About BITCOIN

비트코인 설명 자료

한국비트코인거래소 Korbit / www.korbit.co.kr / 김진화 공동창업자 이사 louis@korbit.co.kr

---

1. 비트코인이란

지난 2009년 등장한 글로벌 금융거래 시스템이자 독립적인 디지털 화폐다. 기존 전자금융시스템과 달리, 금융기관의 개입 없이 개인간 빠르고 안전한 거래가 가능하다. Peer-to-Peer 네트워크 기반의 암호화 프로토콜을 사용, 중앙의 관리나 개입 없이 분권화된 화폐발행과 안정적인 거래환경을 제공한다. 금처럼 유통량이 제한적이며 수학적 알고리즘에 의해 향후 100년간 발행될 화폐량이 미리 정해져 있다. 2013년 11월 현재 대략 1200만 비트코인이 유통중이고 발행량이 서서히 증가해 2145년경까지 2100만개까지만 발행된다. 지난 2008년 사토시 나카모토라는 가명을 사용하는 개인 혹은 집단에 의해 개발돼 인터넷을 통해 보급되었고, 전 세계적으로 수백만 명이 사용 중인 것으로 추정된다. 달러화로 환산한 전체 통화가치는 100억 달러(10조원) 규모이며 하루 거래규모도 9억달러에 육박한다. 폭발적인 관심 속에 올 들어 가치가 급등했고 관련 기업들의 대규모 투자유치가 러시를 이루는 등 전체 생태계 규모가 급성장하고 있다.

2. 비트코인에 대한 반응

“가상화폐가 장기적인 장래성을 가질 수 있으며, 특히 그것이 가져올 혁신이 더 빠르고, 더 안전하며, 더 효율적인 결제시스템을 촉진시킬 때 그러할 것이다"
- 벤 버냉키 미국 연방준비제도이사회 의장

Bitcoins are, in an abstract sense, perfect money.
추상적인 관점에서 볼 때, 완벽한 화폐
- 타임지

Like gold, Bitcoin has no central authority...Like gold there will always be a limited supply, and thus its value will increase, and like gold, Bitcoin is brilliant.
마치 금처럼, 비트코인은 중앙집중적 통제를 필요로 하지 않는다, 또한 항상 제한적으로 공급된다. 때문에 그것의 가치는 증대될 것이다, 그리고 마치 금처럼, 비트코인은 번뜩이는 무엇이다
- 인터넷의 아버지 테드 넬슨

We believe that Bitcoin represents something fundamental and powerful, an open and distributed Internet peer to peer protocol for transferring purchasing power.
It reminds us of SMTP, HTTP, RSS, and BitTorrent in its architecture and openness.
비트코인은 근본적이고 강력한 무언가를 상징한다.
구매력을 전이시키는 개방적이고 분산적인 인터넷 P2P 프로토콜이기 때문이다. 비트코인의 설계구조와 개방성은 우리로 하여금 (인터넷의 인프라적 프로토콜인) SMTP, HTTP, RSS 그리고 비트토렌트를 떠올리게 한다
- 미국 유력 벤처캐피탈 유니온 스퀘어 파트너, 프레드 윌슨

I am very intrigued by Bitcoin. It has all the signs. Paradigm shift, hackers love it, yet it's derided as a toy. Just like microcomputers.
비트코인은 나를 흥미진진하게 만든다. 그것은 모든 표식을 갖고 있다. 패러다임 전환, 해커들의 열광 등 하지만 여전히 장난감 취급을 받고 있다. 딱 마이크로컴퓨터가 (과거에) 그랬던 것처럼
- 실리콘밸리 최고의 스타트업 엑셀러레이터 & 인큐베이터 와이컴비네이터 파트너, 폴 그레엄

Bitcoin is the biggest invention since the internet
인터넷 이후 가장 거대한 발명
파미르 겔렌베 Pamir Gelenbe, Partner at Hummingbird Ventures

은행계좌가 없는 이들에게 금융서비스를 제공해주고
신규 금융상품의 개발도 가능케 하는 등 가상화폐경제는 전망이 밝다...
가상화폐가 사회에 혁신과 금융접근성을 제공한다고 우리는 인정한다…
우리는 이런 발전이 계속되길 바란다.
Jennifer Calvery, FinCEN Director 美재무부 금융범죄수사네트워크 부장

3. 비트코인의 혜택과 위험

<혜택>

- 쉽고 빠르게 금융 거래가 가능하다
- 글로벌 커버리지로 전 세계 누구나와 거래가 가능하다
- 수수료가 거의 발생하지 않아, 특히 소상공인에게 유리하다
- 통화량 고정, 인플레이션 방지 설계로 장기간 투자효과가 있다
- 제3기관에 의존하지 않고 자신의 편의와 판단에 의한 금융거래가 가능하다

<위험요소>

- 가격불안정성 : 실험적이고 초기 적용단계라 가격이 불안정하다. 계속 오르고 급등하는 추세
- 취급과 보관에 따른 개인 책임 : 현금과 마찬가지로 분실할 수 있으며 보안이 취약한 피씨에 무방비로 보관할 경우 해킹을 통해 도난 우려가 있다.
- 시스템 공격 : 유수의 해커들조차 해킹에 실패하고 비트코인의 지지자가 되었지만, 비트코인 시스템을 파괴하는 시도가 성공할 가능성은 이론적으로 허용돼 있다. 비트코인 네트워크의 컴퓨팅 파워를 능가하는 컴퓨팅 파워를 갖고 공격할 경우 거래 기록 등에 혼선을 초래하는 게 가능하다. 참고로 2013년 8월 현재 비트코인 네트워크의 컴퓨팅 파워는 전 세계 상위 500대 수퍼컴퓨터 연산능력의 합계보다 10배 가량 높다
- 규제 위험 : 각국 정부의 규제 관련 예측불가능성이 존재한다. 올 들어 비트코인에 대한 관심이 증폭되며 각국 정부 차원의 입장이 속속 제출되고 있다. 이에 자세한 내용은 8절 참고

* 유럽중앙은행 비트코인의 다음과 같은 특장점들로 인해 가상화폐가 보다 널리 쓰이며 성장할 것으로 전망하고 있다.

- 인터넷의 접속과 이용이 늘고 있으며 가상 커뮤니티의 이용자 역시 증가하고 있음
- 이커머스의 증대 특히 가상화폐의 이상적인 기반시장이 될 디지털 재화 분야에서의 두드러진 성장
- 다른 전자 지불수단 대비 높은 수준의 익명성
- 다른 전자지불수단 대비 낮은 거래수수료
- 가상 커뮤니티에서 요구되어지는 더 직접적이고 빠른 거래 처리

4. 비트코인의 기본적 이해

지난 2008년 사토시 나카모토라는 닉네임으로만 알려진, 실체가 드러나지 않은 개발자(혹은 그룹)에 의해 비트코인이 등장했다. 이전까지는 온라인상의 자금 거래에 항상 제3자(금융기관)의 신용을 바탕으로 한 개입이 필요했다. 비트코인의 등장은 이 과정이 불필요하게 만들었다는 점에서 의미심장한 혁신이었다.

예를 들어 보자, 영희가 철수에게 10만원의 돈을 인터넷상으로 보내려면, 은행이나 신용카드회사 또는 페이팔 같은 서비스에 의존해야만 했다. 거래 당사자인 두 사람 외에 또 다른 당사자, 즉 금융 기관의 개입이 필요한 것. 이들 중개자는 계좌소유자의 잔고와 거래내역이 기입된 온라인상의 장부를 유지/관리하는 역할을 한다. 예컨대 영희가 철수에게 10만원을 보내면, 금융기관은 영희의 계좌 장부에서 10만원을 빼고, 철수의 장부에 10만원을 더하는 식으로 거래를 처리하게 되는 것이다.

이런 과정을 거쳐야 하는 이유는 무엇일까? 여러 이유가 있겠지만, 가장 핵심은 중개자, 공인된 장부관리자가 없다면 디지털화된 돈의 경우 이중으로 사용될 수 있기 때문이다. 알다시피 디지털 캐시는 디지털 문서와 마찬가지로 단지 컴퓨터 상의 파일일 뿐이다. 장부를 관리하는 중개기관이 없다면 (우리가 컴퓨터 파일을 쉽게 복제할 수 있는 것마냥) 쉽게 복제해서 이중, 삼중으로 반복해서 사용할 수 있다. 이런 중개기관 없이 영희가 철수에게 직접 디지털 캐시를 보낸다면, 10만원에 해당하는 파일을 메시지에 첨부해서 보내게 될 것이고, 이메일을 쓸 때와 마찬가지로 첨부한 파일은 컴퓨터에서 사라지지 않고 그대로 남게 된다. 고로 영희는 또 다른 친구, 예컨대 영철에게도 10만원을 보낼 수 있게 될 것이다. 그리고 아마도 엄청난 혼란이 야기될 것은 불을 보듯 뻔하다. 이 같은 문제는 컴퓨터과학에서 이중지불 문제로 알려져 있다. 비트코인이 등장하기 전까지 이 문제는 신용을 기반으로하는 제3기관의 장부관리 역할을 채택하는 것에 의해서만 해결할 수 있는 것이었다.

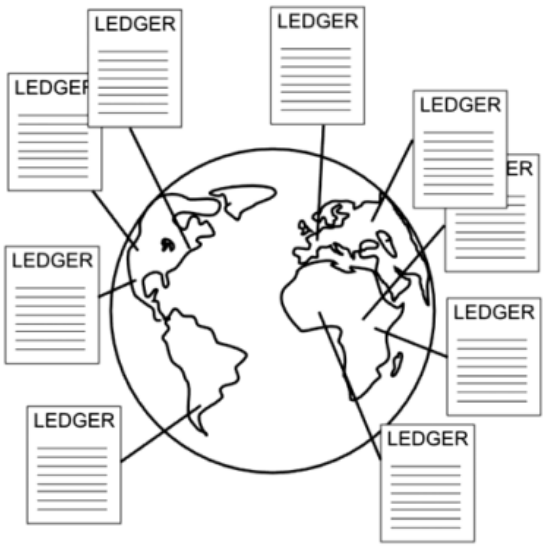
비트코인의 등장이 혁명적으로 받아들여지는 것은 이런 배경 때문이다. 즉 역사상 최초로 제3기관의 개입 없이 이중지불 문제를 해결했다는 점. 이게 어떻게 가능했을까? 비트코인이 택한 전략은 분산과 공개였다. P2P 네트워크를 통해 시스템의 모든 이용자들에게 장부를 공개하고 분산했다. 그리하여 비트코인 시스템 상에서 발생하는 모든 거래는 하나의 공개 장부에 기록되고, 분산되어 저장된다. 이 단일장부를 블럭체인이라 칭한다. 새로운 거래가 발생하면, 그 거래에 사용된 비트코인이 예전에 사용된 적이 있었는지 검증된다. 그리하여 이중 사용으로 문제가 발생할 여지가 사라지게 된다. 수만명의 자발적 검증인(마이너, 채굴자) 및 이용자들로 구성된 전지구적 규모의 P2P 네트워크가 스스로 금융기관의 역할을 하게 되는 것이다. 그리하여 영희와 철수는 은행이나 페이팔 없이도 온라인 상으로 금전 거래를 할 수 있게 되었다.

비트코인은 이처럼 분산적이고 수평적인 금융거래 네트워크이면서 동시에 독립적인 화폐시스템이기도 하다. 비트코인 네트워크 상에서 이루어지는 거래는 페이팔이나 인터넷뱅킹과 달리 달러 또는 원, 유로 등으로 표기되지 않는다. 비트코인을 화폐 단위로 거래가 이뤄지고 금액이 표기된다. 이 화폐의 가치는 금 또는 국가 화폐에서 비롯되는 게 아니라 사람들이 부여한 가치만큼 평가된다. 비트코인에 대한 달러의 가치는 서로 다른 국가 화폐들 간 환율과 마찬가지로 공개 시장에서 결정된다. 수요와 공급에 따라서 말이다. 중앙은행이 임의대로 발행량을 조절하고 그에 따라 가치가 점차 낮아지는 기존 화폐와 다른 점이다.

5. 비트코인의 기술적 이해

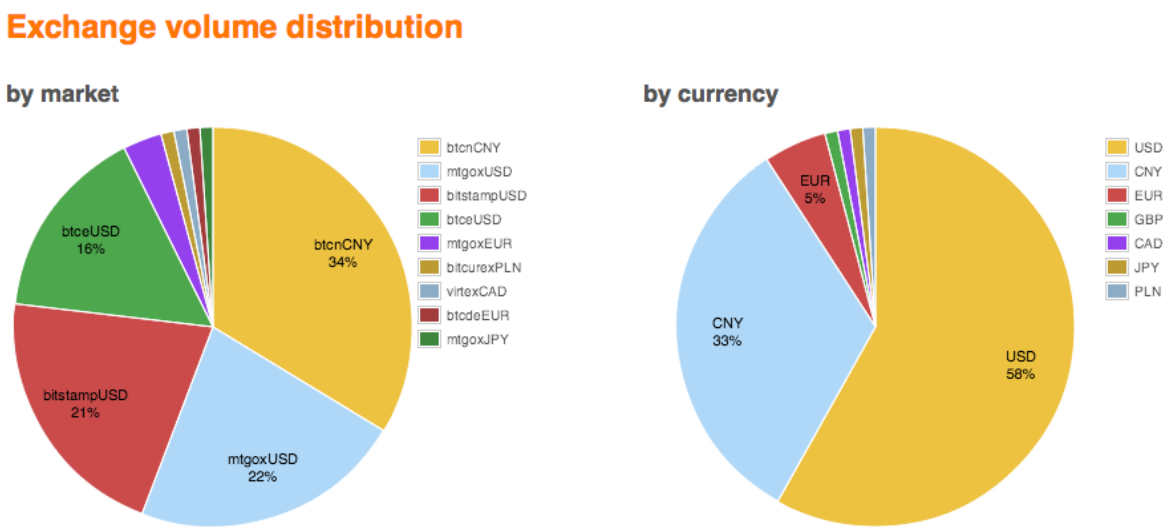
핵심적으로 말해 비트코인은 분산된 공개 장부를 가진 거래 네트워크이다. 거래라는 것은 다음과 같은 메시지를 포함하는 파일들에 불과하다 : “이용자 X가 3 비트코인을 이용자 Y에게 보냈음” 그리고 “이용자 Y가 Z에게 그 가운데 2.5 비트코인을 보냈음"
이용자들은 이름으로 구분되지 않는다. 그들의 정체성은 디지털 서명체계를 위한 공개 키가 대신한다. 이를 통해 이용자는 그들의 거래에 서명을 하게 되고, 그럼으로써 (누군가) 이 거래를 조작하는 걸 매우 어렵게 만든다. 사실 이런 구성요소들은 전혀 새로울 게 없는 것들이다. 비트코인을 특별하게 만드는 것은 거래장부를 관리/운영하는 방식에 있다.
일반적인 방식처럼 모든 거래기록을 하나의 서버에 저장하는 대신에, 블럭체인이라고 부르는 공개장부는 P2P(개인 대 개인) 네트워크 상에서 구동하는 상호 신뢰가 없는 참여자 그룹 간의 집단적 작업에 의해 대규모로 복제되고 업데이트 된다.
이 작업을 위해, (참여하는) 노드들은 P2P 네트워크 상에 공표되는 거래기록을 끌어 모은 후 그것들을 체인의 말미에 포함시키는 기회를 얻기 위해 경쟁하게 된다- 이 경쟁에서 이기는 참가자는 새로 발행되는 비트코인(현재 25BTC)을 보상으로 얻게 된다. 어느 한 참가그룹이 이 과정을 독점(하고 거래 기록을 조작)하는 것을 방지하기 위해 참여자들은 ‘작업 증명'이라고 불리는 어려운 수학 문제를 푸는 경쟁에 임할 것을 요구받는다. 블럭체인의 통합성은 해시 체인 기법을 통해 강화되는데, 이를 통해 누군가 거래 이력을 바꾸는 시도가 매우 어려워지게 된다.

- 미 존스홉킨스대학교 교수 매튜그린



6. 비트코인의 제도적 이해

- 누가 발행하는가? 발행 주체 : 수학적 알고리즘과 인터넷 상의 컴퓨터 네트워크에 의해 자동발행
- 누가 관리하는가? 관리 주체 : 별도의 중앙서버나 정산소 없이 P2P 네트워크 상에서 업데이트되고 전체 기록이 복제되어 관리
- 어디에서 사용할 수 있는가? 사용처 : 자발적으로 비트코인을 지불수단으로 채택하는 웹사이트, 상점 등에서 사용 가능.
- 국가 화폐로의 전환 : 자율적으로 설립된 여러 거래소를 통해 비트코인을 사고 파는 사람들에 의해 전환. 중국의 BTC China가 세계 최대 거래소, 이어서 일본 도쿄에 위치한 마운틴곡스(mt.gox) 거래소. 나라 마다 각국 화폐로의 전환을 중개하는 거래소가 생겨나는 상황



7. 비트코인의 경제학적 이해

- 발견되고 채굴된 금이 아닌, 발명된 금 : “마치 금처럼, 비트코인은 중앙집중적 통제를 필요로 하지 않는다, 또한 항상 제한적으로 공급된다. 때문에 그것의 가치는 증대될 것이다, 그리고 마치 금처럼, 비트코인은 번뜩이는 무엇이다.” 인터넷의 아버지 테드 넬슨(영국 옥스포드대 사회학 교수)

- “비트코인의 경제학적 뿌리는 오스트리아 학파에 있음" 유럽중앙은행 : 명목화폐 시스템과 정부 및 중앙은행에 의한 시장개입이 경기순환을 악화 시키고 막대한 인플레이션으로 귀결된다는 오스트리아 학파의 입장과 맥락을 같이 함.

- 미 연방준비제도 출범 후 지난 100여년간 달러의 가치는 95% 하락

- 키프러스 사태 등 유로존 금융위기로 비트코인 가치 급상승. 글로벌 금융시스템과 국가금융정책에 대한 불신이 비트코인에 대한 수요로 연결

- 준비제도에 따른 금보유량의 10% 대체할 경우, 765억 달러 가량의 시장 차지 (현재 비트코인 전체 가치는 100억달러 규모)

- 연간 금 투자 시장의 20% 대체할 경우, 매년 14억 달러 규모 시장 차지

- 국제이주자 송금 (연간 570조원)의 10% 대체할 경우 연간 550억달러

8. 각국 규제당국의 반응 및 입장

- 2012년 9월 유럽중앙은행의 보고서, 2013년 초 미국 금융당국의 가이드라인 발표를 시작으로 세계 주요국가에서 정부 입장이 개진되는 중

- 미국은 비교적 신중한 입장이었고, 거래소에 연계된 은행계좌 동결 조치 등 규제 움직임을 보이기도 했으나, 11월 의회청문회를 기점으로 비트코인의 제도적 포용 쪽으로 가닥을 잡아가는 양상
- 연방행정연구처, 금융정보분석원, 시카고연방준비은행 등의 보고서에서 비트코인의 혁신성과 파급력을 강조한데다, 실리콘밸리와 월가를 중심으로 민간자본의 움직임이 활발해지면서 정부 입장에 변화 (새로운 금융혁신에서 미국이 뒤쳐지면 안된다는 위기 의식 또한 발호)

- 캐나다, 네덜란드, 노르웨이의 경우 거래소 등 비트코인 관련 비즈니스가 금융송수신업에 해당하지 않는다는 탈규제 입장, 네덜란드 재무장관은 다음과 같이 언급:
  “비트코인은 돈을 받고 교환하는 과정에서 발행되지 않는다. 또한 발행자에 대한 청구권을 표상하지도 않는다. 그렇기 때문에 비트코인은 법률상 규정된 화폐의 네 가지 요건 중 적어도 두 가지를 충족시키지 않는다. 아울러 비트코인은 어떠한 다른 방식으로도 법률상의 금융상품이 되지 않는다. 비트코인 매매 중개 또한 금융서비스가 아니다. 따라서 금융감독법안이 적용되지 않는다.”

- 독일 정부는 6월초, 비트코인 관련 과세 입장 발표 : “비트코인을 1년 이상 보유한 경우 매매차익에 대해서 과세하지 않는다.” 소득세법 상 증권, 채권 등 일반적인 투자 상품과 달리 개인 거래로 규정
- 뒤이어 8월, 비트코인을 공식적인 화폐로 인정

- 전 세계에서 유일하게 태국만 불법이라는 입장, 태국 중앙은행은 현행법상 비트코인 이용이 불법이라고 해석. 하지만 이용 단속 및 규제 등 구체적 정책은 수반되지 않고 있음
- 영국 보수당 의원 더글라스 카스웰은 태국 정부의 이 같은 결정을 두고, “밀려오는 파도를 향해 멈추라고 명령했던 카누트 대왕만큼이나 어리석은 짓"이라고 공개 비난

- 중국 정부는 사실상 암묵적 승인. 올 들어 관영 CCTV에서 연달아 관련 다큐멘터리 등 방영
- 이에 중국 비트코인 업계는 규제에 대한 우려 없이 매우 공격적으로 시장 개척 및

성장 중. 중국 비트코인 거래소 BTC차이나는 10월 세계 최대 거래소로 급부상. 미국의 라이트스피드벤처가 5백만불 투자. 전 세계 통화 중 위안화가 비트코인 경제에서 달러에 이어 2위로 급부상

9. 한국 사회 시사점

- 인터넷 혁명, 모바일 혁명에 뒤 이은 가장 거대한 혁신
- 인터넷 혁신기, PC통신 등 기존 지배적 사업자의 이해 관철과 정부 규제로 뒤늦은 대응
- 모바일 혁신기, 한국형 모바일 플랫폼(WIPI) 등 고집하며 글로벌 표준 막았다가 '갈라파고스 고립 위험'
- 뒤늦게 패스트팔로 전략으로 많은 사회적 비용을 치르며 대응 중

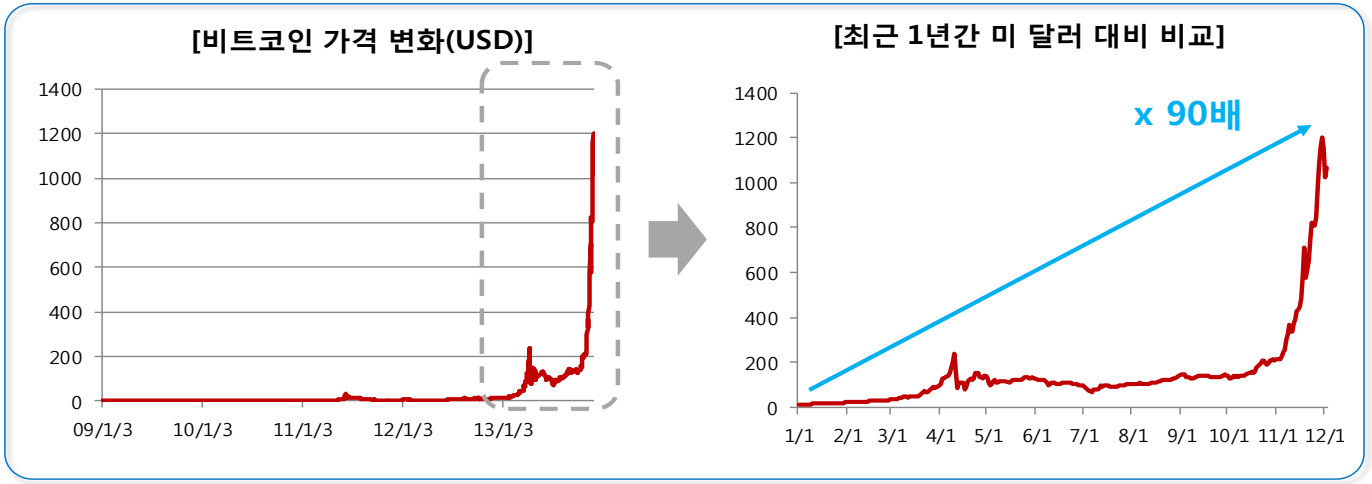
- 비트코인 혁신의 시계는 인터넷 혁명기의 1994년 정도라는 평가 (야후가 등장했던 해)
- 금융에서 벌어지는 혁신이라 그 파급력을 가늠하기 어렵다는 전망
- 역기능에 대한 우려도 있으나 이 역시 빠른 적응과 대응 필요
- 그동안 추진해 온 금융개방, IT인프라 및 저변 확산 등의 사회적 자원을 토대로 발빠르게 대응하면 리더십을 가질 수 있음
- 과거 정책적 구호로만 난무했던 '동북아 금융허브' 구상 등이 새로운 혁신적 금융의 아시아 허브 (중국을 배후시장으로 하는) 등으로 구체화 될 수 있음

비트코인(Bitcoin) 시스템 분석 노트

kt 경제경영연구소 이 성 춘(sungchoon.lee@kt.com)
박 유 진
손 현 진

Prologue…

- **최근 비트코인에 대한 관심이 급증하고 있음**
  - 4월 키프로스 예금 사태 때 언론을 통해 알려지면서 대중의 관심 시작
  - 2009년 처음 도입된 이후 4년 동안 가격에 큰 변동이 없었으나, 올해 4월 이후 급 상승
  - 미국 달러 대비 환율은 연초 대비 90배 상승 (1월 2일 $13.4 → 11월 30일 $1,203)



- **비트코인에 대한 최근 관심의 대부분은 '화폐'로서의 '가능성'에 초점이 맞춰져 있음**
  - 신뢰 제공 방식, 급등락하는 가치의 변동성, 실물 경제와의 연동 가능성 등이 주요 쟁점

- **하지만 코인이 작동하는 메커니즘이나 시스템에 대한 부분은 거의 논의되지 않고 있음**
  - 비트코인은 **'Technology'** 측면에서도 놀라운 '혁신'을 다수 포함하고 있음

➔ **본 리포트에서는 이러한 비트코인의 작동 메커니즘을 집중 분석하고자 함**

I. Bitcoin이란 무엇인가?

Satoshi 논문 Abstract 번역

사토시 나카모토(Satoshi Nakamoto)는 2008년 Bitcoin 개념을 소개하는 논문을 발표

"Bitcoin: A Peer-to-Peer Eclectroinic Cash System" (http://bitcoin.org/bitcoin.pdf)

다음은 위 논문의 Abstract을 번역한 것임

순수한 P2P 버전의 전자 화폐는 금융기관의 개입 없이 한 쪽에서 다른 쪽으로 직접 보낼 수 있는 온라인 지불 수단을 제공할 수 있다. 디지털 사인은 솔루션의 한 축이지만 만약 부정행위(double-spending) 방지를 위해 신뢰할만한 제 3자가 개입한다면 (P2P 버전 전자화폐의) 주요 장점이 곧 사라지게 될 것이다. 우리는 이 논문에서 부정행위 방지 문제의 해결책으로서 P2P 네트워크 활용을 제안한다.

P2P 네트워크는 거래를 해시(암호화)로 전환한 후 타임스탬프**(timestamp)**를 찍고 이 과정을 일련의 '해시 기반의 **proof-of-work** 사슬'로 연결함으로써 이러한 **proof-of-work** 과정을 반복하지 않고서는 거래 기록을 수정할 수 없도록 한다.

가장 긴 연결고리 사슬은 발생한 거래의 시퀀스(순서)를 증명할 뿐 아니라 가장 많은 CPU 파워를 사용하여 만들어진 사슬임을 증명하는 역할을 한다.

과반수 이상의 CPU 파워가 네트워크 공격에 협조하는 노드(node)에 의해 제어되지 않는 한, 정직한 네트워크의 노드들이 가장 긴 연결고리 사슬을 만들어 낼 것이며, (연결고리 사슬 만들기 경쟁에서) 공격자들을 앞서 나가게 될 것이다.

네크워크 자체는 단순한 구조라도 상관 없다. 거래 내역은 일반 인터넷 망을 통해 모두에게 전파되고 노드들은 수시로 네트워크에서 이탈하거나 다시 접속해도 문제될 게 없다. 네트워크를 떠나 있을 동안 일어난 일들에 대해서는 가장 긴 연결고리 사슬을 증거로서 받아 들이기만 하면 된다.

**** 제가 컴퓨터 쪽에 기본 지식이 없어서 번역 및 용어 선정에 문제가 있을 수 있음을 미리 알립니다. 보다 좋은 해석이나 용어가 있으면 코멘트 부탁 드립니다.***

I. Bitcoin이란 무엇인가?

비트코인은 전자화폐로 가상화폐, 디지털 화폐로도 불림 → 실물 화폐와 대조되는 개념
핵심 특징: ① 암호화 기술 채용, ② P2P (Peer-to-Peer) 운용, ③ 통화 공급량 고정

정의

비트코인 = 디지털 서명이 고리로 연결된 전자 화폐 (코인)

an electronic coin as a chain of digital signatures

- *Satoshi Nakamoto의 논문*

오픈 소스 P2P 결제 네트워크 & 디지털 화폐

- *Wikipedia*

특징

1. 암호화 기술 채용 – 거래관련 기록 전체의 암호화로 익명성 제공
2. P2P 분산 네트워크로 거래 관리 – 신뢰를 제공하는 집중화된 관리 기구 대체
3. 통화 공급량 고정 – 통화 공급 측면의 안정성 제공
4. 오픈 소스 – 시스템 운영 소스 코드가 공개되어 누구나 수정 가능
   * 다만 새로운 룰이 적용되기 위해서는 80% 이상의 수용 필요 (CPU 수 기준)

II. Bitcoin 거래 메카니즘

1. Bitcoin 클라이언트 프로그램 SW를 인터넷에서 다운로드

2. 다운로드된 프로그램은 지갑 역할을 하며 지갑에서는 계정을 만들 수 있음

계정을 만들면 계정은 한 쌍의 암호키(공개키 & 비밀키, Public & Private Key)를 생성

ex) 15ChaTuCDpaPXkmigDWZMKzvCCxiMCmjFB

1dag1WuFyHQkGM7YQvXKsbRNzPWYbsWEH

15DqqynVTwbc7VsTtz51HnhJpXV2XncBDt

➔ 이 복잡한 형태의 계정정보가 바로 **공개키(Public Key)**이면서 **돈이 송금될 주소(address)**

➔ 각각의 계정에는 일정 액수의 Bitcoin이 함께 연동되어 있고 입출금에 따라 금액은 증감

➔ 계정을 만들 때 공개키와 함께 만들어진 나머지 비밀키(Private Key)는 지갑 속에 저장되어 있으며 계정에 접속할 때나 송금할 때 사용하게 됨 (현금 인출에 필요한 비밀번호 기능)

II. Bitcoin 거래 메카니즘

Bitcoin 취득 방법 두 가지

1. 주식시장과 같은 거래소에서 실물화폐, 즉 달러나 원화를 주고 Bitcoin을 구매
2. 채굴(mining)에 성공하면 그 보상으로 (현재는) 25비트코인이 부여됨

   * 채굴 길드와 같은 조직(pool)에 참여하면 25 비트코인이 기여한 비율에 따라 나누어 지급됨

Bitcoin 보내기 (송금): 1이 2에게 보낼 때

1. 먼저 돈을 받을 2가 돈을 보낼 1에게 '돈 받을 2의 계좌(공개키 & 주소)'를 보냄
2. 1은 2의 계좌(공개키)와 보낼 액수를 기입 (네트워크 전체에 돈이 갈 곳을 공표하는 것)
3. 1은 자신의 지갑 속에 있는 비밀키(Private key)로 사인 (공개키와 맞는 유일한 키)
4. 1은 거래 내역을 비트코인 네트워크에 공표 (블록에 저장되어 채굴에 사용 – 추후 설명)

- 돈 보내는 사람이 하는 것은 1과 2의 절차
- 3과 4의 절차는 클라이언트 소프트웨어가 수행

II. Bitcoin 거래 메카니즘

아래 그림은 사토시 논문에서 가져온 것임.

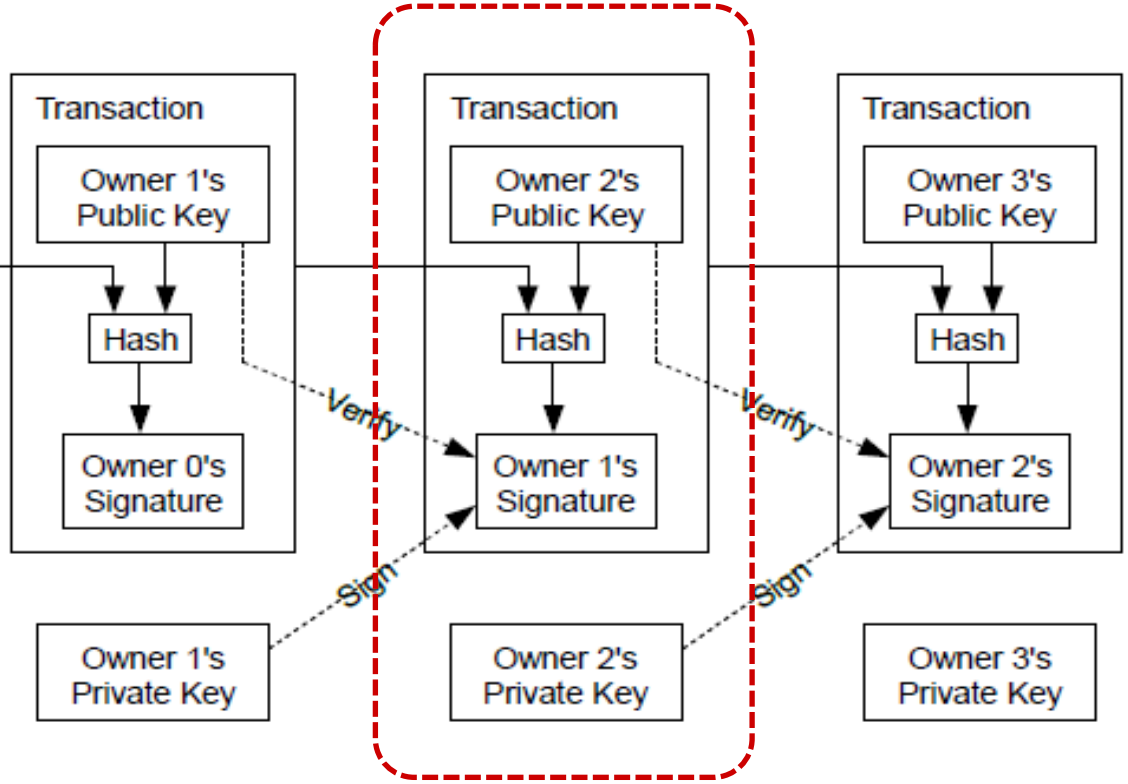
보다 자세한 거래 작동 원리는 다음 슬라이드의 해시(hash, 암호) 중심 흐름도 참조

- Owner 1 = 철수
- Owner 2 = 영희

3116d82e9c97e92296111a85610a1c3d891ad4390df17550d0b0a3cd95294db3

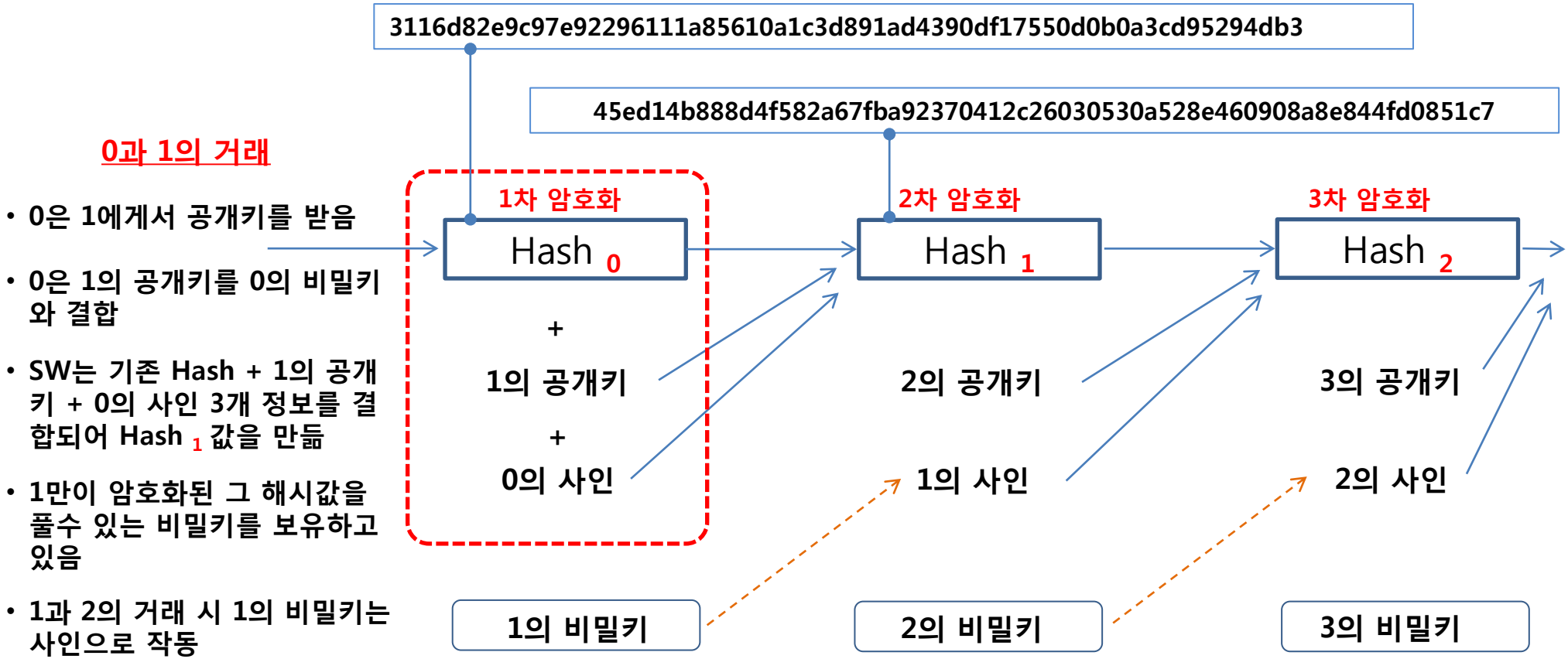
암호화된 계좌로 송금한 내용이
다시 암호화된 값, 즉 해시(Hash)로 기록됨

※ 해시: 특정 데이터를 영문, 숫자로 구성된 일정 길이의 배열로 변화시키는 것. 그 결과가 해시값



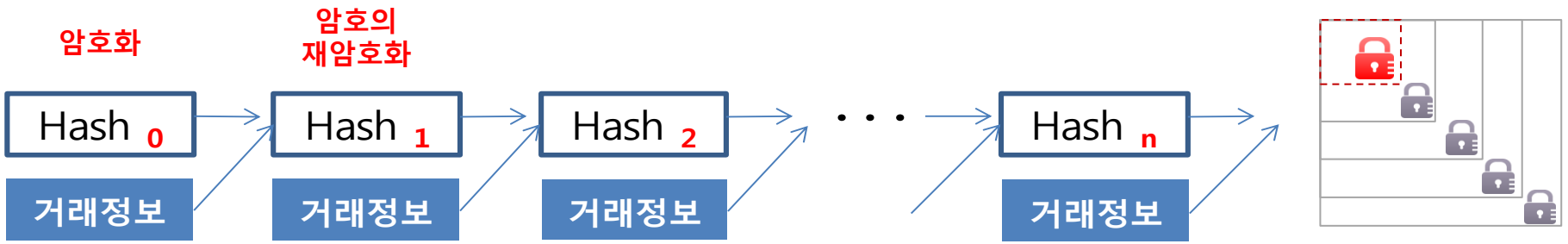
II. Bitcoin 거래 메카니즘

- 해시는 (이전 해시 + 거래 내역)을 또 다시 새로운 해시로 암호화하는 과정을 계속 되풀이
- 결과적으로 최종 해시는 최초의 거래 내역부터 모든 거래 내역을 반복화되는 암호화를 통해 보관
- 해시는 불가역 암호 함수여서 3이 2와의 거래로 얻은 해시 값에서는 1과 2의 거래내용을 볼 수 없음



II. Bitcoin 거래 메카니즘

• 거래 메커니즘에서 나타나는 해시(Hash)의 형태는 사토시가 왜 Bitcoin을 디지털 사인의 연결 고리 (a chain of digital signature)라고 했는지를 잘 보여줌



• 해시는 해시 함수에 의해 알파벳과 아라비아 숫자(alphanumerical)로 표시된 값을 만들어 냄

* ex) 3116d82e9c97e92296111a85610a1c3d891ad4390df17550d0b0a3cd95294db3

해시 함수는 불가역 함수로서 결과값을 만드는 처음 조건 값을 알아내기 어려움

* ex) 500,000이라는 결과 값을 만들어 내는 두 정수의 조합은 너무나 많은 것과 같은 이치

해시 함수는 오리지널 값의 조합이 어떻게 표현될지를 예측하는 것도 매우 어려운 특징이 있음

* 이 특징은 부정행위 방지 시스템에서 깊게 활용됨

➔ 이렇게 풀기 어려운 암호화 과정을 통해 거래 내역이 노출되지 않음

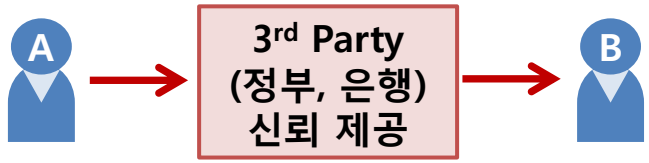
➔ 거래 시 돈을 받는 사람에게 돈을 보내는 사람의 개인 정보가 전혀 제공되지 않음

III. Bitcoin 채굴(mining) 메카니즘

신뢰를 대신하는 P2P 메카니즘

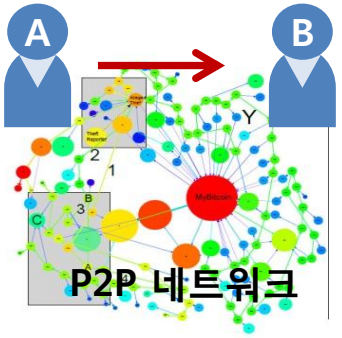
- 비트코인의 혁신의 일부는 거래의 암호화 부분보다 그 거래를 P2P 네트워크를 통해 확증하는 시스템을 만들었다는 점에 있음
- 실물화폐 시스템에서는 정부나 은행과 같은 중앙 관리 기구가 신뢰를 제공하여 거래를 성사시킴
- 반면 비트코인은 P2P 네트워크에 참여하는 사람들의 자발적 참여로 거래를 성사시킴

[실물화폐 거래]



VS.

[비트코인 거래]



- 비트코인 거래를 확증(verification)하기 위해 네트워크에 있는 노드(node)들이 자발적으로 참여하는 것을 mining, 즉 '채굴'이라고 하며 이러한 노력에 대한 보상으로 비트코인이 지급됨
- 따라서 채굴(mining) 과정은 ① 비트코인 거래 시스템을 유지하는 핵심 메커니즘에 자발적으로 참여할 유인을 제공하며, ② 비트코인 통화 공급 역할을 하는 매우 중요한 과정임

III. Bitcoin 채굴(mining) 메카니즘

채굴(mining)이란?

- 비트코인 시스템에서 채굴(mining)이란 '특정 조건을 충족시키는 해시(암호값)을 찾아 내는 것'

- 채굴을 이해하기 위해서는 먼저 블록(block)이라는 개념을 먼저 이해할 필요가 있음
- 블록은 상자(box) 개념으로 이해해도 됨
- 블록과 상자는 차곡차곡 쌓여 가는 것, 혹은 고리로 연결되어 뻗어 나가는 '줄기'로 상상하면 됨
  (앞에서 살펴 본 거래 내역이 담긴 정보가 해시에서 해시로 끊임 없이 이어져 나가는 것과 동일)

- 비트코인 네트워크에 참여하는 모든 노드에는 모두 같은 블록(상자)이 주어지고 모든 거래 내역도 모든 참여자, 즉 노드에게 전파됨 (논문에서는 broadcast로 표현)
- 따라서 블록(상자)에는 앞에서 살펴 본 거래 내역의 암호값(해시)이 차례로 담겨짐
- 이렇게 특정 블록에 쌓인 거래 내역을 확증, 즉 클리어링 해주는 과정이 바로 '채굴(mining)'

- 채굴(mining)이 작동하는 방식은 앞에서 살펴 본 거래 내역을 암호화하는 방식과 거의 동일함

- 그러나 채굴에서 찾아 내려는 해시 값은 거래에서 사용되는 해시값과 다른 형태를 띠고 있음

  ex) 거래 해시값 3116d82e9c97e92296111a85610a1c3d891ad4390df17550d0b0a3cd95294db3

  채굴 해시값 0000000000000000135c058d5e52a6cd73b834b4e7395897527e8dd55b3236686

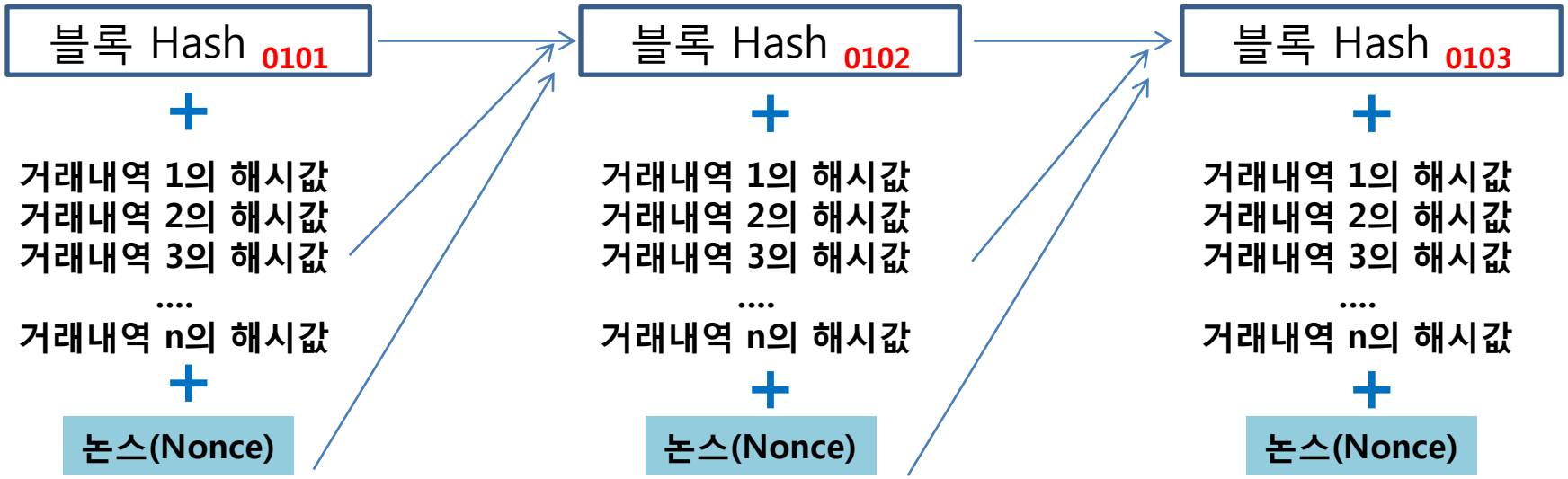
  특정 조건 (Target)

III. Bitcoin 채굴(mining) 메카니즘

- 채굴자(miner)는 ① 현 블록의 해시 값, ② 거래내역 해시값들, ③ Nonce 세 정보를 결합하여 특정 조건, 즉 target이라고 불리는 해시 첫 부분의 '0'수 보다 많은 0을 가진 해시값을 찾아야 함
- 채굴자는 임의의 거래내역 일부분(chunk)와 임의의 수 논스(nonce)를 조합하여 다음 해시값을 계산함
- 특정 조건을 충족시키는, 즉 leading zero 수가 target보다 많은 해시 값을 찾게 되면 현 박스(블록)에 있는 거래가 '정상 거래'로 확증되고 다음 블록(상자)이 열리며 거래 정보가 새 블록에 쌓이기 시작함

현 블록의 해시값 00000000000000135c058d5e52a6cd73b834b4e7395897527e8dd55b3236686

다음 블록의 해시값 0000000000000057784f105ff6177e6272f2fdca72e358fbad0bec7aa0faee4



III. Bitcoin 채굴(mining) 메카니즘

블록 연결 고리 진행 읽기 (사례)

https://blockchain.info를 방문하면 언제든 최신까지 채굴된 블록 정보를 볼 수 있음

Blockchain Home Charts Stats Markets Developers Wallet

Block #273954 ← 1번부터 시작한 블록(상자)이 27만개 이상 열렸음(채굴됨, 해시값이 풀렸음)을 보여 줌.

Summary	
Number Of Transactions ← 포함된 거래 수	363
Output Total ← 거래된 비트코인 총액	3,394.30105415 BTC
Estimated Transaction Volume	1,740.66932404 BTC
Transaction Fees	0.08571565 BTC
Height	273954 (Main Chain)
Timestamp	2013-12-09 10:27:15
Received Time	2013-12-09 10:27:32
Relayed By	BitMinter
Difficulty	707,408,283.05
Bits	419828290
Size	229.806640625 KB
Version	2
Nonce	3808164999 ← 해시값을 푸는 데 사용된 논스(nonce) 값

Hashes

Hash	현 블록의 해시값 000000000000000aedb94fcd1b127bb10ff0fdd6b0664fb70cbc4b2c2586c23
Previous Block	이전 블록의 해시값 000000000000000135c058d5e52a6cd73b834b4e7395897527e8dd55b3236686
Next Block(s)	토론토에 있는 채굴자가 3가지 정보를 사용하여 풀어낸 다음 블록의 해시값 (채굴 성공 → 363 거래 정상 확정) 000000000000000057784f105ff6177e6272f2fdca72e358fbad0bec7aa0faee4
Merkle Root	97410149f9f08f55e230ffe008778fcba23d5692d422618d39db6d10d5137b87

Network Propagation (Click To View) ← 채굴된 곳: 토론토

III. Bitcoin 채굴(mining) 메카니즘

채굴(mining)의 의미

- 채굴(mining)이란 '특정 조건을 충족시키는 해시(암호값)을 찾아 내는 것'
- 이 때 새롭게 발견된 해시값은 현재 블록의 번호를 잇는 다음 번호를 가진 블록(상자)의 주소가 됨
- 그리고 현 블록(상자)에 담긴 거래 내역이 정상 거래임을 확정하게 됨
- 이를 비트코인 거래장부로 보면 블록은 한 장의 페이지가 되고 채굴자가 채굴에 성공했다는 것은 현 페이지에 기록된 거래 내용을 확정하고 이 후의 거래는 다음 페이지에 기록하는 것과 같은 것임

- 거래 해시 값에는 그 거래에서 움직인 비트코인이 처음부터 지금까지 어떤 경로로 흘러 왔는지에 대한 모든 정보가 기록되어 있듯이
- 채굴 결과로 얻어진 새 블록의 해시값에는 이 전의 해시값과 이전 거래 해시 값들이 모두 들어 있으므로 최초의 비트코인 거래부터 현재까지의 모든 비트코인 거래 내역이 모두 담겨 있는 것임

- 따라서 블록 해시 값은 모든 비트코인 거래 내역의 암호화 값이고
- 채굴(mining)은 그 값을 계속 업데이트 하는 행위, 즉 비트코인 거래 장부 업데이트 행위가 됨

IV. Bitcoin 중복사용 방지 메카니즘

- 정당하지 못한 수단으로 비트코인을 획득하는 방법에는 세 가지가 있음

  1. 근거 없이 허위로 만들어 내는 것 (creating value out of thin air)
  2. 자기 것이 아닌 것을 훔치는 것 (taking money that never belonged to the attacker)
  3. 자신의 거래 내역을 조작하여 재사용 하는 것 (double-spending, 중복사용)

- 위에서 언급한 세 가지 방법 중 가장 문제가 되는 것은 '3'번의 경우임

  1. 비트코인은 마이닝을 통해 통화량이 공급되기 때문에 현재 거래 내역이 쌓이는 블록(상자) 번호에 따라 총통화량이 자동 계산됨. 따라서 임으로 새로운 통화를 만들면 바로 들통이 남
  2. 거래에서 수신자의 공개키와 송신자의 비밀키가 결합되기 때문에 수신자의 비밀키가 없는 사람은 거래에서 전송된 비트코인 자체를 열어 볼 수 없음 (즉 전달되지 않음, 거래되지 못함)
  3. 이 문제를 풀기 위해 도입한 것이 바로 '채굴(mining)'과 연계된 proof-of-work 시스템임

  ➔ 이 솔루션이 비트코인 혁신의 핵심이며 향후 ICT 산업에 거대한 영향을 미칠 것으로 보임

  ➔ 이 솔루션은 모든 P2P 분산 시스템이 공통적으로 직면하고 있는 '비잔틴 시대의 장군들' 문제'에 대한 최초의 실질적 해결책으로 받아 들여지고 있음

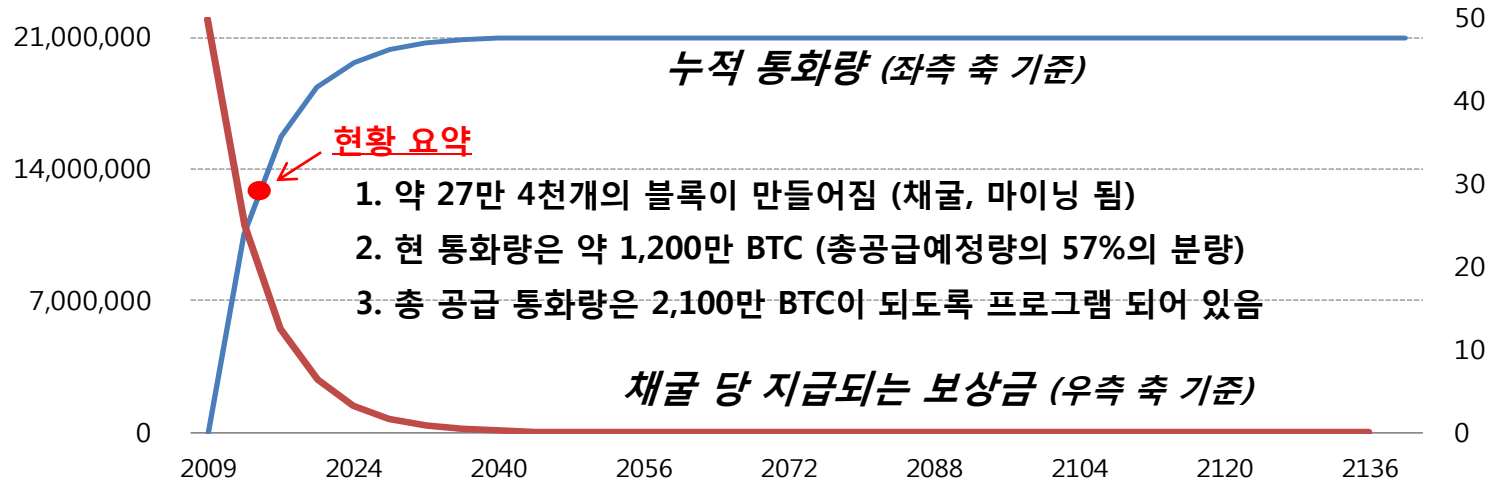
IV. Bitcoin 중복사용 방지 메카니즘

근거 없이 비트코인을 만들어 내는 것은 불가능

- 비트코인 총 통화량은 채굴된 블록(상자) 수에 따라 결정됨.
- 채굴된 블록(상자)에는 일련 번호가 부여됨 (12월 10일 아침 현재 채굴된 블록 번호는 #274061번)
- 채굴된 블록 번호에 따라 현재 유통되고 있는 총 통화량을 계산하는 방법은 다음과 같음

1. 비트코인은 처음 210,000개의 블록을 채굴할 때까지는 블록마다 50 BTC를 보상금으로 지급
2. 210,001 블록부터 420,000번째 블록까지는 25 BTC 지급 (42만 1번부터 63만까지는 12.5BTC 지급) …
   (21만개의 블록이 마이닝 될 때마다 지급되는 보상금(reward)가 1/2로 감소됨)
3. 따라서 현재 블록 번호 274061에서 유통되는 총 통화량은 다음과 같이 쉽게 계산할 수 있음
   (210,000 x 50 BTC) + (64,061 x 25 BTC) = 12,101,525 BTC (총 발행 예정액의 약 57%에 해당)

- 따라서 임으로 비트코인 만들어 내면 총 통화량과 맞지 않게 되어 부정행위가 즉각적으로 드러남



IV. Bitcoin 중복사용 방지 메카니즘

- 모든 P2P 네트워크으로 운영되는 시스템은 '합의(consensus) 도출'이라는 커다란 문제에 직면
- 널리 퍼져 있고 중앙통제 시스템이 없는 관계로 의사 결정에 어려움이 발생
- 인터넷에서는 이와 유사한 상황이 거의 항상 발생하게 되는데 이 문제를 'Byzantine Generals', 즉 비잔틴 시대의 장군들이 직면한 문제라고 부름
- 이러한 문제는 컴퓨터 시스템에서도 일어남. 특정 부품에서 에러가 발생하여 잘못된 정보를 전달할 경우 정보간에 충돌이 발생함. 이러한 문제들이 모두 Byzantine Generals 문제와 같은 것임
- 실제로 마이크로소프트는 이러한 문제 해결을 Leslie Lamport 등에게 의뢰했고 그 결과 나온 논문이 "The Byzantine Generals Problem"임 (http://goo.gl/Ey7M9c 참조).

Byzantine Generals 문제

- 비잔틴 시대에 여러 나라의 장군들이 적을 공격하기 위해 출병
- 적은 충분히 강해서 ½ 이상의 병력이 동시 출병해야 공격 성공
- 장군들은 '연락병'을 통해서만 정보를 교류할 수 있음
  (한 자리에 모여서 의사 결정할 수 없는 상황, P2P 분산 네트워크 상황)
- 장군들 중 '배신자'는 거짓 정보를 유포하고 아군을 위태롭게 함
- 문제는 공격시간을 '합의'하여 출격해야 하는데 시스템은 없음

➔ 이 상황에서 어떻게 공격 시간에 대한 합의를 만들 수 있을까?

➔ 비트코인은 분산 컴퓨팅 시스템이 직면한, 불가능하게만 보였던 이 문제를 글로벌 규모에서 실질적으로 해결한 혁신 시스템

IV. Bitcoin 중복사용 방지 메카니즘

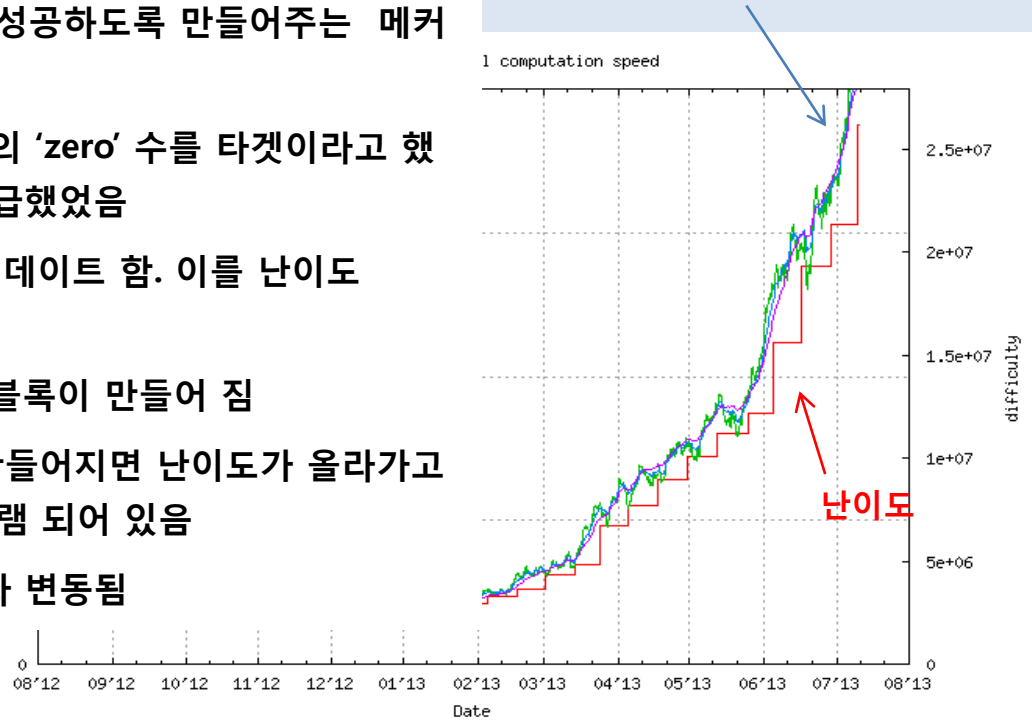
- 비트코인은 'Byzantine Generals' 문제 해결을 위해 세 가지 아이디어를 결합함

  ① 채굴과 인센티브 제공, ② 게임 (혹은 도박) 요소 추가, ③ proof-of-work

- 인센티브는 채굴에 성공했을 때 주어지는 보상(25 BTC) 지급금. 도박적 요소로 승자 한 사람에게만 지급
- 채굴은 앞에서 설명한 것처럼 ***평균적으로 약 10분 마다 문제를 풀어****현 블록에 담긴 거래 내역을 암호화하고 그 해시값을 다음 블록으로 전달하는 과정을 계속적으로 반복하는 것

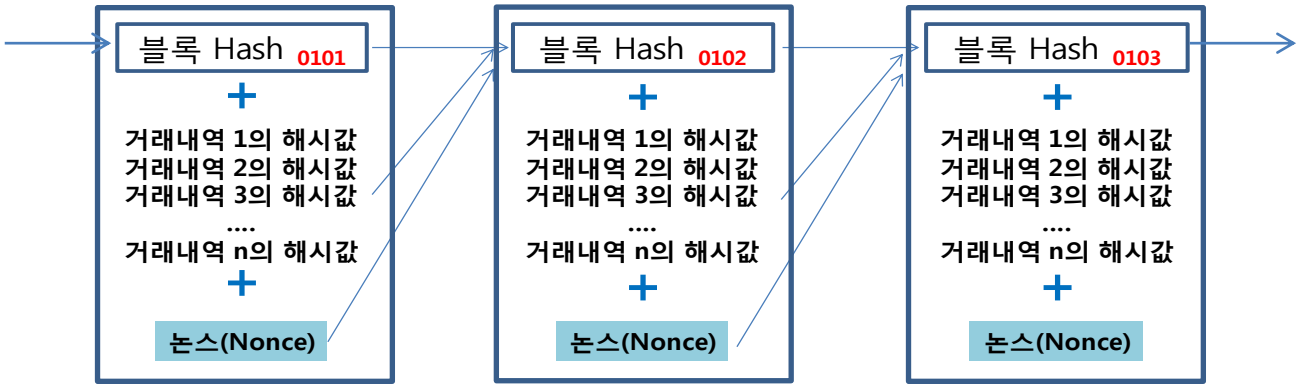
*
- 여기서 평균적으로 약 10분마다 채굴(mining)이 성공하도록 만들어주는 메커니즘이 또 따로 있음
- 채굴(mining)을 설명할 때, 블록 해시 값 첫 부분의 'zero' 수를 타겟이라고 했는데 이 수가 많을 수록 풀기 어려운 문제라고 언급했었음
- 비트코인은 이 첫부분의 'zero'수를 약 2주마다 업데이트 함. 이를 난이도 (difficulty) 조절이라고 함
- 10 분마다 채굴이 성공하면 2주 동안 2,016개의 블록이 만들어 짐
- 따라서 2,016개의 블록이 2주일이 되기도 전에 만들어지면 난이도가 올라가고 2주일보다 늦어지면 난이도가 내려가도록 프로그램 되어 있음
- 채굴 시간은 <u>채굴 참여자 수</u>와 <u>컴퓨팅 파워</u>에 따라 변동됨

2주동안 계산되는 해시 수
이동 평균 (컴퓨팅 파워)

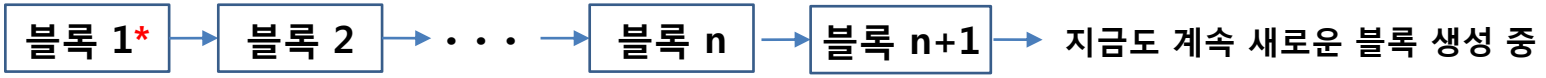


IV. Bitcoin 중복사용 방지 메카니즘

- Proof-of-Work(POW)은 채굴(mining)으로 만들어지는 새로운 블록들의 연결 고리 (a chain of blocks)



- 위 그림을 좀 더 단순화 하면 다음과 같이 블록들이 고리로 연결된 줄기 모양이 됨



* 블록 1, 즉 최초의 블록은 2009년 1월 3일 사토시 나카모토에 의해 만들어짐
(비트코인 창조의 순간)

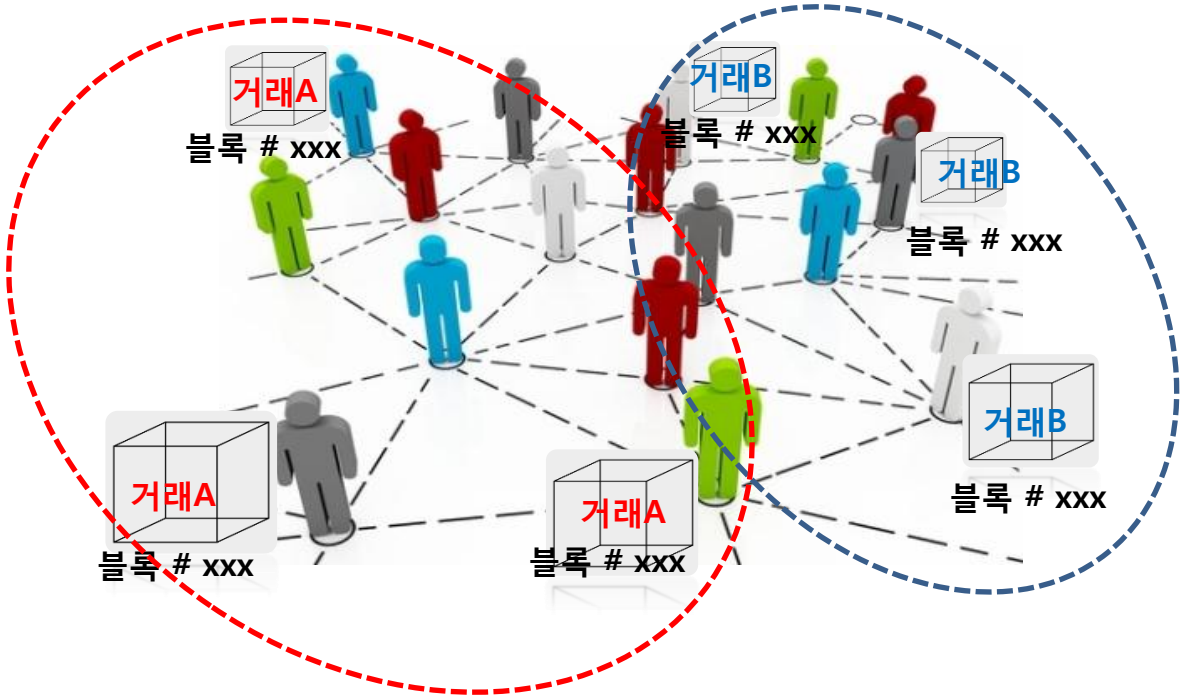
- 한 사람이 자신의 비트코인을 두 곳에 보낼 때, 즉 중복 사용하는 문제의 해결책은 '블록 줄기의 길이'임
- 사토시 나카모토는 이 개념을 'The longest chain wins'라고 설명하고 있음

다음 페이지에서 메커니즘을 좀 더 자세하게 설명하겠음

IV. Bitcoin 중복사용 방지 메카니즘

- 먼저 비트코인 네트워크에 있는 모든 노드는 가장 최근, 즉 가장 높은 번호를 가진 블록을 가지고 있으며 새 거래 내역의 해시 값과 임의로 주어진 논스(Nonce)를 조합하여 다음 블록을 만들기 위해 경쟁
- 모든 비트코인 거래 내역은 모든 노드에게 전달됨
- 한 사람이 비트코인을 중복 사용하면 그 거래 내역이 각각의 노드로 전파될 때, 각 노드는 '충돌'하는 내역을 가진 두 거래 중 하나 만을 접수 (원칙은 먼저 도착하는 거래 내역만 접수)
- (*부정 사용자가 거래1과 거래2로 중복사용 할 경우*) 비트코인 네트워크는 글로벌 단위이기 때문에 노드들 중 일부분은 거래A를 가지고, 나머지 일부분은 거래B를 가지고 작업을 수행(채굴)하는 상황이 발생함

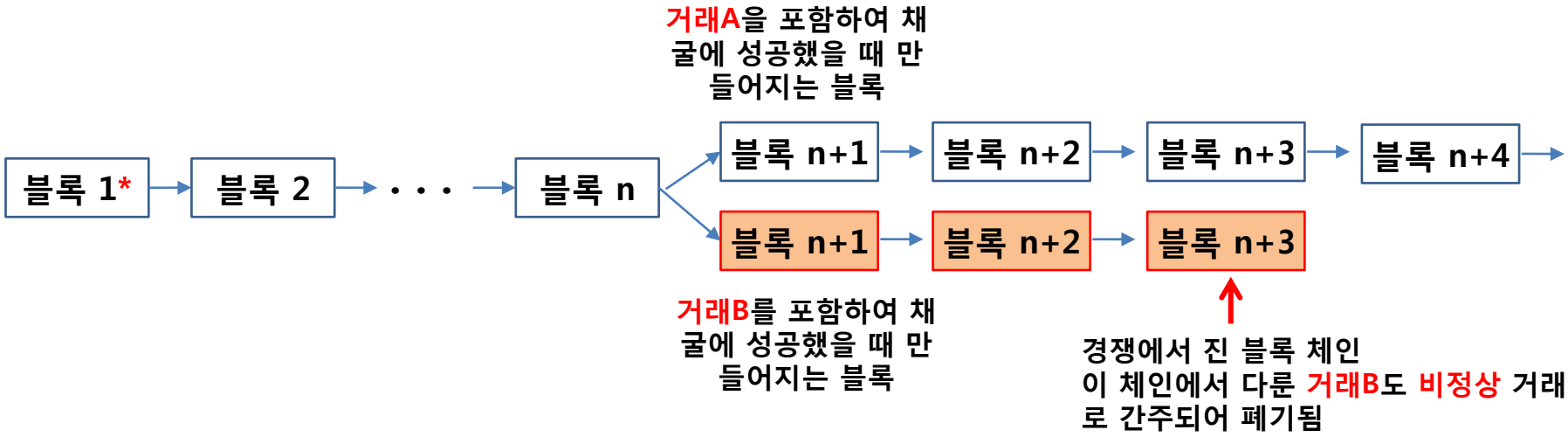
거래A를 먼저 접수한 노드들



거래B를 먼저 접수한 노드들

IV. Bitcoin 중복사용 방지 메카니즘

- 앞 페이지에서 설명한 상황을 블록 체인으로 그려 보면 다음과 같은 상황이 연출됨

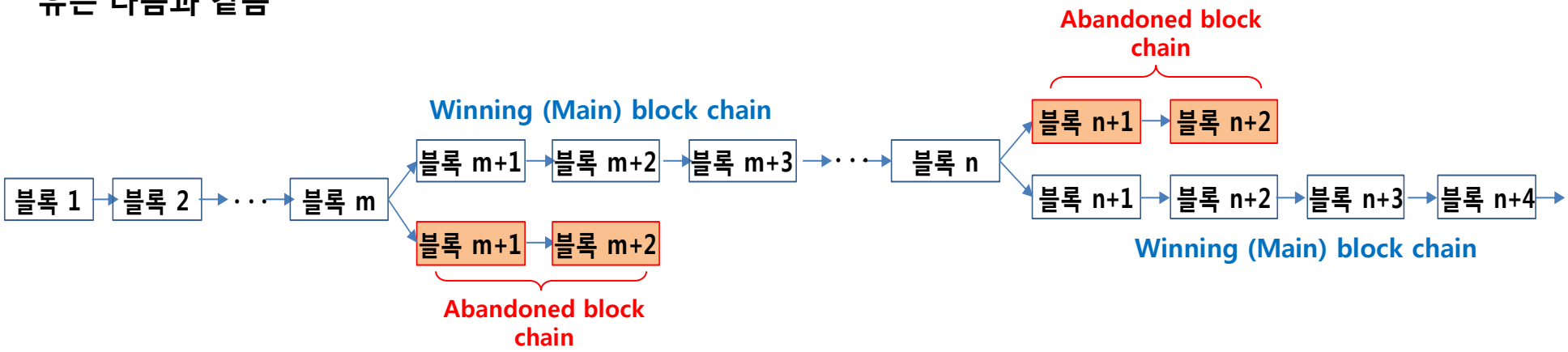


- P2P 진영은 둘로 나뉘어 서로 다른 거래 내역을 담은 데이터를 바탕으로 채굴 경쟁을 함
- 그러다 한 진영이 먼저 다음 블록을 만들어 내는 순간, 즉 한 진영이 만들어 내는 블록 체인의 길이가 다른 한쪽의 블록 체인보다 길어진 순간 경쟁은 종료!
- 비트코인 네트워크는 가장 긴 블록 체인의 블록을 전체 P2P 네트워크로 전파하고 모든 노드들은 그 가장 긴 체인의 끝에 있는 블록을 가지고 다음 채굴 작업을 시작하게 됨
- 따라서 한 사람이 동일 비트코인을 중복 사용할 경우, 두 거래 중 가장 긴 블록 체인을 만들어 내는 쪽에 접수된 거래만 '정상'적인 것으로 처리되며, 긴 블록 체인 만들기 경쟁에서 실패한 블록에 포함된 거래는 '비정상' 거래로 간주되어 자동으로 폐기됨

IV. Bitcoin 중복사용 방지 메카니즘

Byzantine Generals 문제 해결책

- P2P 분산 네트워크에서 필연적으로 마주치게 되는 '합의'도출 문제에 대해 'the longest chain'이 해결책이 되는 이유는 다음과 같음



- 위 그림에서 붉은 색으로 된 블록은 'Byzantine Generals' 문제 중 배신자 (혹은 비트코인 네트워크의 공격자)들이 퍼뜨린 '거짓 정보'가 담겨져 있는 것이데 이러한 정보가 체계적으로 소멸되는 지를 보여줌

- 결국 Winning block chain은 '충성스럽고 정직한' 장군들의 '협업 증거 (Proof-of-Work)'이며 과반수 이상의 장군들이 정직하게 협업하게 되면 '공격자'들이 유포하는 거짓 정보는 자연스럽게 소멸됨

- 따라서 다수의 정직한 참여자들이 협업하면 '부정직한' 네트워크 공격자보다 훨씬 빠르게 일을 해 나갈 수 있으며 그 결과 가장 긴 블록 체인(the longest block chain)을 만들어 내고 이를 활용하여 공격자들의 거짓 정보를 무력화시킬 수 있음 ← Byzantine Generals 문제 해결 (중복 사용 문제 해결)

IV. Bitcoin 중복사용 방지 메카니즘

- 중복사용의 또 다른 방법은 거래를 한 후 정상 블록 체인에 있는 블록의 정보를 해킹하는 것
- 하지만 이 경우, 부정사용자 혹은 '비트코인 네트워크 공격자'는
  1. 정상블록의 해시를 역으로 계산하여 거래 정보를 얻고
  2. 이 거래 정보를 다시 해킹하여 자신이 거래한 내역을 다른 곳에 사용하는 내역을 만들고
  3. 이 해시값을 가지고 다시 다음 블록을 만든 후 다른 거래 기록들을 더하여 계속 블록 체인을 만들어
  4. 결국에는 그 블록 체인 길이를 '정상 블록 체인'보다 빠르게 증가시켜야 하는데 이는 거의 불가능함

- 사토시 나카모토는 비트코인 네트워크에 있는 컴퓨팅 파워가 압도적으로 '공격자'에게 쏠릴 경우를 우려하고 있지만 그러한 압도적인 컴퓨팅 파워를 불법적으로 사용하여 얻을 수 있는 경제적 이익이 전혀 'feasible'하지 않기 때문에 그러한 일은 일어나지 않을 것이라고 전망

- 한 아티클에 따르면 2011년 중반 새로운 블록(상자)를 만들기 위해 채굴자들이 계산 해시값 계산 횟수는 7,500조 이상이었다고 함 (정확히는 7,539,609,386,691,347번, http://goo.gl/1nqJAX 참조)

- 약 10분에 한 번씩 채굴 경쟁을 지속해야 하는데 특정 집단이 나머지 전체가 작업하는 컴퓨팅 파워를 지속적으로 압도하지 않을 경우 결국 블록 체인 만들기 경쟁에서 지게 되어 있기 때문에 해킹은 경제적으로 매우 '비경제적인' 행위가 되어 버림

IV. Bitcoin 중복사용 방지 메카니즘

정리

- 실물 화폐의 경우 중복사용은 '제 3의 기관'이 개입하여 해결함 (은행의 전산망)
- 비트코인에서 중복사용 문제는 가장 긴 블록 체인(가장 높은 번호를 가진 블록이 있는 체인(줄기))에 의해 해소됨. 다시 말하면 가장 높은 번호를 가진 블록이 있는 체인에 기록된 거래가 '정상'거래로 인정됨
- 따라서 P2P 분산 네트워크에서의 '합의(consensus)' 도출 문제인 'Byzantine Generals Problem'을 비트코인은 'the longest chain' 아이디어를 통해서 해결함

- 다시 사토시 나카모토의 논문을 인용하여 P2P 네트워크에서 일어나는 일을 정리하면 다음과 같음

1. 새로운 거래는 모든 노드에게 전파됨 (broadcast 됨)
2. 각각의 노드는 새로운 거래내역을 블록(상자)에 수집함
3. 모든 노드는 세 가지 정보(현 블록의 해시값 + 거래 해시값 + Nonce)를 활용하여 다음 해시값 계산
   (이 과정이 바로 채굴(mining) 과정임)
4. 새로운 해시값(proof-of-work)이 발견되면, (그 결과로 만들어진) 새 블록을 모든 노드에 전파
5. 노드는 새 블록이 '이미 사용되지 않은, 즉 정당한 거래내역만을 포함하고 있을 때' 그 블록을 접수
6. 노드가 블록의 수용을 인정하는 것은 새 블록에 포함된 해시값을 다음 블록 만들기에 사용하는 것임

- 비트코인 사용자는 수시로 네트워크에서 이탈하거나 재접속해도 문제 없음. 재접속 했을 때 네트워크에서 가장 긴 블록 체인만 업데이트 하면 되기 때문임

V. 추가 정리 및 시사점

추가 정리

- 비트코인 아이디어는 처음 2007년에 나타남. 이후 오픈소스 형태로 개발되어 옴
- 아이디어 출발점은 양자간 직거래 시스템을 만들 수 있으면 수수료가 없어져 효용이 증가한다는 것이었음
- 이를 위해 수수료를 부과하는 '제 3 기관'의 개입이 없이 안전한 거래 시스템 구축이 문제가 되었으며
- 이 문제를 해결하기 위해 암호화와 P2P 네트워크를 통한 부정 방지 시스템 구축이 핵심 과제로 부상함

- 사토시 나카모토(Satoshi Nakamoto)는 2008년 비트코인에 대한 아이디어를 종합한 논문을 발표

- 사토시 나카모토 2009년 1월 3일 첫 비트코인 블록을 만들고 50 BTC를 받으면서 마침내 비트코인 탄생

- 비트코인 시스템 이해에는 다음 개념을 이해하는 것이 중요
  - 비트코인은 일련의 디지털 사인으로 연결된 전자 화폐 (a chain of digital signatures)
  - 암호화(공개키와 비밀키) & 해시(Hash)
  - 블록과 채굴(mining)
  - 타겟(target)을 활용한 난이도 조절
  - 가장 긴 블록 체인을 활용한 중복사용 방지 (Byzantine Generals Problem 해결)

- 비트코인 거래는 암호화로 익명성이 보호된다고 알려졌으나 연구에 따르면 신원 추적이 어렵지 않다고 함

  Reid, F. & Harrigan, M. (2011), "An Analysis of Anonymity in the Bitcoin System" (http://goo.gl/t8wSr2) 참조

V. 추가 정리 및 시사점

시사점

- 비트코인은 '화폐'라는 측면에서 아직도 많은 한계를 가지고 있지만 '글로벌 단일 통화'란 점은 매우 중요

  - 직거래를 통해 無수수료 시스템을 만들려 했지만 제 3 기관 개입이 없어도 수수료는 여전히 존재
    (향후 채굴 보상금 지급액은 약 4년마다 ½로 줄어들도록 설계되어 있으며 부족분은 수수료로 지급될 것으로 전망)
  - 거래증가 → (화폐) 수요증가 → 가치증가 선순환을 타게 되어 있는데 여기서 deflation 문제 발생
    (현재 비트코인을 가지고 있는 사람은 비트코인 가치가 증가함에 따라 점점 더 비트코인을 사용하지 않게 되는 문제)
  - 거래를 되돌릴 수 있는 방법이 없어 물건을 팔고 돈을 받는 사람은 유리, 구매자는 불리
  - 비록 화폐로서 성장 초기라 해도 변동성이 너무 커 화폐로서 안정성 확보까지 갈 길이 많음

  ➔ 하지만 글로벌 단일 통화가 출현했다는 점은 매우 중요 (인터넷 기업들의 사업에 꼭 필요했던 요소)

- 비트코인은 화폐로서의 가능성 외에도 'Technology 측면에서 이루어 낸 혁신'부분에 주목해야 함

  - 비트코인은 P2P 네트워크가 직면하는 '합의도출, 관리' 문제에 대해 실질적 해결책을 제시
  - 최고 수준의 수학과 첨단 암호화 알고리즘을 결합하여 거래 기록을 보호 기술 도입
  - P2P 네트워크의 'Byzantine Generals' 문제를 채굴(mining)과 The longest chain 개념으로 풀어냄
  - 위 모든 작업을 인터넷 오픈소스 프로젝트로 추진하여 이루어 낸 점도 평가 받아야 하는 부분

  ➔ 비트코인은 Wiki가 가지고 있는 문제를 해결하며 한 단계 업그레이드 시킨 놀라운 혁신
  Wiki는 자발적 참여를 통해 빠른 정보교류와 성장을 제공하지만 '오류나 잘못된 정보'를 없애지 못함.
  비트코인 시스템은 오류를 체계적으로 배제시키는 솔루션을 제공하여 Wiki를 한 단계 업그레이드

V. 추가 정리 및 시사점

시사점

- 비트코인에 숨어 있는 기술들은 인터넷 기업들에게 많은 기술적 '인사이트'와 사업 기회를 제공
  - 인터넷 상에서 거래될 수 있는 80여 종의 유사 화폐가 만들어지고 유통되고 있음
    (이는 기본적으로 인터넷 전체, 즉 글로벌 수준에서 단일한 시스템으로 작동하는 화폐에 대한 수요가 있음을 보여줌)
  - 수학적 암호화 기술, 분산 시스템의 합의도출, 체계적 오류 배제 시스템 기술은 글로벌 사업을 준비 하고 있는 startup들에게 많은 영감을 줄 수 있음
    (제공하고자 하는 서비스를 이러한 기술과 결합할 경우 보다 안정적이고 광범위한 지역 대상의 시스템 가능)

- 실제로 미국에서 펀딩에 성공한 startup들 중 상당 수는 비트코인에 관한 것들임

[비트코인 관련 스타트업들]

- 비트코인의 중개, 환전, 결제 솔루션 등과 관련된 스타트업 활성화로 생태계 형성
- 개인 간 비트코인 거래의 중개 역할을 하는 거래소 뿐 아니라 (ex. Mt.Gox, Korbit 등)
- 실시간 또는 고정 환율로 환전해주는 사이트, 대출 중개 사이트 및
- 온/오프라인의 매장에서의 결제 솔루션 제공 서비스 등 다양한 스타트업 등장