— 그러나 비트코인 시스템이 자금이체 거래의 유효성을 확인하고 거래를 최종 승인하는 과정에는 복잡한 수학적 장치들이 활용됨

○ 비트코인은 자금이체 거래가 실제 공개주소의 소유주에 의해 실시되었는지 확인하고 아울러 비트코인이 이중사용(double spending)되는 것을 방지할 필요

■ 특정 공개주소에 대응하는 비밀키를 가진 자가 해당 공개주소의 소유주

(실소유주 확인)

□ 비트코인은 전자서명(digital signature)을 활용하여 실제 공개주소의 소유주가 해당 주소로부터 자금을 이체하는 거래를 요청한 것인지 확인

— 공개주소에 나타난 비트코인 잔액은 해당 주소를 목적지로 지정한 과거 거래기록의 합으로 표시되는데 이들을 입력값(input)으로 사용하여 출금(output)을 요청하고 거래기록(암호화된 메시지)을 네트워크 참가자들에게 전파

■ 암호화된 거래기록은 채굴자들이 실소유주 여부를 확인하는 데 사용되며 수취인의 경우 자신의 비밀키를 입력하여 이체된 비트코인을 사용 가능

○ 아래 표에서 지급인의 공개주소 1은 합이 4BTC인 4개의 과거 거래기록을 보유하고 있으며 공개주소 2에 3.5 BTC를 이체

비트코인 잔액

<b>공개주소 1</b> (1L8217A7VZ31bLsTaoUjp8X4fh8MaNyNrA)	
거래 #238 : 주소 3 → 주소 1	0.95 BTC
거래 #ad2 : 주소 4 → 주소 1	1.15 BTC
거래 #782 : 주소 5 → 주소 1	0.90 BTC
거래 #1e9 : 주소 6 → 주소 1	1.00 BTC
<b>Balance : 4.00 BTC</b>	

비트코인 거래기록

거래 #9z7	
Input	Output
거래 #238	index 0 주소 1 → 주소 1 0.50 BTC
거래 #ad2	index 1 주소 1 → 주소 2 3.50 BTC
거래 #782	
거래 # 1e9	
4.00 BTC	4.00 BTC

— 지급인은 비트코인 이체시 거래기록에 전자서명을 첨부하는데 전자서명은 거래기록마다 다른 값으로 암호화

- 전자서명은 자신의 비밀키와 거래기록을 특정한 함수에 입력하여 생성

$$f(\text{비밀키}, \text{거래기록}) = \text{전자서명}$$

- 네트워크 참가자들은 지급인의 전자서명, 거래기록, 공개주소를 특정한 함수에 입력하면 실소유주 여부를 확인 가능

$$v(\text{전자서명}, \text{거래기록}, \text{공개주소}) = \text{참 또는 거짓}$$

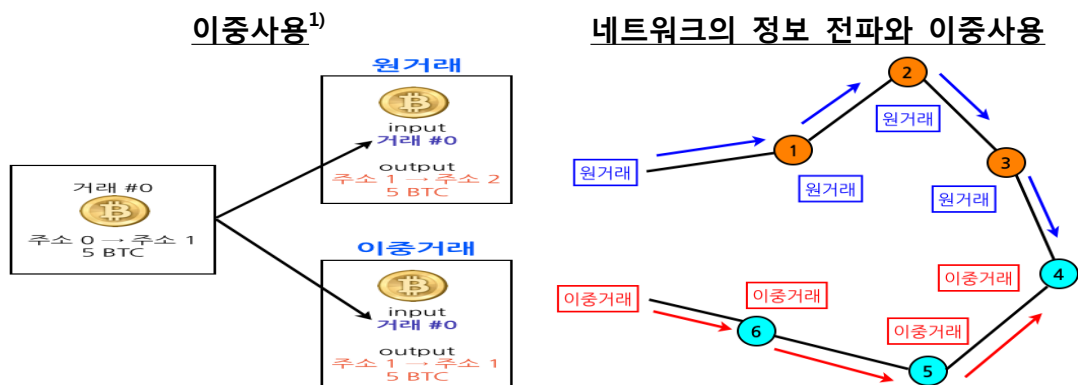
### (이중사용 방지 절차)

- 전자서명은 비트코인이 실제 소유주에 의해 사용되었는지에 대해서만 확인할 뿐 해당 비트코인이 이중사용 되었는지는 확인할 수 없음

- 이중사용(double spending)이란 동일한 거래기록을 입력값으로 하여 서로 다른 거래를 요청하는 행위

— 비트코인 네트워크에서 이중사용이 발생한 경우 참가자들은 먼저 이루어진 거래만을 유효한 것으로 인정

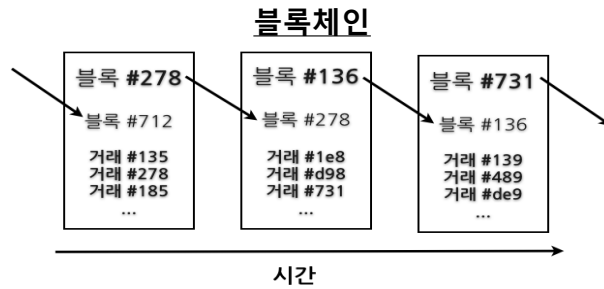
- 그런데 아래 그림에서 원거래가 먼저 이루어졌음에도 참가자 4, 5, 6은 이중사용 거래가 먼저 이루어진 것으로 인식



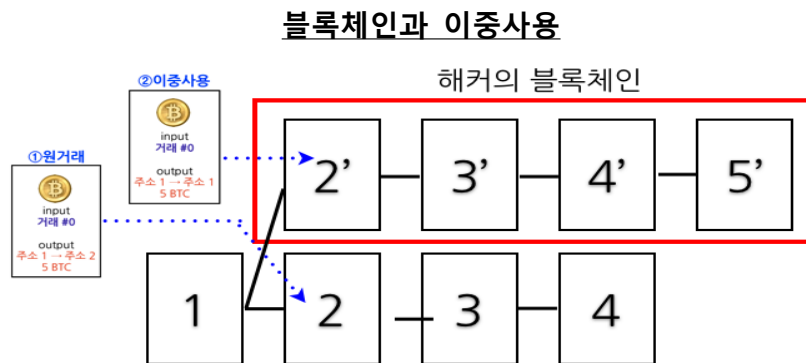
주: 1) 우측그림의 숫자 1~6은 참가자를 표시

- 비트코인 시스템은 특정 거래가 언제 이루어졌는지를 확정하기 위해 블록체인(blockchain)을 사용

- 블록체인은 약 10여분간의 거래기록을 포함하는 블록들을 시간 순서대로 연결한 것으로 모든 비트코인 거래기록을 시간 순서대로 기록하고 있는 일종의 장부(ledger)
- o 네트워크 참가자들은 채굴자에 의해 블록이 생성되면 동일한 블록에 포함된 거래들은 동일한 시각에 거래가 이루어진 것으로 간주



- 해커가 비트코인을 이중사용하기 위해서는 다른 모든 채굴자들보다 빠른 속도로 채굴에 성공하여야 함
- 비트코인 시스템은 복수의 블록체인이 존재할 경우 더 긴 블록체인을 유효한 것으로 인정하기 때문에 이중사용을 성공시키기 위해 해커는 기존의 블록체인보다 더 긴 블록체인을 만들 필요
- o 아래 그림에서 새로운 블록체인이 생성되면 블록2에 담겨 있던 원거래는 미승인 거래가 되어 유효하지 않은 거래로 간주됨



- 그러나 기존의 블록체인보다 더 긴 블록체인을 만들기 위해서는 네트워크의 모든 컴퓨터를 합한 것보다 더 많은 컴퓨터 연산능력이 필요하므로 이중사용은 사실상 어려움
- 이와 같이 네트워크 참가자에게 상당한 양의 컴퓨터 연산능력을 필요로 하는 작업을 요구함으로써 네트워크에 대한 악의적인 공격을 억제하는 방법을 작업증명(**proof of work**)이라고 함



## <참고 문헌>

- 김태오, “가상화폐의 이용현황과 시사점”, 지급결제와 정보기술 제53호2013
- Aleksander Berentsen, “Monetary Policy Implications of Digital Money”, Munich Personal RePEc Archive, 1997
- Christian Decker and Roger Wattenhofe, “Information Propagation in the Bitcoin Network”, 13-th IEEE International Conference on Peer-to-Peer Computing, 2013
- Cozemi Catalina Caloian Florentin, “The Bitcoin Economy, An Anti - Crisis Remedy?”, Revisita Economica, 2012
- ECB, “The Social and Private Costs of Retail Payment instruments: A European Perspective”, 2012
- \_\_\_\_\_, “Virtual Currency Schemes”, 2012
- European Commission, “Directive on Payment Services”, 2009
- Félix Brezo and Pablo G Bringas, “Issues and Risks Associated with Cryptocurrencies such as Bitcoin”, The Second International Conference on Social Eco-Informatics, 2012
- Jan A. Bergstra, Karl de Leeuw, “Bitcoin and Beyond: Exclusively Informational Monies”, 2013
- Joshua S. Gans and Hanna Halaburda, “Some Economics of Private Digital Currency”, Bank of Canada Working Paper, 2013
- Matthew Elias, “Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy”, 2011
- Michael Woodford, “Monetary Policy in a World Without Money”, NBER Working Paper, 2000
- Nicholas Plassaras, “Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF”, Chicago Journal of International Law, 2013

- Nicolas T. Courtois, Marek Grajek, Rahul Naik, "The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining", 2013
- Nikolei M. Kaplanov , "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation", Temple University Legal Studies Research Paper , 2012
- Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal. Vol.4, 2011
- Rhys Bollen, "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice, 2013
- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
- Tetsuya Saito, "Bitcoin: A Search-Theoretic Approach", Research Institute of Economic Science College of Economics, Nihon University Working Paper, 2013
- Tobias Bamert, Christian Decker, Lennart Elsen, Roger Wattenhofer and Samuel Welten, "Have a Snack, Pay with Bitcoins", 13-th IEEE International Conference on Peer-to-Peer Computing, 2013

---

---

## 금융결제국 발간자료 목록

---

---

### ■ 정기간행물 (연간)

- 지급결제보고서
- 우리나라 및 주요국의 지급결제통계
- 지급결제정보
- 지급결제제도연구회 연구발표 자료집
- 금융정보화 추진현황

### ■ 조사연구 및 업무참고자료

- 1996.11 주요국(G-10)의 지급결제제도
- 1996.12 각국의 전자화폐 개발현황
  
- 1997.12 실시간총액결제(RTGS)시스템의 이해
  
- 1998. 2 지급결제제도
- 1998.10 전자화폐에 관한 보고서
- 1998.12 주요선진국 중앙은행의 결제시스템 운영현황 및  
민간결제기구와의 관계
  
- 1999.12 주요국 소액지급수단 이용현황 비교
  
- 2000. 5 외환결제리스크의 현황과 감축전략
- 2000. 6 Payment Systems in Korea
- 2000.12 BIS 은행감독위원회의 외환결제리스크 관리 감독지침

- 2001. 1 지급결제환경의 변화와 중앙은행의 대응방안
- 2001. 1 호주의 지급결제제도
- 2001. 3 외환동시결제시스템의 이해
  
- 2002. 2 지급결제제도운영관리관련 규정집
- 2002. 2 중요지급결제시스템의 핵심원칙
- 2002. 3 각국의 전자화폐 개발현황
- 2002. 5 지급결제제도관련 용어집
- 2002. 6 전자금융: 전망과 과제
- 2002. 9 미연준의 지급결제시스템 리스크관리정책
- 2002. 9 주요국 중앙은행의 지급결제시스템 감시제도 현황
- 2002. 9 한국은행 예금 및 환업무 해설
- 2002.11 국내금융기관의 정보화투자 효과분석에 관한 연구
- 2002.12 지급결제분야에서 일본은행의 역할
  
- 2003. 7 국내 금융부문의 영업방법(BM)특허 동향 및 시사점
- 2003. 9 국내전자화폐 및 전자상거래와 금융정책
- 2003.12 한국은행 대출업무 해설원고
  
- 2004. 2 지급결제제도와 한국은행
- 2004. 3 주요국의 결제완결성 보장을 위한 법률현황
- 2004. 3 지급결제제도 운영관리관련 규정집
- 2004. 3 전자금융총람
- 2004. 6 지급결제제도와 중앙은행의 역할(지급결제제도 컨퍼런스 보고서)
- 2004.12 우리나라의 지급결제제도
  
- 2005. 3 주요국 총액결제시스템의 유동성 절약방식 비교분석
- 2005. 4 우리나라의 외환동시결제제도
- 2005. 6 지급결제의 환경변화와 발전방향(지급결제제도 컨퍼런스 보고서)
- 2005. 6 영란은행의 지급결제시스템 감시보고서
- 2005. 9 중앙은행의 지급결제시스템 감시
- 2005.10 지급결제제도의 이해
- 2005.11 Payment Systems in Korea

- 2005.11 거액결제시스템의 발전동향 및 시사점
- 2005.12 「한국은행 예금·환업무 해설」
- 2005.12 지급결제시스템 리스크의 유형별 관리대책과 정책과제
- 
2006. 5 지급결제제도의 미래와 결제리스크 관리  
(지급결제제도 컨퍼런스 보고서)
2006. 6 싱가포르의 「지급결제시스템 감시법」
2006. 7 비은행금융기관의 지급결제서비스 제공현황
2006. 8 호주의 「지급결제시스템 규제법」
2006. 8 주요국의 실시간총액결제시스템 운영 현황
2006. 8 지급결제제도 관련 법규집
2006. 9 캐나다의 「지급 청산 및 결제법」
- 2006.10 노르웨이의 「지급결제시스템법」
- 2006.11 미국의 선불카드 규제현황 및 시사점
- 2006.12 홍콩의 「청산결제시스템법」
- 
2007. 1 주요국의 지급결제시스템 감시 등에 관한 법률
2007. 6 비은행금융기관의 지급결제서비스 제공 확대와 정책과제  
(지급결제제도 컨퍼런스 보고서)
2007. 9 지급카드 수수료에 대한 이론적 논의와 주요국의 정책적 대응
2007. 9 지급결제제도 관련 법규집
- 
2008. 1 ECB의 카드결제시스템 감시기준
2008. 2 중앙은행과 지급결제 : 상호관계에 대한 역사적 고찰
2008. 2 지급결제부문에서의 경쟁정책 운용 현황
2008. 2 지급결제의 이해
2008. 4 국내 비금융기관의 지급결제업무 취급 현황
2008. 5 유럽의 지급결제제도 대변혁과 향후 전망
2008. 6 지급결제제도의 안정성 - 의미와 과제
2008. 7 유가증권의 매매 및 결제 메커니즘
2008. 7 영국·프랑스의 증권결제 메커니즘
2008. 8 국가간 지급결제서비스 산업의 국제 동향과 국내 금융기관의 대응 방안
2008. 8 자본시장통합법상 금융투자회사에 대한 규제 및 감독의 주요내용

- 2008.11 지급서비스의 기본개념과 취급요건
- 2008.12 국내외 금융EDI 이용 현황 및 시사점
  
- 2009. 1 금융투자회사의 자금이체업무 해설
- 2009. 5 전자금융총람
- 2009. 6 지급결제제도 관련 규정집
- 2009. 8 금융안정과 지급결제제도(지급결제제도 컨퍼런스 보고서)
- 2009. 9 주요국의 차액결제리스크 관리제도
- 2009.12 우리나라의 지급결제제도(2009년 개정판)
  
- 2010. 6 호주의 소액결제시스템 개편 동향
- 2010. 8 우리나라 및 주요국의 지급결제통계
- 2010. 9 지급결제제도의 환경변화와 정책과제(지급결제제도 컨퍼런스 보고서)
- 2010. 9 장외파생상품 CCP에 대한 「CCP 권고안」 적용 지침
- 2010. 9 장외파생상품시장의 거래정보저장소 관련 고려사항
- 2010.10 Repo 청산결제제도의 강화
- 2010.10 Payment Systems in Korea
- 2010.11 미국 카드시장 규제와 주요 내용과 카드산업의 대응 현황
- 2010.12 금융권의 공인전자문서보관소 이용 현황 및 제도적 문제점
  
- 2011. 1 영국·캐나다·호주의 지급결제시스템 발전전략 및 시사점
- 2011. 2 국가간 개인송금서비스의 현황 및 개선과제
- 2011. 4 유엔국제전자계약협약(UN CUECIC) 수용을 위한 국내의 입법 동향 및 시사점
- 2011. 4 주요국의 장외파생상품시장 인프라 구축 동향과 시사점
- 2011. 4 금융투자회사의 자금이체업무 해설
- 2011. 6 지급수단의 사회적 비용 추정사례
  
- 2012. 7 주요국 RP시장 결제시스템 개선의 주요 내용
- 2012.10 전자금융 조성자로서의 중앙은행 역할 사례 및 시사점
- 2012.12 증권사의 퇴직연금 취급에 따른 잠재리스크 분석
  
- 2013. 5 모바일 지급결제 발전 현황 및 주요 이슈