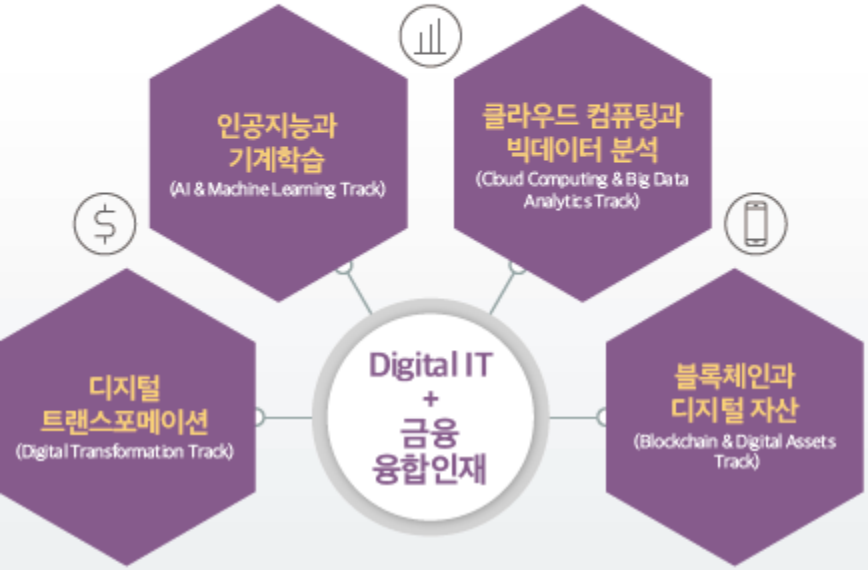
Blockchain Economy

이흥노 (Heung-No Lee)
GIST, South Korea
여의도 디지털금융대학원

Home page: http://infonet.gist.ac.kr
Facebook/Publication ID: Heung-No Lee

디지털금융전문가과정

DIGITAL FINANCE MASTERSHIP PROGRAM



2021 봄학기

- **블록체인과 디지털 자산**
  금융혁신과 신사업준비를 위하여 블록체인 분야에 특화된 기술 교육이 필요한 자
- **클라우드 컴퓨팅과 빅데이터 분석**
  금융 분야에서 클라우드 컴퓨팅 기반 기술 적용과 빅데이터 기획, 분석, 활용을 통한 가치 창출에 관심있는 금융 관련 종사자

2021 가을학기

- **디지털 트랜스포메이션**
  디지털금융/핀테크 분야 백그라운드가 없는 전통 금융 종사자 대상
- **인공지능과 기계학습**
  인공지능과 기계학습 분야를 중점적으로 이수하여 금융 산업에서 해당 분야의 전문가로 성장 하고 싶은 자

KAIST 정영대학

디지털금융전문가과정 Digital Finance Mastership Program
07326 서울특별시 영등포구 국제금융로 10 KAIST 디지털금융전문가과정
(One IFC 17층 KAIST 이의도 캠퍼스)
T. 02) 6274-6181~2 F. 02) 6274-6194 E.kaistdfmp@kaist.ac.kr
www.business.kaist.ac.kr/executive

협력기관 서울특별시 금융위원회

QR 바로가기

280 mm

디지털금융전문가과정

BLOCKCHAIN & DIGITAL ASSETS

Digital Finance Mastership Program

2021년 교육일정 (2021. 3. 17 ~ 7. 14)

KAIST 정영대학

이흥노 교수 강의

교육일자	일자	시간	시간	강의 주제	강사진	모듈
04월 02일	금	19:00~22:00	3H	블록체인 이코노미	이흥노 (GIST)	디지털금융과 블록체인
04월 14일	수	19:00~22:00	3H	비트코인 개념과 핵심 기술	이흥노 (GIST)	블록체인 플랫폼과 서비스

Blockchain, Bitcoin, and Future

JCCI 2018

제28회 통신정보 합동학술대회

THE 28th JOINT CONFERENCE ON COMMUNICATIONS AND INFORMATION

2018년 5월 2일(수)~4일(금), 여수 히든베이호텔

Home | 온라인 사전등록

- JCCI 2018
  - 초대말씀
  - 행사안내 (CFP)
  - 운영위원회
- 논문제출 및 확인
- 저자 논문 발표 안내
- 프로그램
  - 특별프로그램
  - 프로그램
  - 세션정보
- 사전등록
  - 등록절차 안내
  - 온라인 사전등록
- 장소 및 숙박안내
- 사진갤러리
- JCCI 지난 행사

특별프로그램

특별프로그램1

- 제목: Blockchain, Bitcoin and Future
- 연사: **이흥노 교수** (GIST)
- 좌장: **신요안 교수** (숭실대)
- 일시: 5월 2일 (수) 14:40-15:50

블록체인은 2009년에 백서와 SW가 공개되었던 암호화폐 Bitcoin을 통해 세상에 알려졌습니다. 시간의 순으로 발생하는 모든 거래 내역을 순서대로 그때 그때 바로 바로 기록한 것을 블록체인 원장이라고 정의할 수 있습니다. 이 원장을 인터넷에 공개해 놓고 거래내역을 누구나 들여다 볼 수 있게 했습니다. 거래기록 작성은 특정인이나 단체 혹은 국가가 독점하지 못 하도록 하였습니다. 오히려 누구든지 거래원장 기록에 참여할 수 있도록 열어 놓은 분산 형 원장 작성 기술입니다. 누구나 작성에 참여하고 인터넷에 공개된 파일임에도 불구하고 어떤 것이 원본인지를 구분할 수 있도록 전혀 새로운 방식의 원장 동의 프로토콜을 만들었습니다. 또한 암호학적 설계로 원장에 기록된 내용을 임의로 바꿀 수 없습니다. 이 분산원장을 블록체인이라고 칭합니다. 누구나 작성에 참여할 수 있게 열려있고 한 번 입력된 기록은 위변조의 위험 없이 보존되기 때문에 거래에 참여하는 모두에게 신뢰를 얻습니다. 즉 블록체인에 기록된 내용은 발생한 시간과 내용이 순전무결하게 그대로 기록되었고 보존되었다는 것을 믿을 수 있다는 것입니다. Bitcoin은 블록체인을 은행이나 국가의 개입이 필요 없는 암호화폐를 만드는데 사용했습니다. 즉 인터넷에서 코인을 주고 받을 수 있게 만든 것입니다. 마치 실물세계에서 화폐를 건네는 사람과 받는 사람이 대면 거래를 하듯이, 인터넷 상에서 거래당사자가 전자서명과 블록체인을 통해 코인의 소유권을 주고받을 수 있게 하였습니다. 현재까지 약 일천오백여 개의 새로운 암호화폐가 탄생했습니다. 블록체인이 확보해주는 데이터 무결성을 통한 신뢰의 가치는 매우 큽니다. 그로인해 스마트계약, 부동산거래, 전자투표, 보험 및 기부 네트워크관리, 토지관리 등 새로운 응용 분야가 속속 개발되고 있습니다. 세계적인 미래학자 돈 탭스콧은 인터넷이 지난 30년을 지배해온 것처럼 앞으로는 블록체인 혁명이 30년 이상 지배할 것이며 세상의 모든 것을 변화시킬 것이라고 언급하였습니다. 본 특강에서는 어떻게 Bitcoin과 블록체인이 이런 혁신을 이루어 내는지 그 핵심 기술들을 설명하도록 하겠습니다.

블록체인 이코노미

- 주요 용어 정리
- 블록체인 (비트코인, 이더리움)
- 이코노미
- 비트코인의 미래

비트코인 관련 용어 정의

- 개인키/공개키(Private Key/Public Key)
- 디지털서명 (Digital signature)
- 지갑(Wallet)
- 소유권(Ownership right)
- 트랜잭션(Transaction)
- 블록체인(Block chain)
- 블록체인 프로토콜(Protocol)
- 블록체인네트워크 노드(Node)
- 마이너(Miners)

비트코인 관련 용어 정의

- 암호화폐(Crypto currency)
- 암호자산(Crypto assets)
- 비트코인(Bitcoin)
- 탈중앙화(Decentralization)
- 코인 주조(Minting coins)
- 주조 일정(Minting schedule)
- 비트코인 총 발행량(Total bitcoins to be created)
- 반감기(Halving)
- 이중지불방지(Double spending attack)
- 작업증명(Proof-of-Work)

이더리움 관련 용어 정의

- Ethereum
- 버츄얼머신(Virtual machine)
- 스마트컨트렉트(Smart Contract)
- 분산앱(dApp)
- 증표(Token)
- 증권형토큰(STO)
- 호위테스트(Howey Test)
- 분산금융(DeFi)
- 대체불가능증표(NFT)

거래소 및 가상자산사업

- 거래소(Crypto exchange)
- 특금법 21(cf. Financial Action Task Force, 1989)
- 자금세탁방지(AML)
- 신원확인(KYC)
- 가상자산사업자(VASP)
- 예치(Staking)
- 수탁(Custody)

거버넌스

- 온체인 프로토콜
- 오프체인 거버넌스

여러 디지털 화폐

- 가치안정코인(Stable Coin)
- Facebook Libra/Diem
- Central Bank Digital Currencies
- Bitcoin/Ethereum을 개선하겠다고 만든 1만 개 이상의 코인 및 토큰 프로젝트

비트코인 (Bitcoin)

밀튼 프리드만, E-cash 예언,1999

- "I think that the Internet is going to be one of the major forces for reducing the role of government."

https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin

밀튼 프리드만, E-cash 예언,1999

- "I think that the Internet is going to be one of the major forces for reducing the role of government."
- "The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A."

https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin

밀튼 프리드만, E-cash 예언,1999

- "The way I can take a $20 bill, hand it over to you, and then there's no record of where it came from."

https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin

밀튼 프리드만, E-cash 예언,1999

- "You may get that (e-cash) without knowing who I am. That kind of thing will develop on the Internet and that will make it even easier for people using the internet."

https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin

밀튼 프리드만, E-cash 예언,1999

- "Of course, it has its negative side. It means the gangsters, the people who are engaged in illegal transactions, will also have an easier way to carry on their business."

https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin

SATOSHI NAKAMOTO가 CRYPTOGRAPHY MAILING LIST에 보낸 메시지 (NOVEMBER 1, 2008)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at http://www.bitcoin.org/bitcoin.pdf.

Bitcoin: A Peer-to-Peer Electronic Cash System

1. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.
2. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending.
3. We propose a solution to the double-spending problem using a peer-to-peer network.
4. The network time stamps 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.
5. 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.
6. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers.
7. The network itself requires minimal structure.
8. Messages are broadcasted 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.
9. The users involved in transaction remain anonymous.

Satoshi Nakamoto

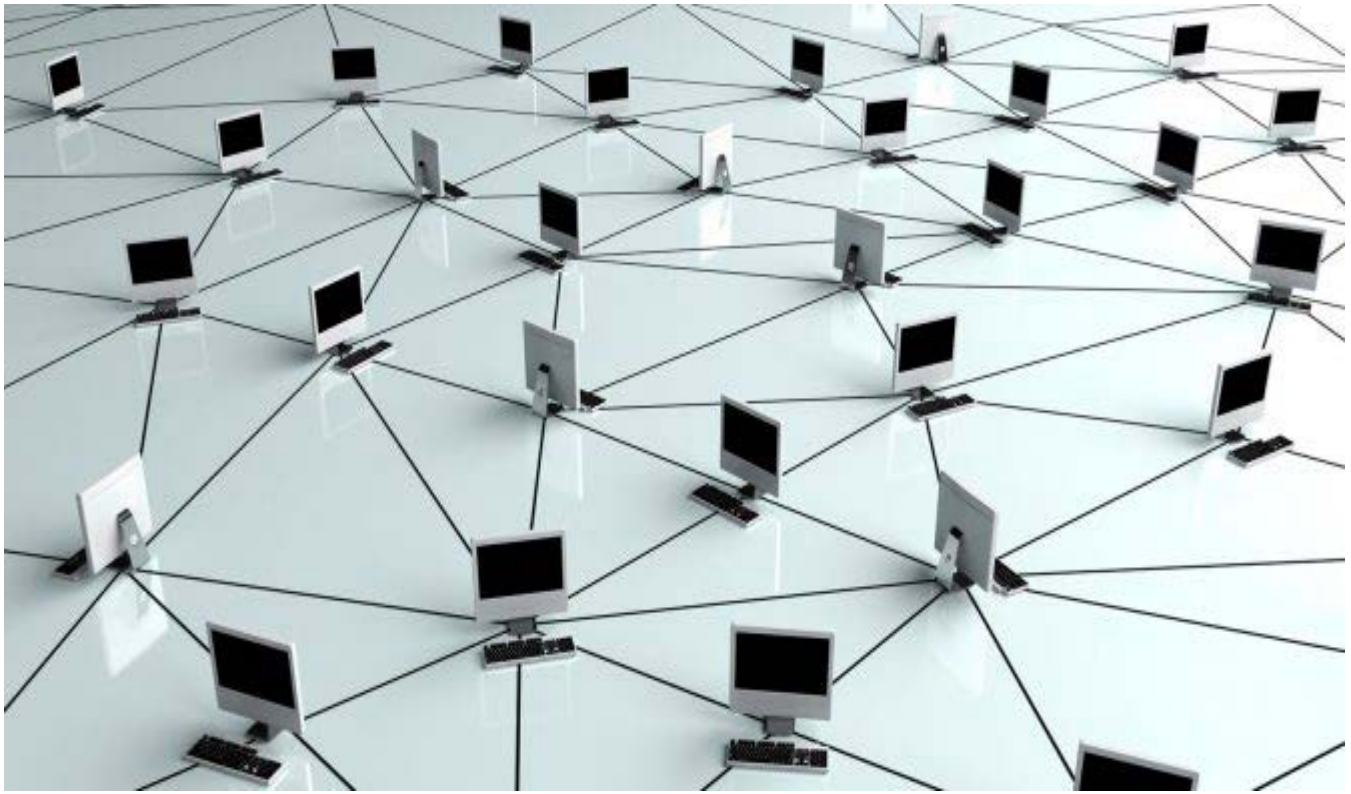
Bitcoin: A Peer-to-Peer Electronic Cash System

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.

비트코인은 인터넷 위에서 동작

P2P 노드 네트워크 구성



YAP섬: 신뢰하고 쓰면 돈이다!

섬마을 사람들은 타지에서 가져온 큰 돌을 돈으로 썼다.
"내 딸 결혼할 때 내가 큰 돌을 김씨 네에 주었다" 라고
공개 선언하면 소유권 이전이 끝난다.

PLANET MONEY

The Island Of Stone Money

Listen · 4:24 Queue Download Transcript

December 10, 2010 · 4:28 AM ET
Heard on Morning Edition

JACOB GOLDSTEIN DAVID KESTENBAUM

There's a tiny island called Yap out in the Pacific Ocean. Economists love it because it helps answer this really basic question: What is money?

멀리 떨어진 두 사람간의 거래

- 지급결제거래: A가 B에게 2 BTC를 보낸다.

A → B 2 BTC

미국에 있는
Adam

한국에 있는
Byungchul

멀리 떨어진 두 사람간의 거래

1. 소유권 증명

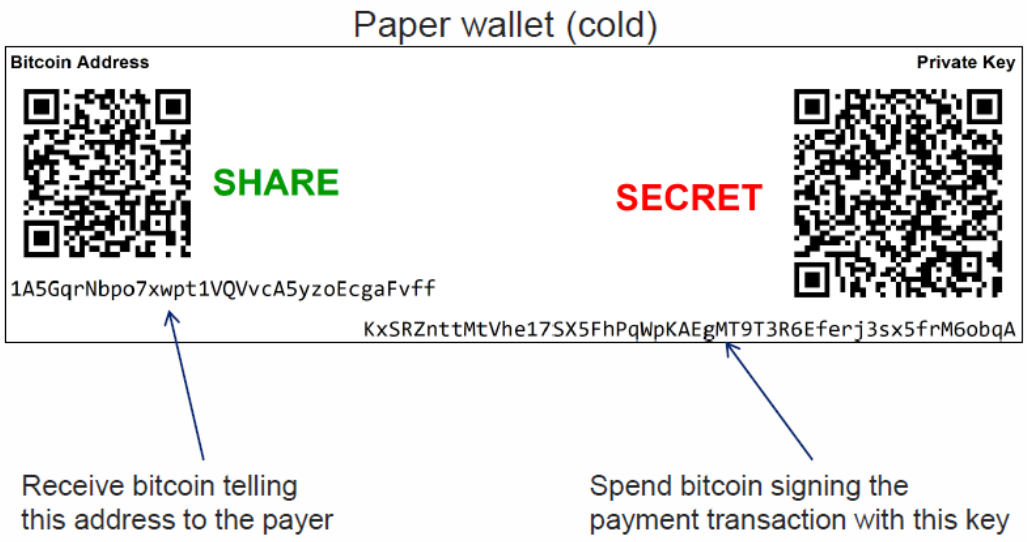
- "A가 2 BTC" 를 진실로 보낼 때
  - A는 2BTC의 소유권을 증명할 수 있어야하고
  - B는 A가 2BTC이상의 소유권을 갖고 있음을 확인할 수 있다.
- "A가 2 BTC"를 거짓으로 보낼 때
  - A는 B를 속일 수 없어야만 한다.
  - 즉 B는 A가 속임수를 쓰고 있음을 확인할 수 있는 수단을 갖고 있다.

멀리 떨어진 두 사람간의 거래

2. 소유권 이전 완료

- A가 2BTC 를 진실로 보냈을 때
  - B는 A가 보낸 2BTC 의 소유권이 자신에게 완전하게 이전되었음을 확인할 수 있다.
- A가 2BTC를 거짓으로 보낼 때
  - B는 A가 보낸 2BTC의 소유권 이전이 완료되지 않았음을 알 수 있다.

지갑 (Wallet), 개인키 와 공개키



Wallets do not store coins. They store addresses (public keys) and private keys.

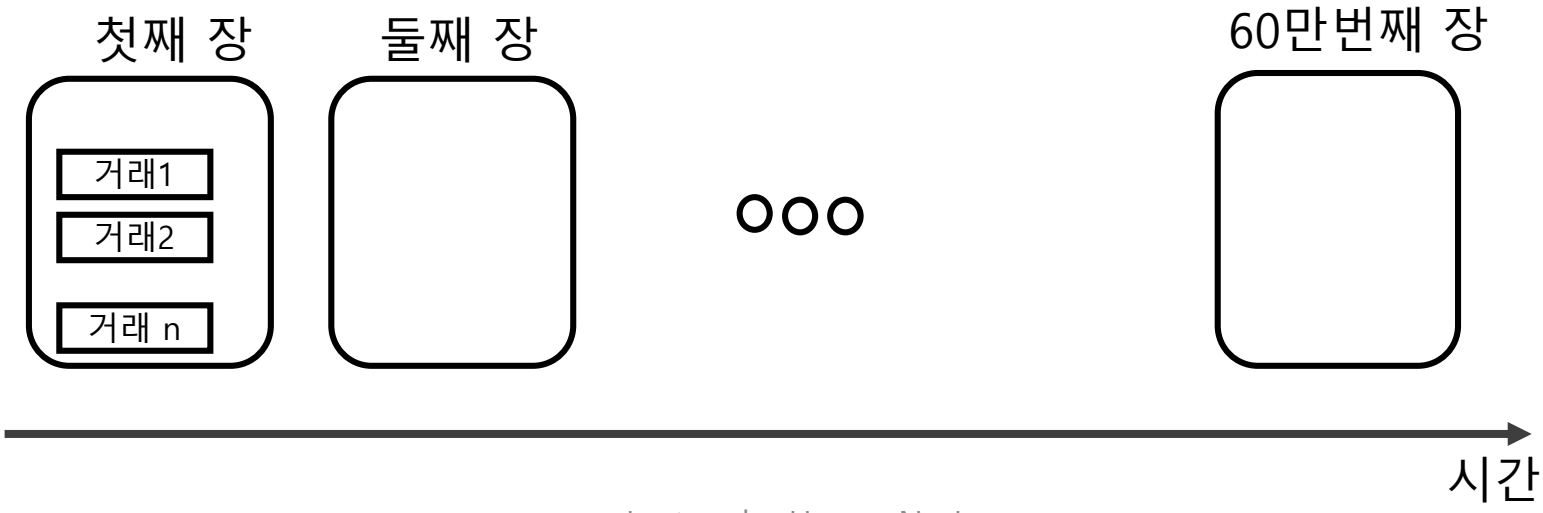
멀리 떨어진 두 사람간의 거래

3. 소유권 증명과 검증, 소유권이전 확인과 완료

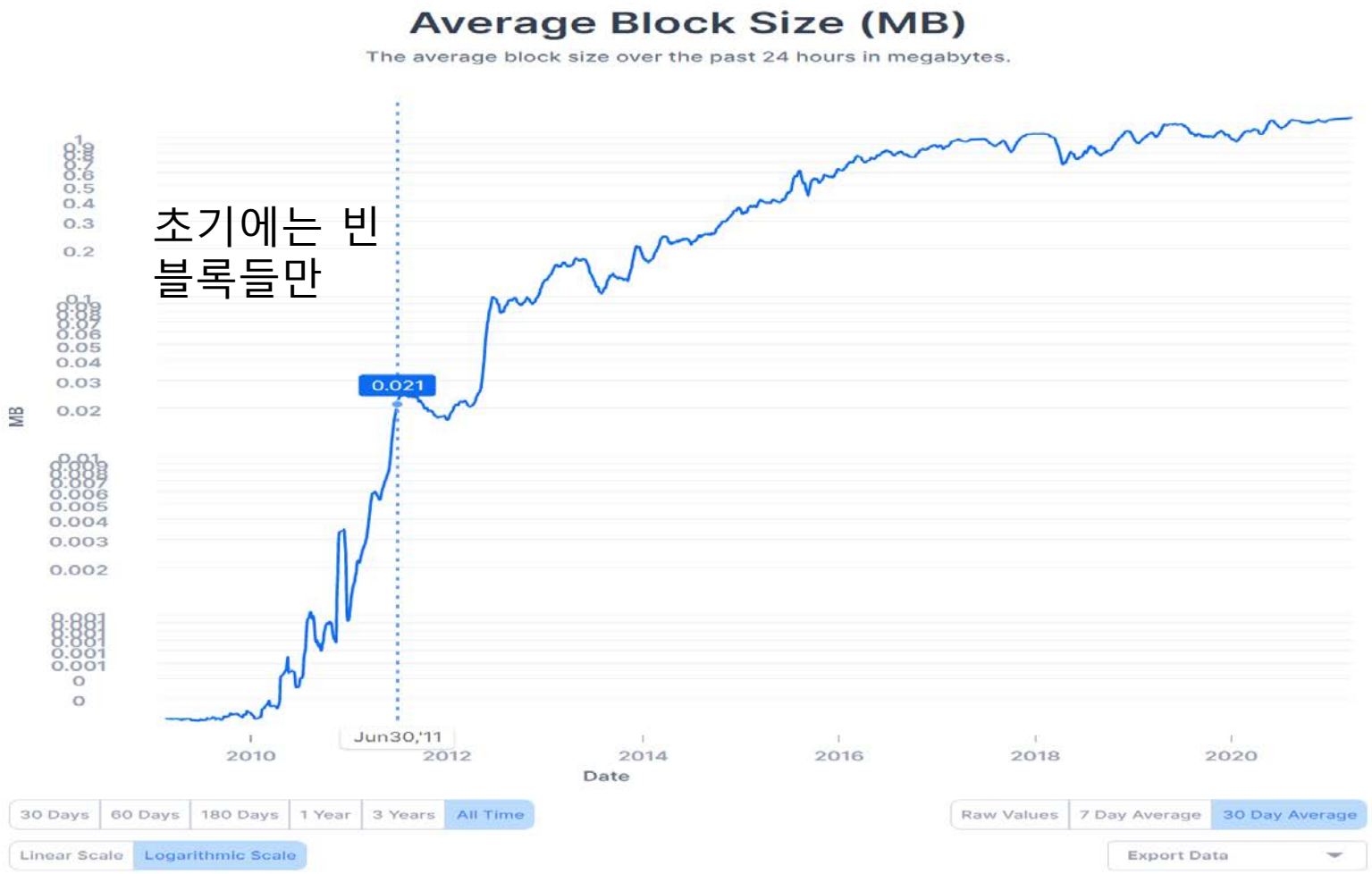
- TX: A는 개인키로 거래를 서명하고 B의 주소(공개키로 만듦)로 코인을 지급한 거래(TX)를 네트워크에 전송.
- 네트워크는
  - TX을 수신하여
  - 검증하고
  - 문제가 없는 거래만 모아 새로운 블록에 담고
  - 블록에 타임스탬프를 찍고
  - 블록 체인의 마지막 장에 연결하여
  - 아무도 바꾸지 못하게 잠근다.

블록체인의 정의

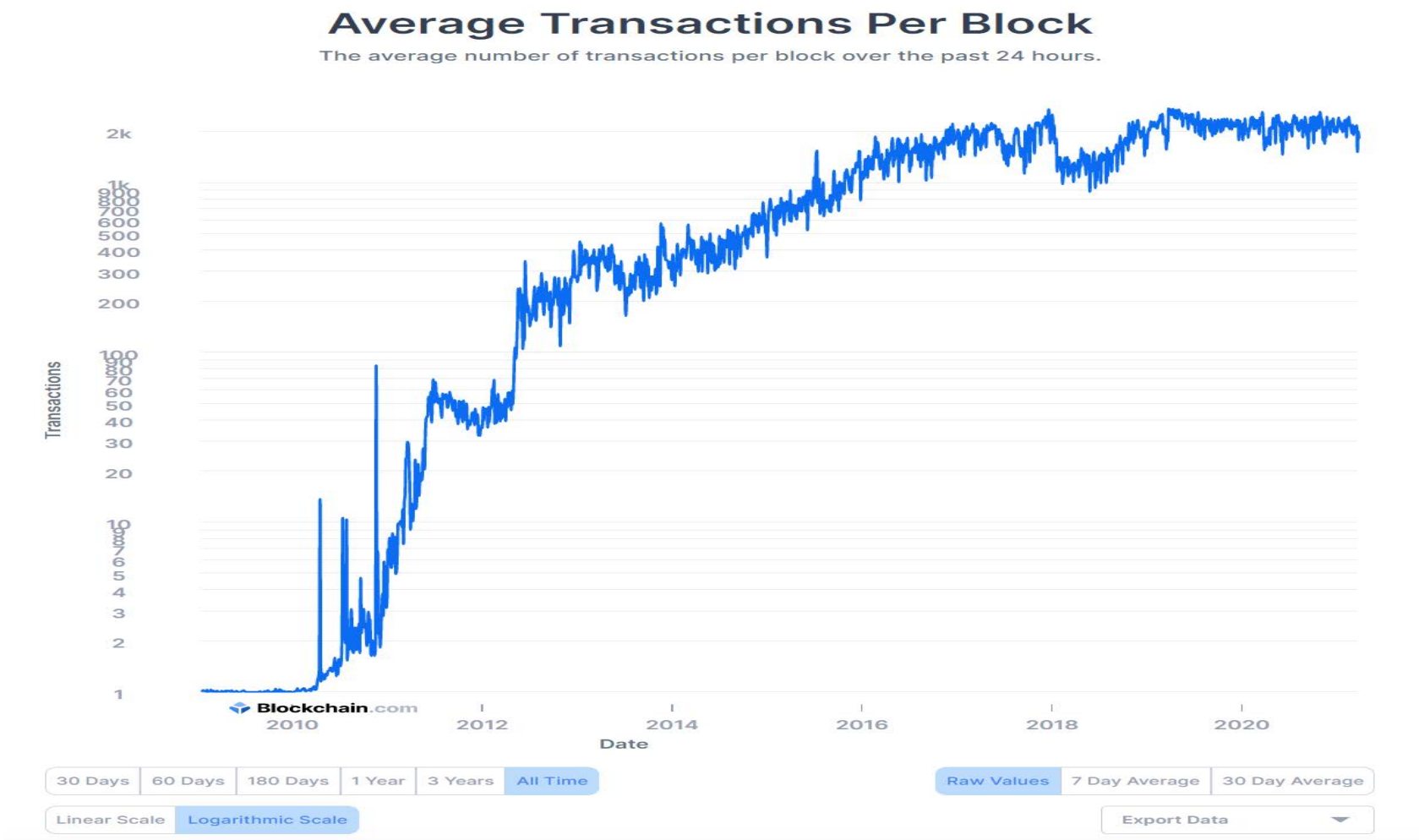
- 블록체인은, 자산 거래가 발생한 시간의 순서에 따라 바로 기록되고, 기록이 완료된 내용은 외부침임이나 기기의 오작동과 같은 장애 가능성에도 불구하고, 작성 당시 그대로 순전무결하고 불변하게 관리되는, 인터넷에 공유되는 원장 임.



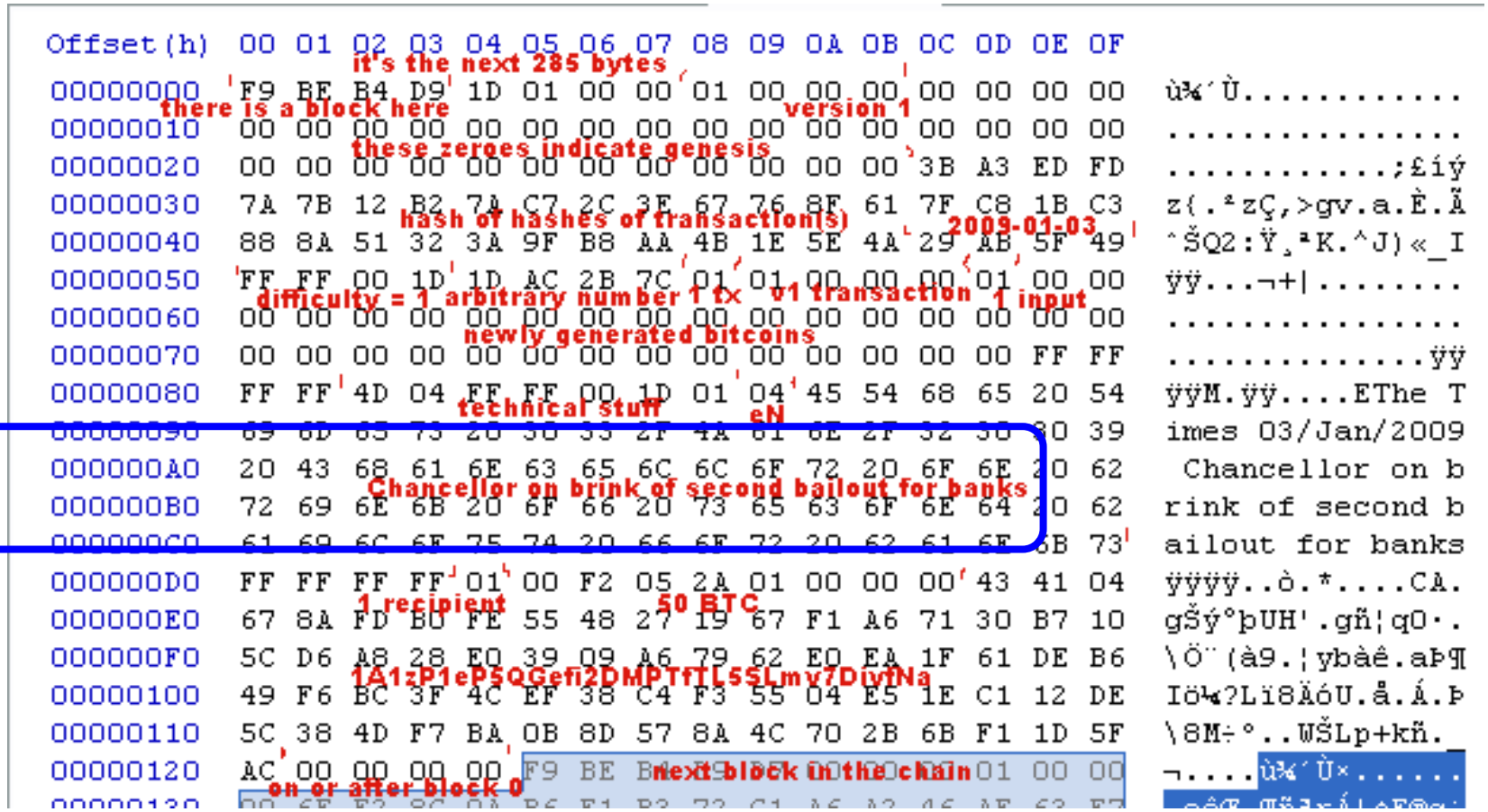
BTC 평균 블록사이즈 1 Mbyte



블록당 TX 개수는 2000 정도



비트코인의 첫 번째 블록


it's the next 285 bytes
there is a block here
version 1
these zeroes indicate genesis
hash of hashes of transaction(s)
2009-01-03
difficulty = 1 arbitrary number 1 tx
v1 transaction
1 input
newly generated bitcoins
technical stuff
eN
Chancellor on brink of second bailout for banks
1 recipient
50 BTC
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
next block in the chain
on or after block 0

Bitcoin Genesis Block

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hoil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1969 levels

Business, page 47

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

인터넷에 공개된 블록체인

- 이 원장을 **인터넷에 공개해** 놓고 거래내역을 누구나 참조해 볼 수 있게 함.
- BTC와 ETH은 공개형 블록체인

전세계 노드 모두 동일한 원장을 공유 (분산원장)

미국에 있는 원장

한국에 있는 원장

누구나 블록생성자로 참여 가능

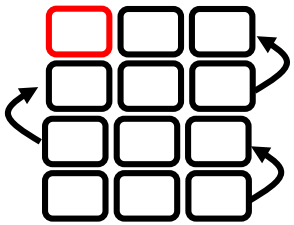
- 거래기록 작성은 누구나 참여할 수 있도록 열려 있음.

프로토콜에 의한 합의

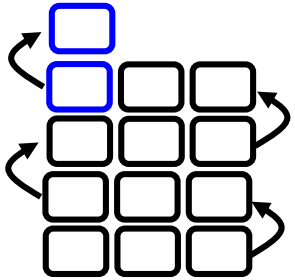
- 어떤 것이 원본인지 판단 가능한 프로토콜

동시에 2개의 다른 체인이 공표될 때
어떤 체인이 원장이 되나?

100번째장 작성
성공! 야호!



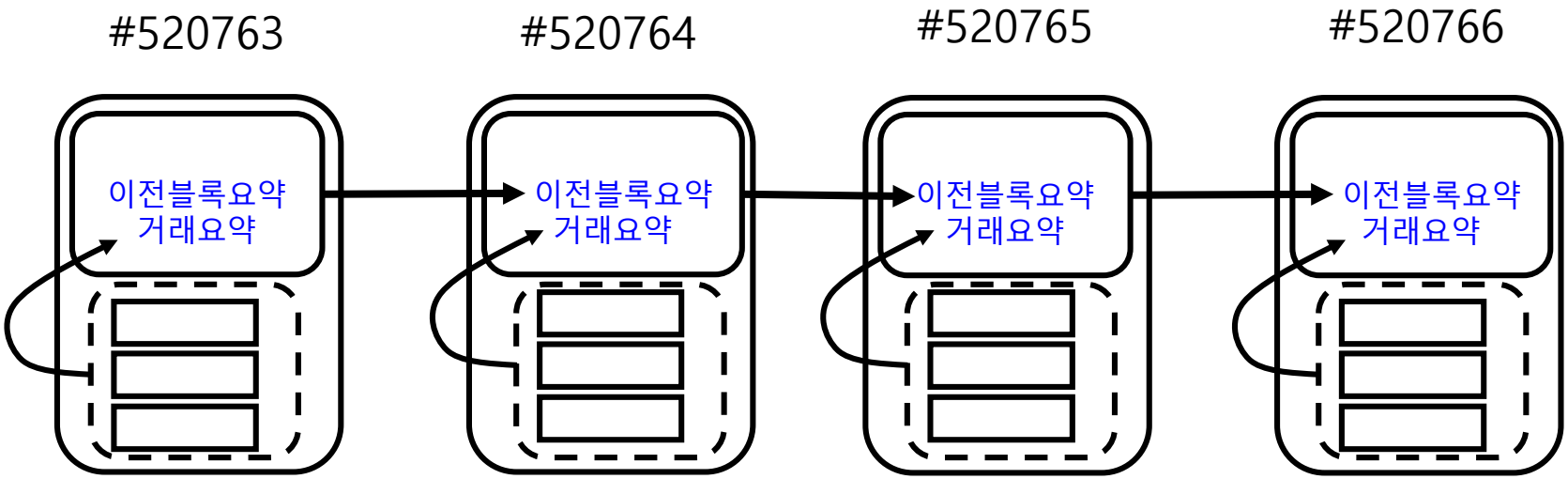
101번째장 작성
성공! 야호!



긴 체인이 승리!

순전무결성, 암호학으로 확보

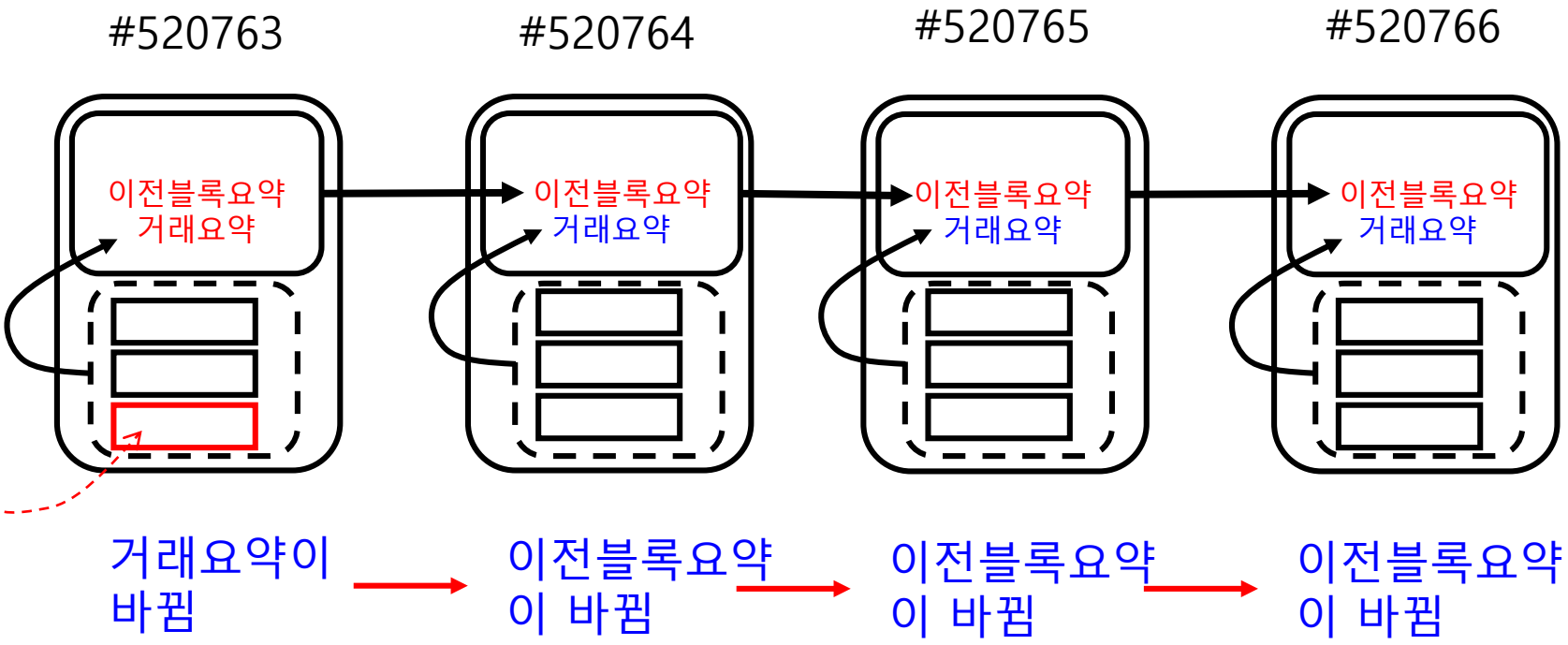
- 암호학적 설계로 원장에 기록된 내용을 임의로 바꿀 수 없음



디지털 파일인데 왜 못 바꿔?

위변조 발생시 바로 간파됨!

- 아래 빨간색으로 표기된 거래에 기록된 내용을 누군가 임의로 내용을 바꿀 때 생기는 일은?



이중거래 방지

- 이중거래를 의심해봐야 하는 사람은 코인을 받는 사람
- 코인을 건네는 자가 동 시간대 혹은 그 이전에 다른 자에게 이미 양도하지 않았는가 확인 필요
- 블록체인에 각 거래가 시간의 순으로 time-stamp가 찍혀 있고 공개되어 있으므로 쉽게 확인 가능 (컴퓨터가 함, 채굴기)

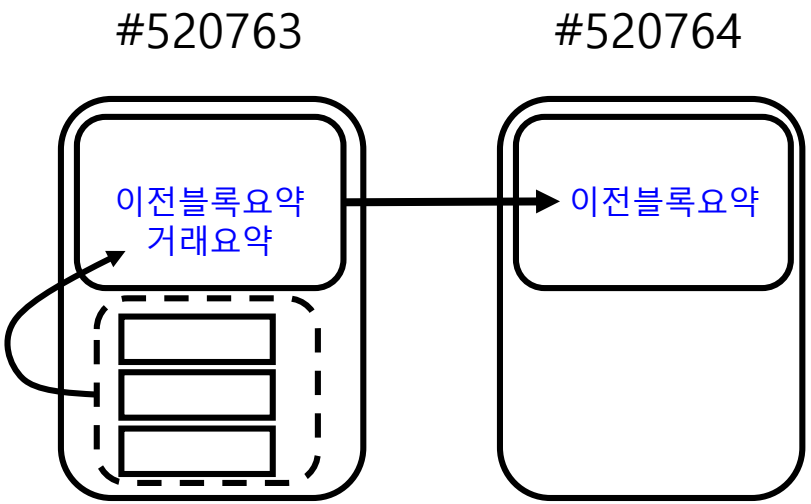
간파되지 않고 위변조하려면?

해당 블록부터 시작해서 그 후 요약을 모두 다시 찾아서 재기록 하면 됨.

이런 짓을 못하게 하기 위해 작업증명이란 것을 수행하게 함.

Proof-of-Work (작업증명)

- 블록요약을 찾는 것을 매우 어렵게 만듦 (시간 소요).
- 가령 하나의 컴퓨터가 좋은 요약을 찾으려면 매우 오랜 시간이 소요되도록 설계.
- 반면에 여러 대의 컴퓨터가 협력하여 찾을 때, 그 중 한대가 단위 시간 안에 답을 찾도록 작업증명 문제를 설계함.
- 블록마다 좋은 이전블록요약을 붙이도록 하므로, 전세계 모든 컴퓨터들이 협력하였음을 증명하도록 함.

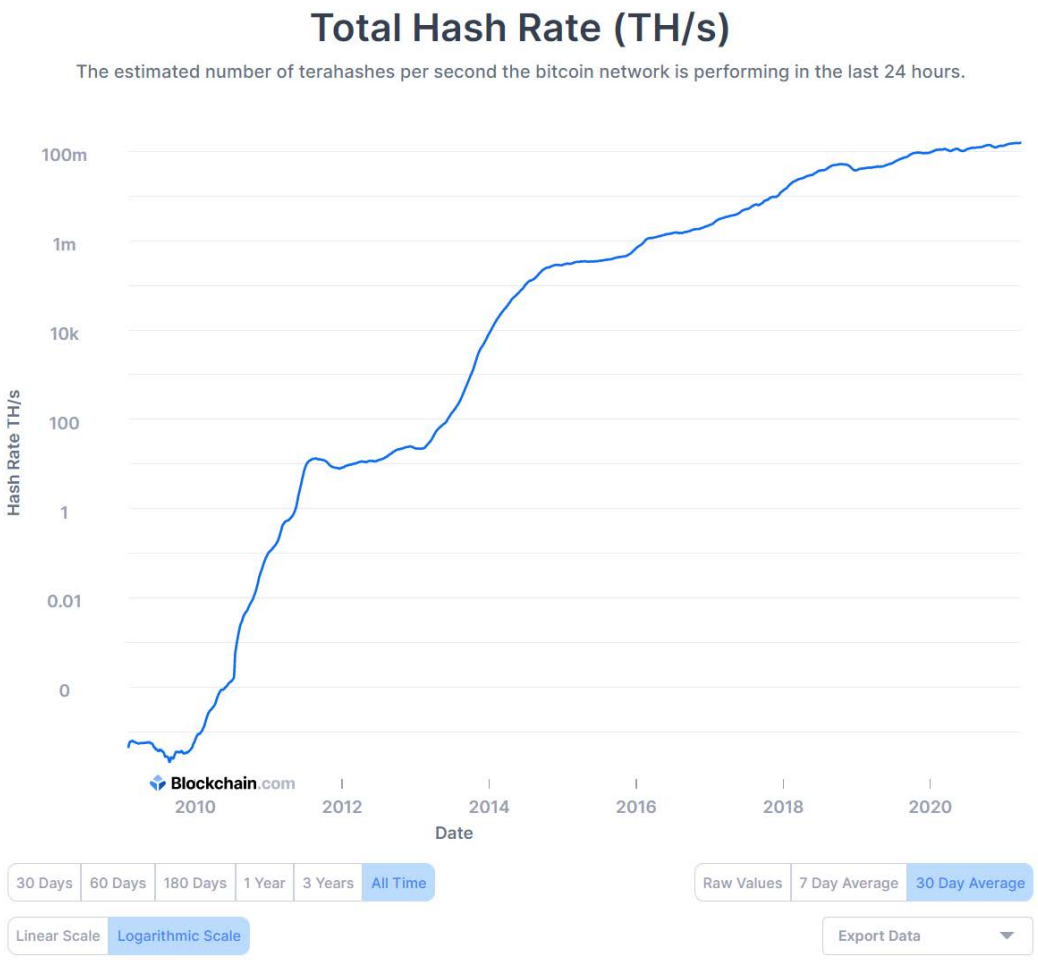


네트워크 해쉬 레잇 = 10^{20} H/sec

이
네트워크를
Attacker가
공격하려면?

시간은?

돈은?



비트코인 네트워크는 전기를 많이 씁니다

Ebit E10, mining **SHA-256 algorithm** with hash rate of **18Th/s** and power consumption of **1650W. 개당 3000불 수준.**

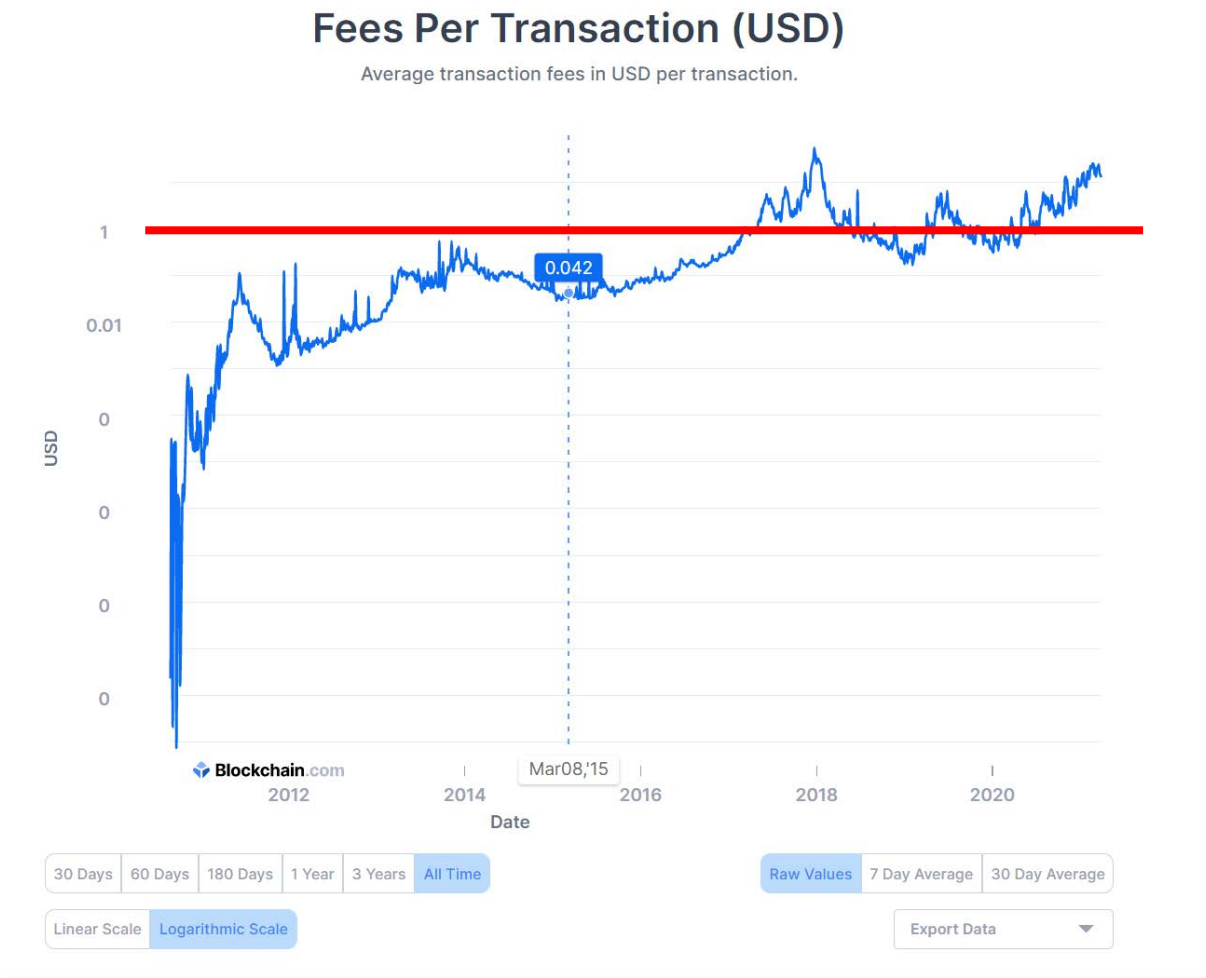
채굴과 보상

- 좋은 블록요약을 찾을 때까지 전세계에서 참여하는 모든 노드들은 각자 컴퓨팅 자원을 동원하여, 해쉬함수 입출력을 반복한다.
  - 채굴 위해 엄청난 전기에너지 사용 비용 발생.

- 작업증명(Proof-of-work)에 성공한 노드에게 일정량의 BTC을 주어 노력에 대한 보상을 줌.

- 채굴자: 작업증명을 하고 블록생성을 수행하는 노드.

평균 TX 수수료는 1 ~ 2 USD



하루 채굴 매출 = 10 ~ 100 M.USD

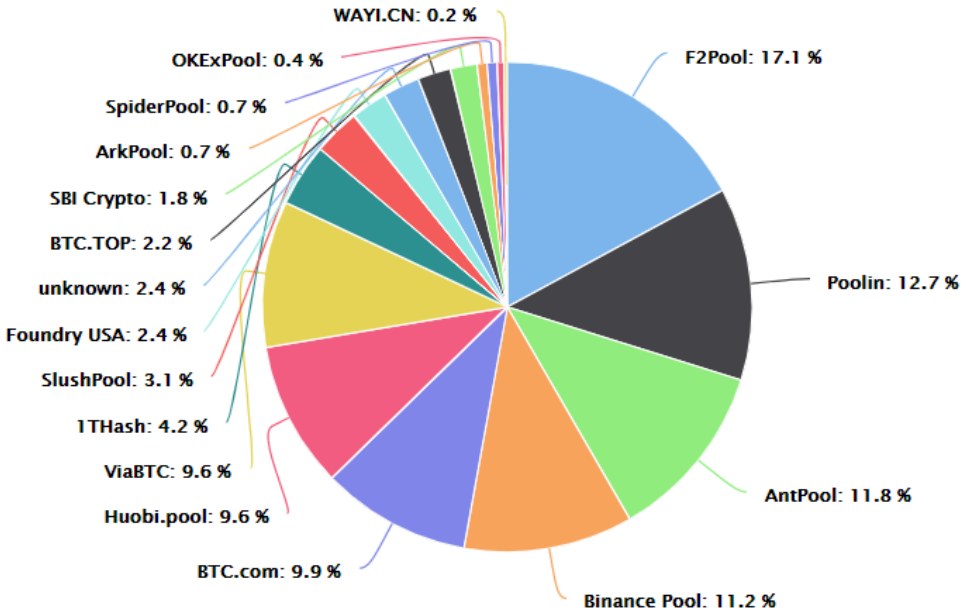
1000억 원

100억 원

6 x 24 = 144 BLs/day
6.25 BTCs/BL
6천 만원/BTC

Bitcoin Mining Pools

- China: 65.08%
- US: 7.24%
- Russia: 6.90%
- Kazakh: 6.17%
- Malaysia: 4.33%
- Iran: 3.80%
- Canada: 0.82%
- Germany: 0.56%



https://cbeci.org/mining_map

마이닝 풀 분포 지도

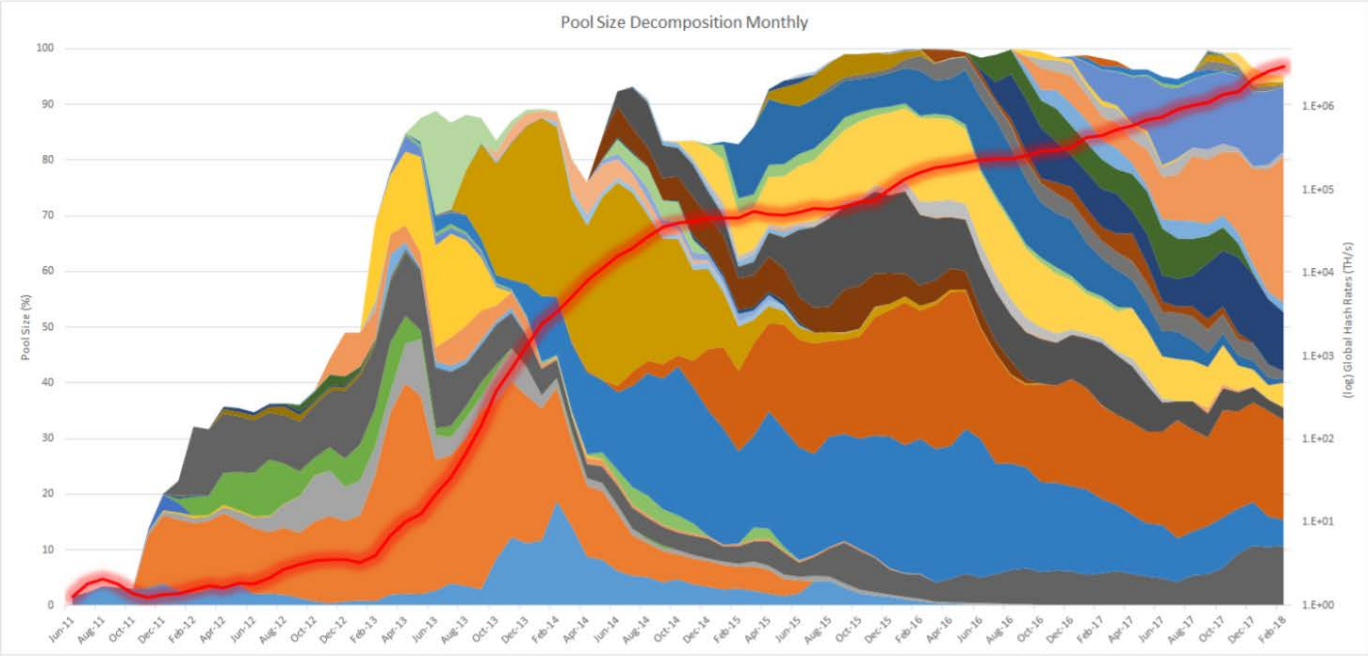

아시아
유럽
북아메리카
태평양
남대서양
아프리카
인도양
오스트레일리아
남아메리카
Bing
© 2021 TomTom, © 2021 Microsoft Corporation Terms

Decentralized Mining in Centralized Pools

https://www.gsb.stanford.edu/sites/gsb/files/fin_11_19_cong.pdf

Figure 1: **The evolution of size percentages of Bitcoin mining pools**

This graph plots (1) the growth of aggregate hash rates (right hand side vertical axis, in log scale) starting from June 2011 to today; and (2) the size evolutions of all Bitcoin mining pools (left hand side vertical axis) over this period, with pool size measured as each pool's hash rates as a fraction of global hash rates. Different colors indicate different pools, and white spaces indicate solo mining. Over time, Bitcoin mining has been increasingly dominated by mining pools, but no pool seems ever to dominate the mining industry. The pool hash rates information comes from Bitcoinity and BTC.com). For more details, see Section 5.



풀 다각화 통한 위험 분산

과

큰 Pool 수수료 높은 구조

참여자 신뢰 확보

- 누구나 작성에 참여할 수 있게 열려있고 한 번 입력된 기록은 위변조의 위험없이 보존되는 순전무결성을 입증하였기 때문에 거래에 참여하는 모두에게 신뢰를 얻음.

- 즉 블록체인에 기록된 내용은 거래가 발생했던 시간과 거래내용이 순전무결하게 그대로 기록되었고 보존되었다는 것을 거래에 참여하는 모두가 신뢰할 수 있다는 것임.

비트코인 익명성

누구나 열람할 수 있는 거래 장부는 사실 암호화 되어 있음.
해당 동전의 소유권을 어느 주소가 갖고 있는지 확인 할 수는 있으나,
소유권자가 아니면 그 권한을 행사 할 수는 없게 만들어 졌음.

거래 A → B 2 BTC 예시에서
A는 Adam이 그의 개인키로 만든 서명
B는 ByungchuI이 그의 공개키로 만든 주소

"**B** may get that (e-cash) without knowing who **A** is. That kind of thing will develop on the Internet and that will make it even easier for people using the internet." **M. Friedman**

WEF 암호화폐 전망

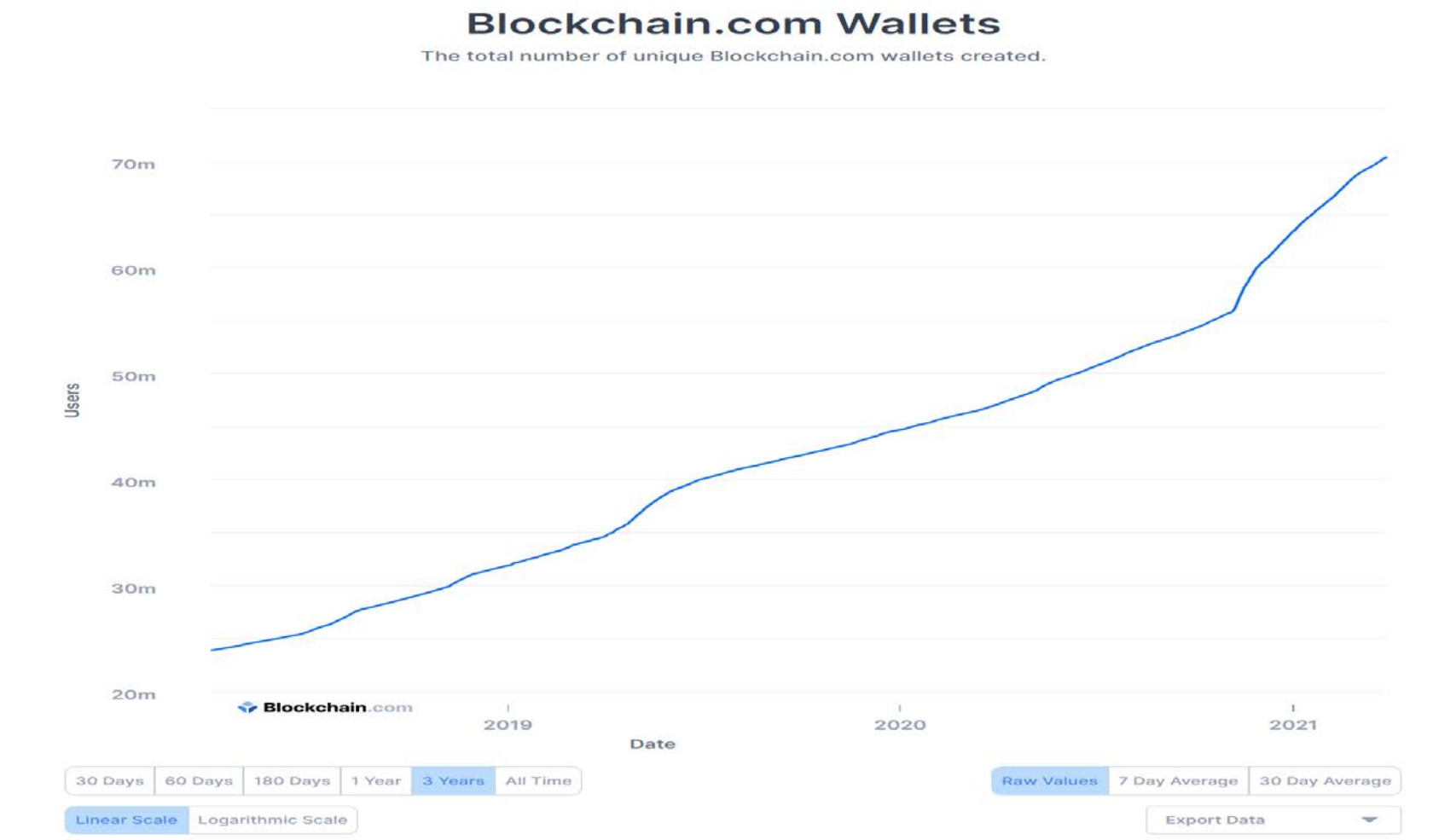
- 2015 WEF 5월 보고서 예측,
  - "27' 전세계 GDP 10% 암호 화폐로 보관",
  - "23' 국가가 세금을 암호화폐로 징수 시작"
- 2016 다보스포럼, 빅데이터와 블록체인이 승자
- Korea GDP 1.4 TUSD 2015에서 1.8 TUSD 2027 전망
- World GDP 80 TUSD 2015에서 100.0 TUSD 2027 전망
- Cryptocurrency, 10 BUSD 2015, 10 TUSD 2027 전망

  (0.01% → 10%, 일천 배 성장)

비트코인 시총 ~ 1 T. USD (2021)

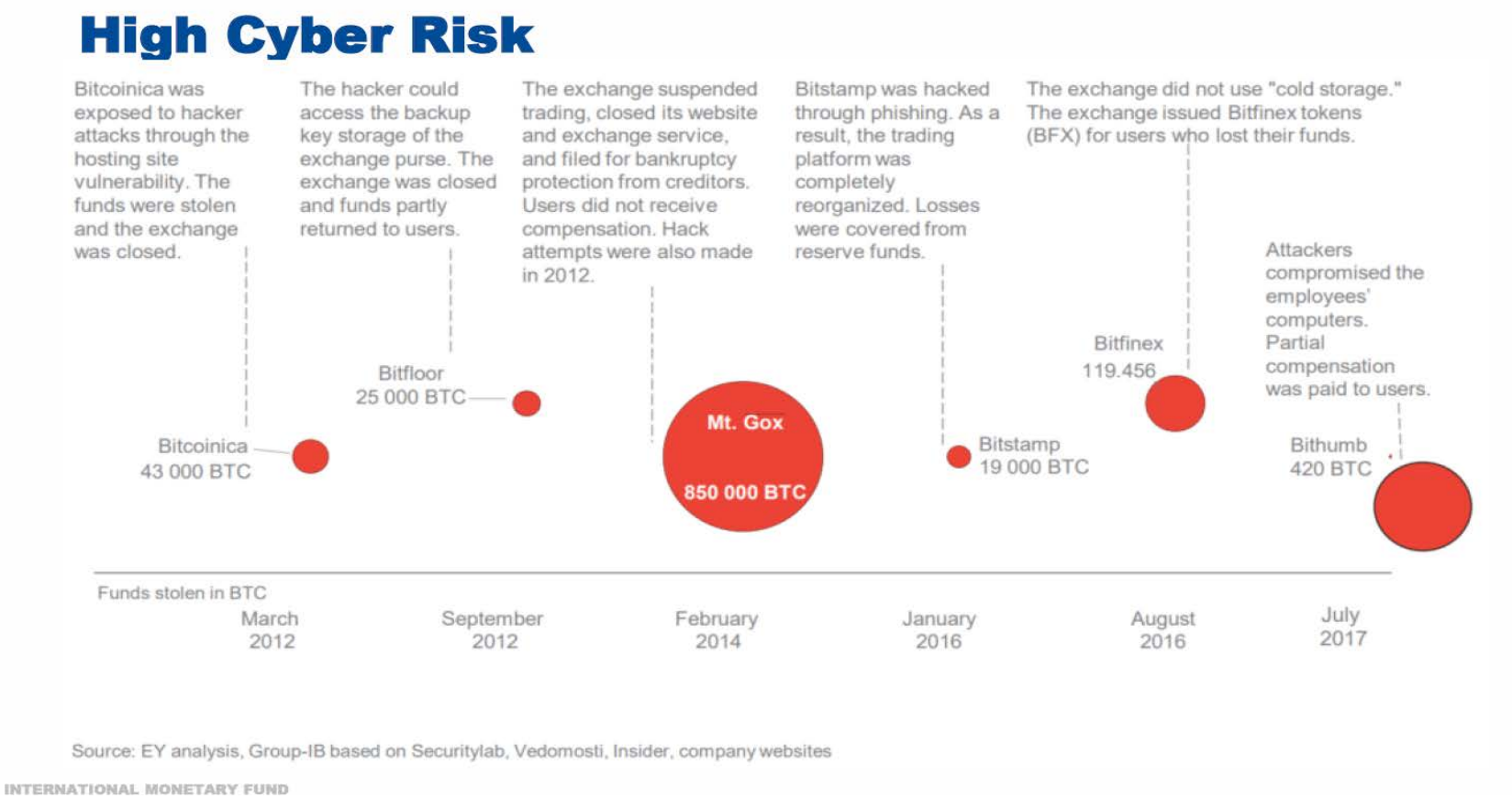
금 시총 10 TUSD

비트코인 지갑 갯수 7천 만



BTC, 단 한 번의 해킹사고 없었음!

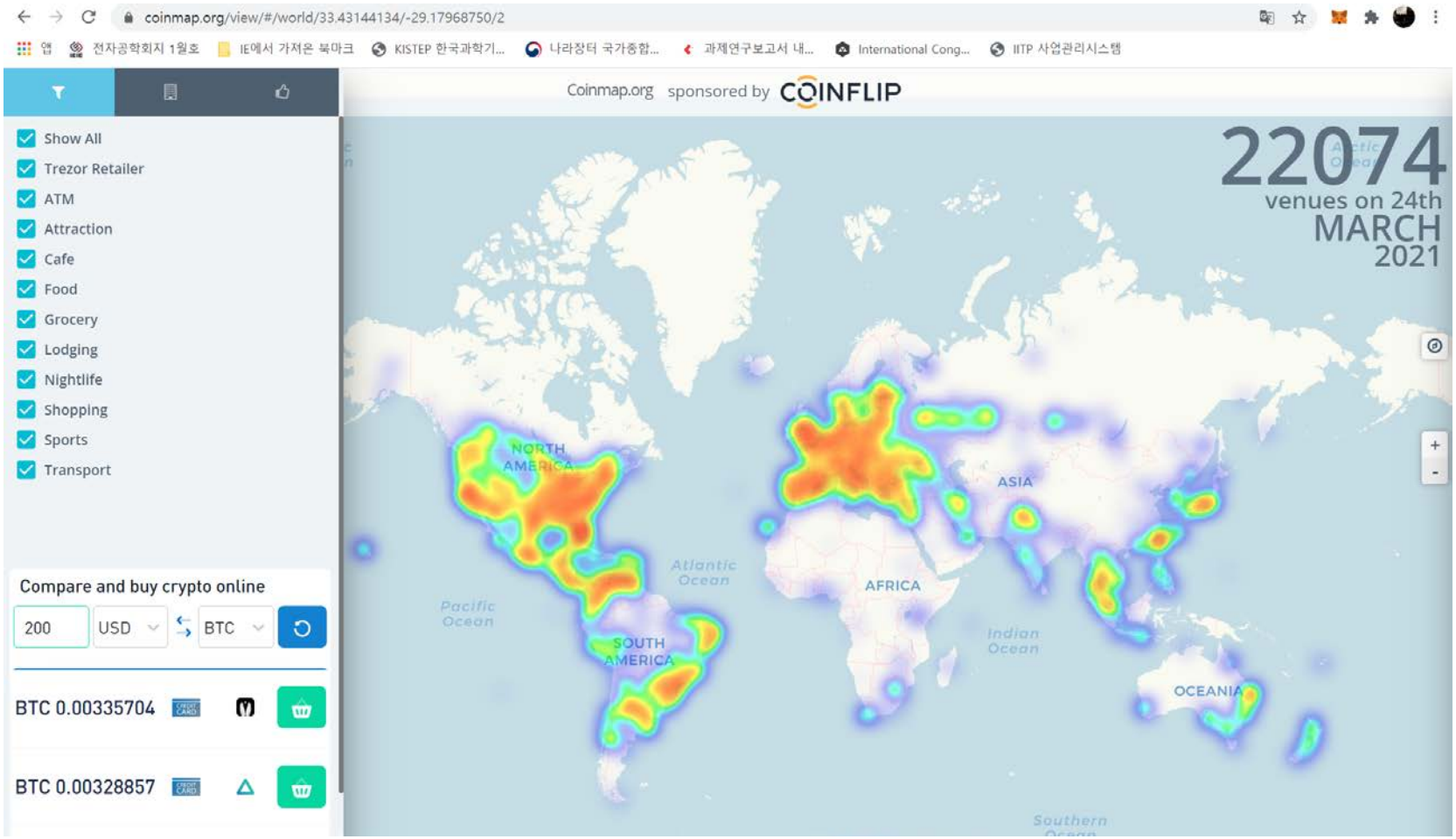
모두 거래소에서 일어난 사고
→ 금융기관급 ISMS(Info Sec Mgmt Sys)인증요구
(특금법, AML + KYC+ Travel Rule)



Bitcoin

- Since birth in 2009, bitcoin has never been stopped breathing and is alive currency system.
- It is a global digital currency which works beyond national boundaries.
- It was born when trust on the banks and governments was severely degraded.
- It mints bitcoins every 10 min.

비트코인 2만 소매점 분포도



페이팔 암호화폐 결제 시사점

- 페이팔 오늘부터 암호화폐 결제 시작 (서울=뉴스1) 박형기 기자 | 2021-03-31 06:40 송고 | 2021-03-31
  - 비트코인은 전일에도 비자카드가 결제에 암호화폐 사용을 허락할 것이라고 밝히자 4% 이상 급등했었다. 전일 비자카드는 미국 달러에 연동된 스테이블코인(가격변동이 없는 암호화폐)인 USDC를 이용해 암호화폐 결제를 허용할 것이라고 발표했다.

- "디지털 화폐가 주류로 진입해 일상적인 결제 수단이 될 것이다. 코로나 팬데믹이 이런 추세를 앞당겼다." 세계 최대 간편 결제 기업 페이팔의 댄 슐먼 최고경영자
- 페이팔 이용자들은 비트코인과 이더리움, 비트코인캐시, 라이트코인 등 4개 가상화폐로 전 세계 2600만 가맹점 물건을 구입할 수 있다. 페이팔 이용자가 물건을 구입하고 가상 화폐로 결제하면, 페이팔이 실시간 환율을 적용해 가상 화폐를 달러로 바꾼 다음 판매자에게 전달하는 방식이다.

화폐 주조권을
채굴 참여자에게 주고,

채굴보상을 매 210,000블
록마다 반으로 감소시켜

BTC 발행 총량을
2100만 개로 한정함.

가장 최근에 발생한
세 번째 채굴보상 반감 시점은
2020년 5월 12일

채굴 보상 반감 시점

- Block mining reward gets halved every 210,000 blocks mined.
- 블록당 채굴보상은 50 BTC 로 시작(2009)함.

1. 첫 번째 반감(25BTC)은 2013년에,
2. 두 번째 반감(12.5BTC)은 2017년에,
3. 세 번째 반감(6.25 BTC)은 2020년 5월 12일

   반감기가 있었던 Block은 (210,000 x 3 =) 630,000 번째 블록 임.

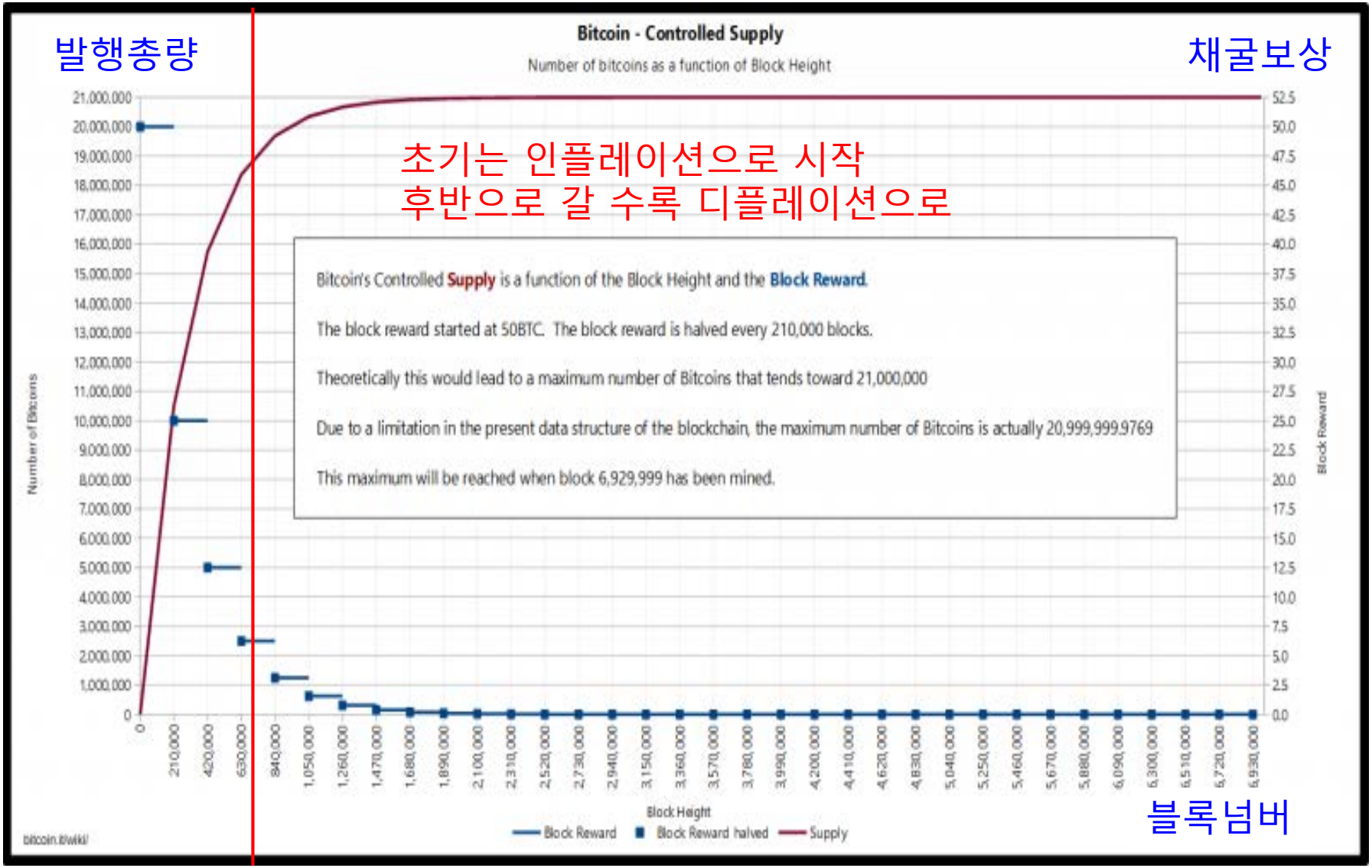
Block# 629999

Hash	00000000000000000000d656be18bb095db1b23bd797266b0ac3ba720b1962b1e
Confirmations	176
Timestamp	2020-05-12 04:23
Height	629999
Miner	F2Pool
Number of Transactions	2,481
Difficulty	16,104,807,485,529.38
Merkle root	f475113d55cb0042d8ab49f5475cbea4a1ff5e22e11750ed2096a2000c573a0f
Version	0×27ffe000
Bits	387,021,369
Weight	3,998,681 WU
Size	1,429,136 bytes
Nonce	2,214,301,135
Transaction Volume	11357.69593246 BTC
Block Reward	12.50000000 BTC
Fee Reward	1.06876397 BTC

Block# 630000

Hash	000000000000000000024bead8df69990852c202db0e0097c1a12ea637d7e96d
Confirmations	175
Timestamp	2020-05-12 04:23
Height	630000
Miner	AntPool
Number of Transactions	3,134
Difficulty	16,104,807,485,529.38
Merkle root	b191f5f973b9040e81c4f75f99c7e43c92010ba8654718e3dd1a4800851d300d
Version	0×20000000
Bits	387,021,369
Weight	3,993,250 WU
Size	1,186,930 bytes
Nonce	2,302,182,970
Transaction Volume	3311.62144322 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.90968084 BTC

비트코인 발행 스케쥴



2021년 현재

비트코인 네트워크에 참여하려면?

Blockchain Core is a Program Suite.

The three parts: networking, wallet, blockchain protocol

1. Networking of P2P nodes over the web interface

- Node registration, get-address, give-address
- Full node or light node
- Communication among the wallets and the miners

2. Wallet app for TX generations

- Make private and public keys, address, store UTXOs, make TX, put signature, announce it to the neighbor, check to see if the TX is supported by the blockchain.

3. Blockchain Protocol

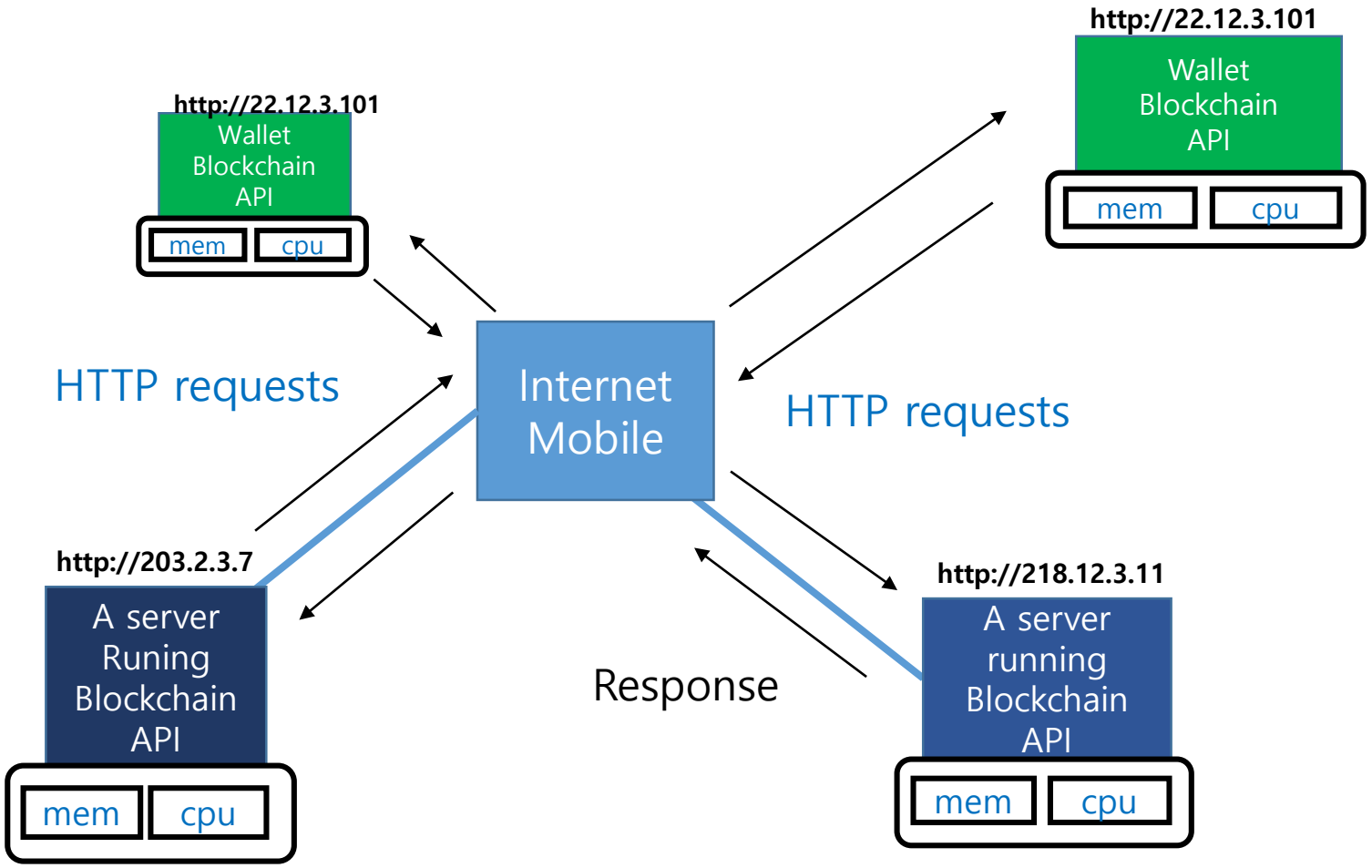
- Data: Genesis block + regular blocks, one block every 10 min, block-size 1Mbyte
- Protocol: consensus, block header, difficulty level adjustment, …
- Mining: Get the longest chain, validate it and all transactions within it, get transactions from mempool and form a block, run SHA repeatedly until you hit a good hash, put the proof into the block header, and attach the proofed block to the longest chain, and make announcement ASAP.

Program Suite

- **C++, Python, Go, Java, Flask, http**
- **Download and run, then you have a blockchain server.**

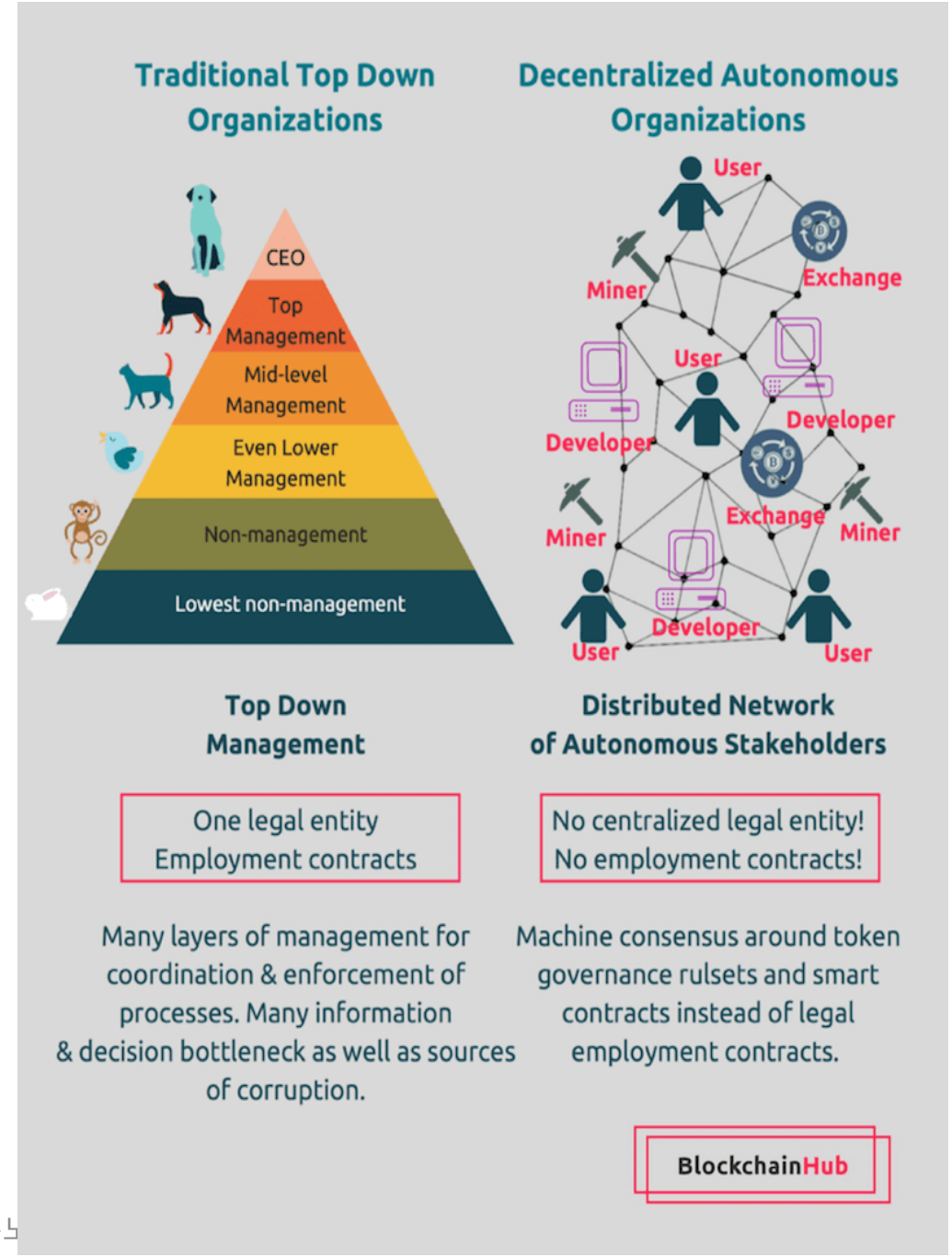
Anybody who downloads and runs the blockchain suite can become the member of

the blockchain internet



Bitcoin Economy

- 설계자
  - 연간 코인 발행량, 거래 및 처리 속도, 인센티브, 블록체인에 담을 내용
- 개발자
  - 버그 및 문제점 개선
  - 시스템 유지 및 보수
- 사용자
  - 송금, 소매, 도매, 은행
- 채굴풀
- 거래소
- 투자자



코인마켓캡 거래소 현황

바이낸스
하루 거래량
29조 원

업비트
하루 거래량
13조 원

#	이름	거래 점수	거래량 (24시간)	평균 유동성	방문 - 유사웹	# 마켓	# 코인	지원 화폐
1	Binance	9.8	₩29,430,135,528,073 ▲ 1.29%	690	14,296,860	1151	346	AED, ARS, AUD and +43 more
2	Coinbase Pro	8.9	₩3,140,395,759,527 ▼ 11.73%	523	2,331,017	156	53	USD, EUR, GBP
3	Kraken	8.5	₩1,336,699,460,606 ▼ 17.08%	563	2,266,008	284	62	USD, EUR, GBP and +4 more
4	Huobi Global	8.4	₩8,195,681,213,065 ▼ 3.52%	648	831,763	937	315	ALL, AUD, BRL and +47 more
5	Bitfinex	8.3	₩1,078,330,073,222 ▼ 18.24%	507	458,234	299	130	USD, EUR, GBP and +1 more
6	KuCoin	8.2	₩927,662,297,479 ▲ 1.56%	504	578,775	672	294	TOKEN
7	Bithumb	8.1	₩2,043,131,201,679 ▲ 24.93%	263	872,727	190	160	KRW
8	Bitstamp	7.9	₩571,630,898,595 ▼ 25.17%	312	406,105	53	18	USD, EUR, GBP
9	Coinone	7.8	₩843,761,401,023 ▲ 16.13%	226	309,143	168	167	KRW
10	Binance.US	7.8	₩430,460,806,201 ▼ 12.82%	325	919,356	109	54	USD
34	Upbit	5.6	₩13,444,924,464,067 ▲ 29.84%	249	1,269,118	254	172	KRW

Bitcoin이전의 E-cash

PoW is money류의 시도들

- B-Money (98') by Wei Dai
  - Uses PoW money and a decentralized servers
  - But assumed almost perfect channel

- Hashcash(02') by Adam Back
  - Proof-of-Work used to limit email spams (97')
  - PoW with a num of high zero bits is token (02')

- Karma file sharing (03') by Vishnumurthy
  - Coin creation is adjusted for inflation and deflation
- BitGold(05') by Nick Szabo
  - PoW is gold.
  - Uses IP addresses (Sybil attack)

ICO and Ethereum

Initial Coin Offering

- ICO는 블록체인기업이 신규 암호화폐를 발행해 자금을 모으는 것을 의미.
- 기업이 자금을 유치하기 위해 기업공개(IPO)를 하는 것과 비슷.

ICO 전형적 유형

- 프로젝트 설명을 위해 블록체인기업은 백서를 쓴다.
- 블록체인과 암호화폐를 활용하여 어떤 새로운 제품과 서비스를 만들 것인지 밝힌다.
- 블록체인의 무결성과 시스템의 안정적 운용을 담보하기 위해서는 개발자와 관리자, 사용자 네트워크를 폭넓게 확보해야 한다.
- 시스템을 빠르게 구축하기 위하여 토큰을 발행한다.
- 발행한 토큰이 거래소에 상장되고,
- 개발된 서비스가 폭넓게 사용 될 때,
- 발행한 토큰에 대한 교환가치가 상승한다.
- 이때 관리자, 사용자, 투자자들은 노력과 투자에 대한 보상을 받는다.

미국의 ICO 규제

- Jay Clayton 증권거래위원회 의장(17'-20')이 쓴 공개서한 (2018).
- 상기한 유형의 ICO **토큰은 증권**이라고 선언.
  - 투자금 모집을 위해 발행하는 토큰이 바로 증권이라는 것이다.
  - 토큰이 증권이 되면 기업의 입장에서는 매우 난감해집니다.
  - 오랜 전통을 가진 증권법을 따라야 하기 때문입니다.
- **Howey Test**(1946, SEC vs. Howey, 대법원 판결)
- 토큰 = 증권 여부를 판가름 기준 제공
  - an investment of money (투자)
  - in a common enterprise (공동기업에)
  - with the expectation of profit (수익을 기대하며)
  - to be derived from the efforts of others (타인의 노력으로)

SEC 헤스터 퍼스 “암호화폐, 증권법 3년 유예하자"

- http://www.coindeskkorea.com/news/articleView.html?idxno=70199
- 미국 증권거래위원회(SEC)의 ‘크립토 대모(CryptoMom)’ 헤스터 퍼스 위원이 암호화폐 프로젝트가 증권법을 어기지 않고 성공할 기회를 주자고 제안했다. 증권거래위원회 위원 2년째를 맞은 퍼스 위원은 토큰 프로젝트가 증권법을 비롯한 규제를 위반해 기소될 걱정 없이 네트워크와 커뮤니티를 개발할 수 있도록 피난처를 제공하자고 공식 제안했다.
- 퍼스 위원의 제안을 보면, 암호화폐 스타트업은 최초 토큰 판매 시점으로부터 3년간 유예기간을 받는다. 유예기간 중에는 규제를 신경 쓰지 않고 호위(Howey) 테스트 등 증권거래위원회의 규제 심사를 통과할 수 있을 만큼 탈중앙화를 이룰 수 있다.
- 지금까지 증권거래위원회는 메신저 플랫폼 텔레그램(Telegram)과 킥(Kik)을 포함해 토큰을 만들어 판매한 여러 회사를 증권법 위반 혐의로 고소하는 등 사법 조처를 했다.
- 이더가 증권으로 시작했을지 모르지만, 네트워크가 수년에 걸쳐 진화했다는 점을 지적했다.
- EOS에서도 비슷한 변화가 있었다. 증권거래위원회는 작년에 EOS와 합의에 이르렀다. 원래 ERC-20 규정을 따라 발행한 EOS 토큰은 증권이지만, 프로젝트의 최종 EOS 토큰은 증권이 아니라고 결론지은 것이다. (네트워크가 완전히 개발된 후에 토큰을 보유한 이들은 기존 토큰을 EOS 블록체인의 고유 토큰으로 바꿨다)

크립토맘
헤스터 퍼스 SEC 위원

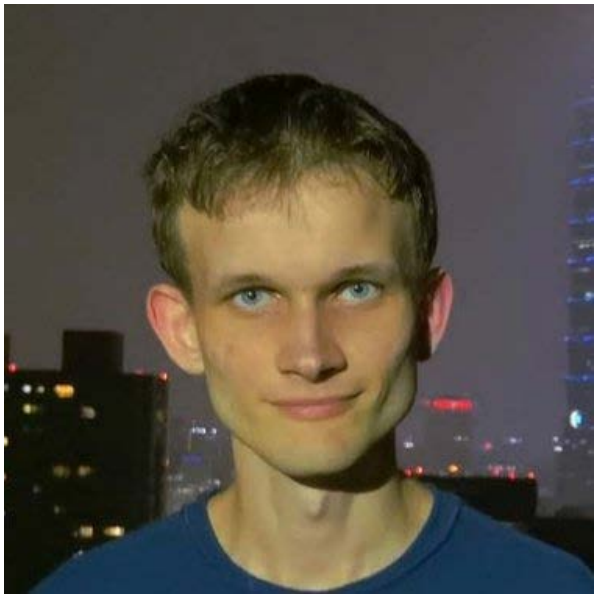
첫번째 ICO, 어떻게 시작했나?

- "We claim that the existing bitcoin network can be used as a protocol layer, on top of which **new currency layers with new rules can be built** ...
- ... **initial funds to hire developers to build software** which implements the new protocol layers, and ... **will richly reward early adopters** of the new protocol."
- **Mastercoin** raised close to **5,000 bitcoins** or **$500,000 2013**.
- https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/#36db35661183

J.R. Willett, the founder of the ICO
COURTESY OF J.R. WILLETT

Ethereum ICO

- Ethereum ICO in 2014, raising coins worth millions of dollars.
- Vitalic Buterin (Russian, Jan. 1994), co-founder of Ethereum, co-founder of Bitcoin Magazine 2011.

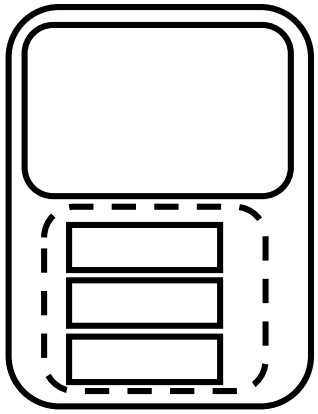


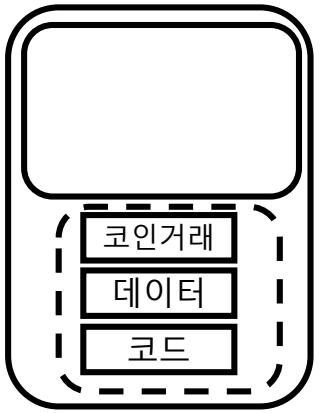
Ethereum

- 블록체인 Layer를 코인거래 부분과 분리시켜 관리함.
- 블록에 Smart Contract코드도 포함함.
- 비트코인은 OP코드에 Loop발생을 허용하지 않음.
- 이더리움은 완전한코딩이 가능하도록 OP코드에 Loop를 허용함.
- 토큰을 쉽게 만들 수 있어서 ICO폭발 추동

Bitcoin 블록은
안전한 코인 거래 중심

Ethereum은 Smart Contract
코딩의 편의성 강조





Ethereum 블록에 들어간 판문점 선언문

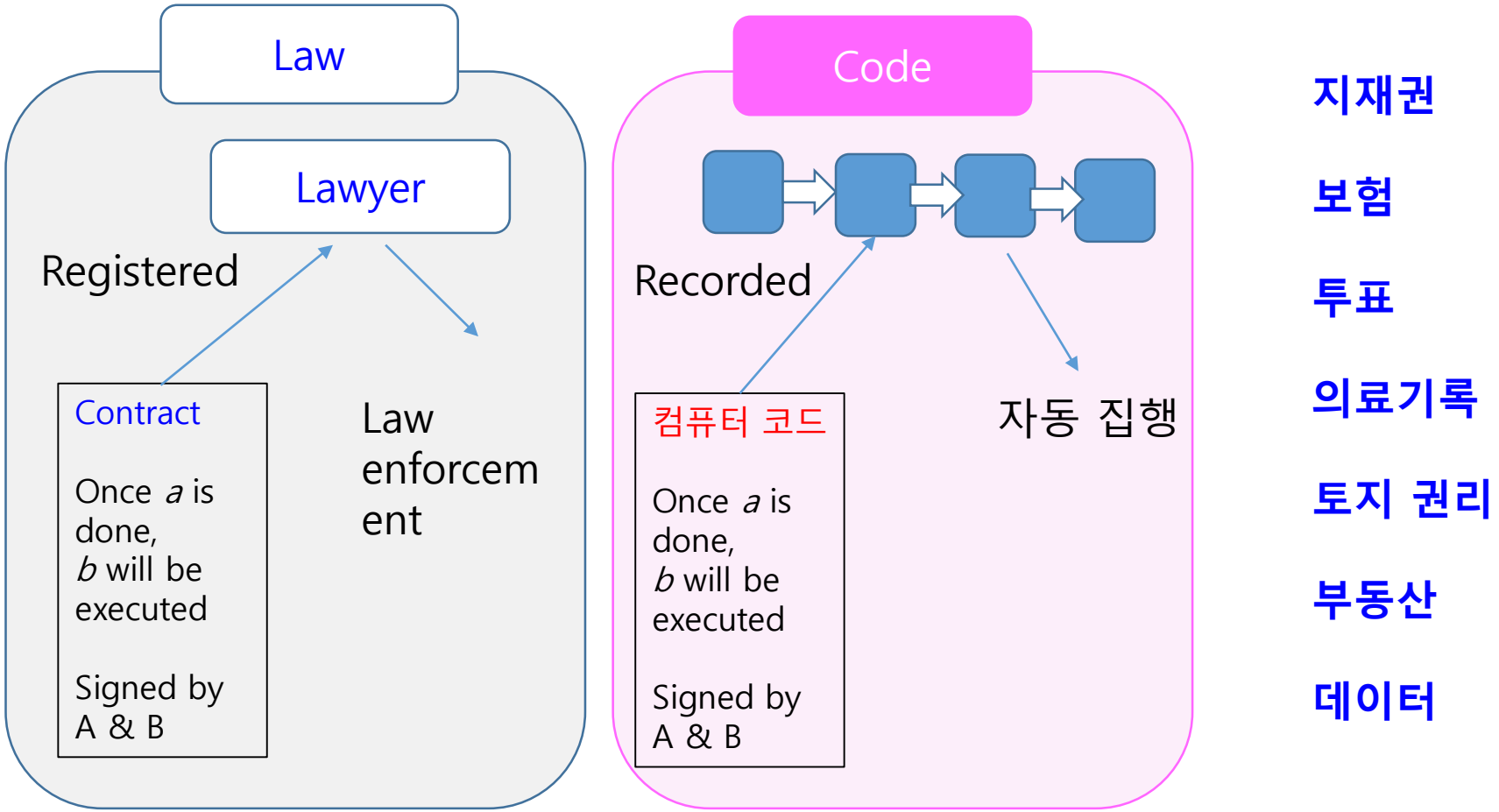
Overview | Comments

Transaction Information — Tools & Utilities

TxHash:	0xe4ee15d3f63db8464a649e3237ed83e930f9b3e40e842537a62
TxReceipt Status:	Success
Block Height:	5517596 (1257 block confirmations)
TimeStamp:	5 hrs 13 mins 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 ($3.47)
Nonce:	0
Input Data:	0x2018년 4월 27일 한반도 판문점 선언 1. 남과 북은 남북 관계의 전면적이며 획기적인 개선과 발전을 이룩함으로써 끊어진 민족의 혈맥을 잇고 공동번영과 자주통일의 미래를 앞당겨 나갈 것이다. Switch Back
Private Note:	<To access the private Note feature, you must be logged in>

2018.04.28

Legal Contracts vs. Smart Contracts



지재권

보험

투표

의료기록

토지 권리

부동산

데이터

NFT 복제 불가 디지털진품 제작 기술

- **게임 체인저, 224억원에 경매**
  - 코로나19 시대 진정한 영웅은?
- **[NFT 시대가 온다] 잭 도시 ' 첫 트윗' 32억원 경매, 이더로 결제** (3/23/2021)
- 비트코인처럼 지갑과 Cryptography를 활용하여, 동영상, 이미지, 음악파일 등 디지털 콘텐츠의 소유권을 만들어 블록체인에 등록하고, 소유권 거래를 추적 관리함
- 복제 불가능 원작 제작 가능.

영국 화가 뱅크시 그림 <게임 체인저>

디파이(DeFi)

- 탈중앙화 금융
- Bitcoin과 같은 가상자산을 본원 통화를 담보로 스테이블 코인을 발행함.
- **디파이**란 탈중앙화(Decentralize)와 금융(Finance)의 합성어 **'탈중앙화 금융'**을 일컫는다.
- 디파이는 예금은 물론이고 분산 거래소, 결제, 보험, 투자 등 다양한 금융 서비스 제공 가능.

DeFi, NFT 시사점

- 분산 금융, NFT 흥미로움
- 초 단기 대출 상품 개발 등 실물경제와 너무 동떨어지는 것은 경계해야 할 듯
- 포용 금융에 활용 가능할 듯함

블록체인 거버넌스 문제

블록체인 생태계에 권력구조가 생겨남

- 채굴 시장의 중앙화
  - A few mining sites emerge and dominate the market. This small core group makes important decisions. They are the ones who get the most benefit from these decisions.
- SW에 쓰여진 프로토콜은 계속해서 업데이트가 되어야 의미가 있다.
- 업데잇 방향과 결정은 누가하는가? 소유의 코어 개발자가 결정하고 공개
- Stakeholders might not accept them.

The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure [Filippi16]

- Bitcoin community was divided with increasing block size. (BitcoinCash 하드포크, 2017)
- Invisible politics shows technocratic power structure
  - Governance by the infra (Bitcoin protocol) : Self-governing and self-sustaining strong market-driven approach to social trust
  - Governance of the infra (developers and stakeholders) : the development and maintenance are done by a small core group

Awareness of Technological Limit

- *Technology alone is not enough to resolve socio-political problems arising in blockchain network.* **[Filippi16]**
- Some form of *social institution are needed.*

- Research on chain policies:
  - PoW, PoS, DPoS, PoA, …

- Research on off-chain policies: Off-chain governance, how to make decisions and reach consensus among people in a blockchain community.
  - 자본주의, 참여주의, 민주주의, 대의민주주의, 철권통치

흔히 지적되는 Bitcoin의 기술적 문제

- Astronomical cost for mining
- *Decentralization?*
  - *Mining pools are re-centralized.*
- **Not very convenient and useful as a currency (store of value but not medium of exchange)**
  - Slow transactions speed
  - Price fluctuation
- **Possibilities of cyberattacks and hacking:**
  - Availability of renting services of mining equipment.
  - Astronomical amount of assets were lost due to 51% attacks, such as Monacoin, Bitcoin Gold, Zencash, Verge, Litecoin cash...
- Quantum computers, emergence of new bitcoin, ...

Proliferated ICO projects

- Be careful!
  - 98% of ICOs done in 2017/2018 did not fulfill their obligations!
  - Not many research articles either!
  - White papers are not peer reviewed!

- 거래 속도 다양화
  - 10min per block, 1min/block, 40초/block, …

- 새로운 블록생성 방식 시도
  - Proof-of-work, Proof-of-Stake, Proof-of-activity, …

Proof-of-XXX, Alternatives to PoW

	Pros	Cons	Coins within top 50 rank
PoW (Proof-of-Work)	▪ Strongest security ▪ Difficult to produce ▪ Easy to verify	▪ Extreme computing power ▪ 51% attacks ▪ Transaction speed / Transaction throughput	Bitcoin, Ethereum
PoS (Proof-of-Stake)	▪ Energy & hardware efficiency ▪ Expensive 51% attacks	▪ Recentralization ▪ The rich-get-richer ▪ "Nothing at stake" problem	ETH2.0, Cardano, Tezos
DPoS (Delegated PoS)	▪ Scalability and speed ▪ Energy & hardware efficiency ▪ Encouraging good behavior by real-time voting	▪ Recentralization ▪ DDoS attacks	EOS, TRON, NEO
BFT	▪ Resistant to n/3 attacks ▪ Validators are randomly selected.	▪ $O(n^2)$ complexity	XRP, NEO, BinanceCoin, Cosmos

블록체인 트릴레마 (V. Buterin)

구분	내용	사례
확장성 (Scalability)	사용자 수 증대에 유연하게 대응할 수 있는 능력 단위 시간당 거래건수가 늘어 날 때 무리 없이 거래를 증대시킬 수 있는 능력을 의미	이더리움 Plasma, Sharding
탈중앙성 (Decentralization)	중앙 집중화 구조를 벗어나 노드들이 소규모 네트워크로 자율적으로 모여 운영주체가 되는 것을 말함 기존의 서버-클라이언트 관계를 벗어나 개별 노드들이 자발적이고 자율적으로 피투피(P2P) 방식으로 연결함 블록체인 기술이 사회적으로 널리 확산됨에 따라 기존의 중앙집중식 조직, 기업, 단체, 기구 등은 탈 중앙 구조로 변경되고 있음	초기 Bitcoin Network
보안성 (security)	블록체인 데이터의 무결성 확보하거나, 오픈 프로토콜이 원래 의도한 바 데로 시스템이 작동하도록 하고, 외부로 부터의 공격으로 부터 시스템을 보호하는 능력 을 의미	

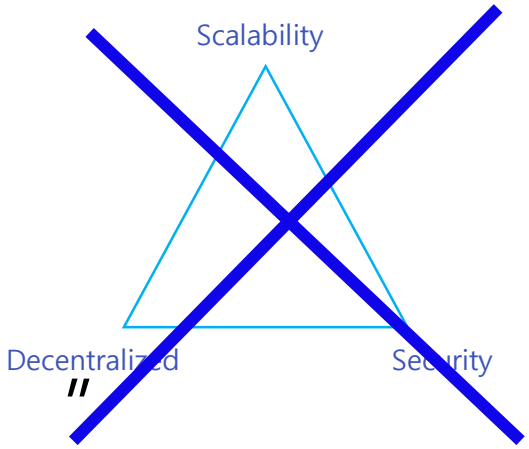
Blockchain Trilemma?

"

blockchain systems can only at most have two of the following three properties

- Vitalik Buterin, Sharding FAQ
https://github.com/ethereum/wiki/wiki/Sharding-FAQ

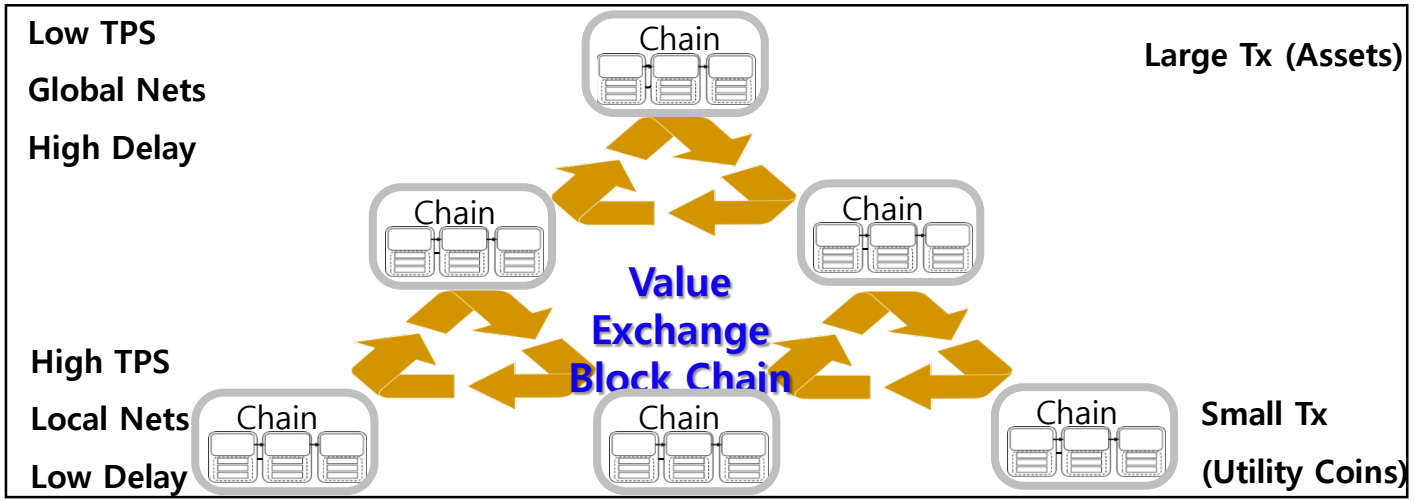
"



- Wrong approach!
- Not in a single blockchain, can it be achieved!
- *We shall promote many decentralized secure (DeSecure) blockchains and approach the scalability problem!*

Provision of DeSecure chains, use ecosystem to solve scalability issue!

- ▣ Global chains → national chains → local chains
- ▣ One chain is designed to hold only up to 20 DApps



<Multi-level DeSecure chains>

2018년 당시 했던 생각들

- 국경을 뛰어넘어 자산급 거래를 10분에 하면 빠른 것 아닌가?
- 비트코인으로 밥 사먹고, 물 사먹을 것이 아니라면 왜 VISA결제와 비교하지?
- (Inclusive Finance) 제 3세계 시민들에게 핸드폰만 있으면 은행서비스와 금융혜택을 제공할 수 있다.
- BTC변동성은 리저브 크기가 성장하며 작아질 것.
- 거래 처리 속도를 원하면 2nd Layer 솔루션을 활용하면 됨
- 글로벌 기업이 국가의 역할을 하게 될 수도 있음

지난 2년 간 진행 상황 확인

- PoW is Money! (Wei Dao, Adam Back, N. Szabo)
- 새로운 합의알고리즘 시도는 대부분 탈 중앙성이나 보안성을 희생하여 확장성을 얻으려 목표함. 혹은 off-chain 정책에 의존함. **그런 메인넷의 결과는?**
  - Staking, Delegation, Activity-checking, Leader Selecting, Random Selection.
- **반면, BTC has grown to be the world reserve asset!**
- **페이팔, 2600만 가맹점에서 오늘부터 비트코인 거래·결제 서비스 개시 (2020/11/13)**
- **테슬라, 비트코인 차량 결제서비스 시작(2021봄)**

Facebook Libra

- 합의알고리즘: **Byzantine Fault Tolerance** O(n^2) + 지분증명
- 노드수 100개
- 1000 ~1500 TPS
- 중앙화 솔루션
- Stable Coin ~ Reserve
- Facebook network has 2B users.
- The era of digital currency may arrive sooner!

Marcus noted that blockchain technology is inevitable and if the U.S. does not lead in building and regulating it, the tech will come from places "out of reach of our national security apparatus," raising the spectre of China.

PoW is Gold! (N. Szabo)

CoinMarketCap

Accessed on 1/21/2020

	#	Name	Market Cap
PoW	1	Bitcoin	$157,523,327,976
PoW+PoS	2	Ethereum	$18,237,664,973
BFT	3	XRP	$10,173,030,507
PoW	4	Bitcoin Cash	$6,324,111,387
PoW	5	Bitcoin SV	$5,514,168,411
PoS	6	Tether	$4,642,239,400
PoW	7	Litecoin	$3,703,645,030
DPoS	8	EOS	$3,489,493,081
BFT+PoS	9	Binance Coin	$2,703,188,581
BFT	10	Stellar	$1,257,162,885
PoS	11	Cardano	$1,133,667,715
PoW	12	Monero	$1,132,339,953
DPoS	13	TRON	$1,110,529,913
PoS	14	Tezos	$1,049,197,574
PoW	15	Ethereum Classic	$1,033,632,329
PoW+PoS	16	Dash	$1,025,878,916
	17	Chainlink	$942,976,348
PoW	18	UNUS SED LEO	$888,524,224
BFTPoS	19	Cosmos	$867,402,795
dBFT	20	Neo	$793,931,677

WEF's Perspective on Cryptocurrency

- 1980 PC Windows
- 1995 Internet, Explorer
- 2005 Mobile, Android iOS
- 2009 ~ : Internet of Values!!!

- May 2015 WEF Reports,
  - "By 2027, 10% of World GDP will be stored in cryptocurrency"

- Cryptocurrencies Market Cap 2018 = 0.22 TUSD (0.25% of WGDP)
- Cryptocurrencies Market Cap 2021 ~ 2.0 TUSD (2.5% of WGDP)

비트코인 커뮤니티
추구하는 가치는
Creation of Sound Money

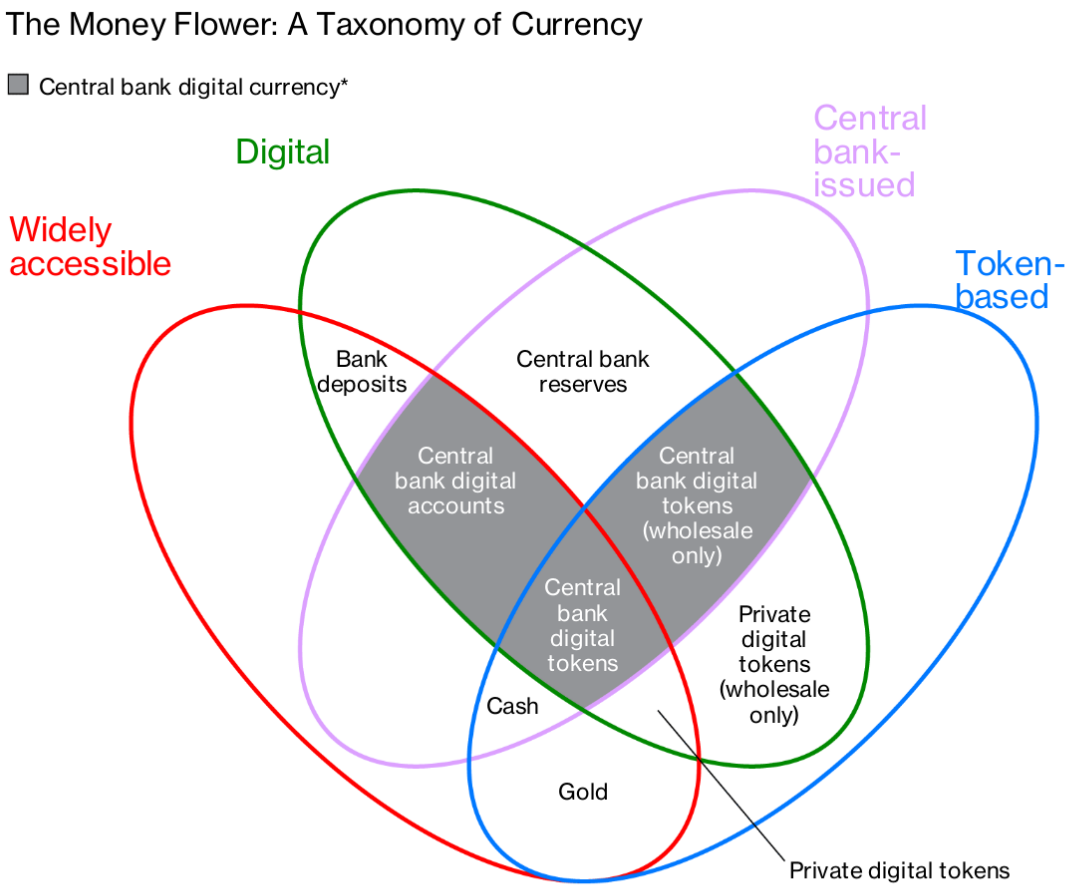
세계 경제의 미래와 Sound Money의 필요성

디지털경제 와 화폐의 미래

- 개인과 개인의 온라인 거래 증가
- 중국 중앙은행의 디지털 위안화 DCEP(Digital Currency Electronic Payment) 발행
  - 법정화폐로서, 알리페이, 위챗페이와는 비경쟁대상
  - 통화 흐름 통제, 돈세탁 방지, 부정부패척결, 위안화국제화

- 글로벌 기업 화폐
  - Facebook Diem(USD 스테이블코인)발행
  - 페이스북 스테이블 코인 '디엠', 테스트넷 트랜잭션 5000만 건 돌파 (2021/1/29)

글로벌 영역에서 화폐 경쟁 시대



*Excludes digital central bank money already available to monetary counterparties and some nonmonetary counterparties
Data: Bank for International Settlements

Money

- To make transactions more convenient, humans have invented "money."

- Medium of exchange
  - 욕구의 일치성 극복
- Measure of value
  - 물고기 한 마리: 5냥 미만이면 살거야.
- Standard of deferred payment
  - 물고기 한 마리 외상: 일년 후 두 마리 갚기로 vs.
    일년 후 10냥 갚기로 약속.
  - Inflation vs. deflation
- Store of value
  - 저축, 저장, 회수 및 사용 – 오랫동안 가치 보존

Time and energy are the most scarce resource.

- A man grows older and he has less energy.
- But he still need to survive.
- He seeks to have a means to keep him alive.
- One way is to have the land and animals.
- But it is very difficult.
- With sound money, it could be done.

Gold Standard

- Gold used as money for thousands of years.
- Gold is scarce.
- No counterfeit is possible.
- It does not get deteriorated.
- Its value is stable.
- It is compact.
- It can be made into gold coins.

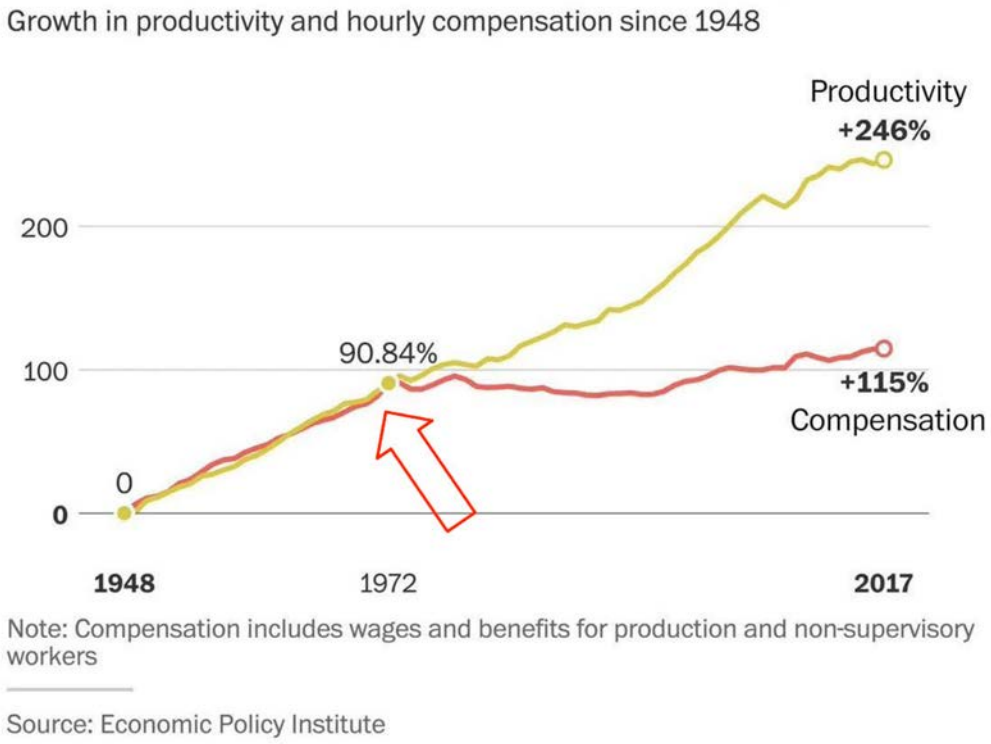
Kinds of Money

- Commodity: shells, sheep, cow, gold and silver coins are examples.
- Representative: tokens, coins, paper money can be used to exchange for gold and silver.
- Fiat currency is a money by (government) decree.
  - For example, “One ounce of gold is 35 USD” (The Gold Standard, Bretton Woods, 1944).
  - After Nixon Shock 1971, the USD is backed by nothing.

US dollars served as money up until the Nixon shock 1971.

- Nixon Shock (1971). Richard Nixon, the 37th President of US, ended the gold standard in 1971.
- With growing world economy (esp. German and Japan), the US share of economic output has shrunken and the trade deficit has grown.
- Wealth (USD) has flown outside the US and US had become no longer able to back the US dollars with the reserve gold.
- US Dollars since Nixon Shock are fiat currency which the central bank of the US (the Fed) can create more than the gold reserve of the US.

There are many reports that wealth inequality has worsened since the Nixon shock.



The Federal Reserve System

- The Federal Reserve System (FED) is the central banking system of the United States of America, created on December 23, 1913, with the enactment of the Federal Reserve Act. …
- Federal Open Market Committee sets the monetary policy.
- FOMC meets regularly, more than four times a year.
- FED Chairs
  - Jerome Powell
  - Janet Yellen
  - Ben Bernanke
- Federal Reserve Notes (FRNs) are the US Dollars.
- See Understanding How the Federal Reserve Creates Money.

FED's Role

- The U.S. Congress established three key objectives for monetary policy in the Federal Reserve Act:
  - 1. maximizing employment (최대 고용)
  - 2. stabilizing prices (물가 안정), and
  - 3. moderating interest rates (이자률 조정)
- The first two objectives are sometimes referred to as the Federal Reserve's dual mandate.[14]
- Its duties have expanded over the years, and currently also include
  - 4.supervising and regulating banks,
  - 5.maintaining the stability of the financial system

FED's during 2008 Financial Crisis

- Financial panic means
  - Money disappears!
    - You don't lend your money to others.
  - Chain defaults
    - You may not be able to withdraw your money.
  - Risk of economic collapse
- Lowers the short term interest rate
- Lowers the long term interest rate
  - In open market, FED purchases US bonds and mortgage backed securities.
- Where do they get the USDs?

Causes and Results

- Causes of Financial Crisis
  - Bank's **predatory lending**
  - Government's **guaranteed loans**
  - Moral hazard of bankers and home owners
- Results of Financial Crisis
  - **Money injected into society created bubble.**
  - Rich got richer; they've got bailout; they did not get punished.
  - Greater inequalities

네덜란드 중앙은행 W. Paper

1 vs. 99

Monetary Policy로 만든 돈 다 어디로 갔나?

Data analysis from 1920 to 2015.

Wage로 갔을까?

Monetary policy and the top one percent:
Evidence from a century of modern economic history

Mehdi El Herradi* Aurélien Leroy †

April 2019

Abstract

This paper examines the distributional implications of monetary policy from a long-run perspective with data spanning a century of modern economic history in 12 advanced economies between 1920 and 2015. We employ two complementary empirical methodologies for estimating the dynamic responses of the top 1% income share to a monetary policy shock: vector auto-regressions and local projections. We notably exploit the implications of the macroeconomic policy trilemma to identify exogenous variations in monetary conditions. The obtained results indicate that expansionary monetary policy strongly increases the share of national income held by the top one percent. Our findings also suggest that this effect is arguably driven by higher asset prices, and holds irrespective of the state of the economy.

JEL Codes: D63, E62, E64
Keywords: Monetary policy, Income inequality, Local projections, Panel VAR

Economy, Currency, Government

- People want an *ever improving state of self* and economic position compared to what they have enjoyed in previous years.

- **Government aims to provide** what people want.
  - Food and house
  - Energy and water
  - Safer environment
  - Less work but improved life style with leisure
  - Equal opportunity for limited resources
  - Improved education for children

Economy, Currency, Government

- Results:
  - Politicians need to get re-elected.
  - They make promises which can be fulfilled only by money creation.
  - Money is poured into the society.
  - Debt is growing.
  - Government guarantees growth.
  - More people live off of government guarantees.
  - Asset price is soaring.
  - Working people belongs no longer to the middle class.
  - More people find themselves in money trading.
  - Less people work in the areas of producing goods and services.
  - Entrepreneurship is reduced.
  - Inequality grows.
- What results in is the society in which honest work is no longer honored.

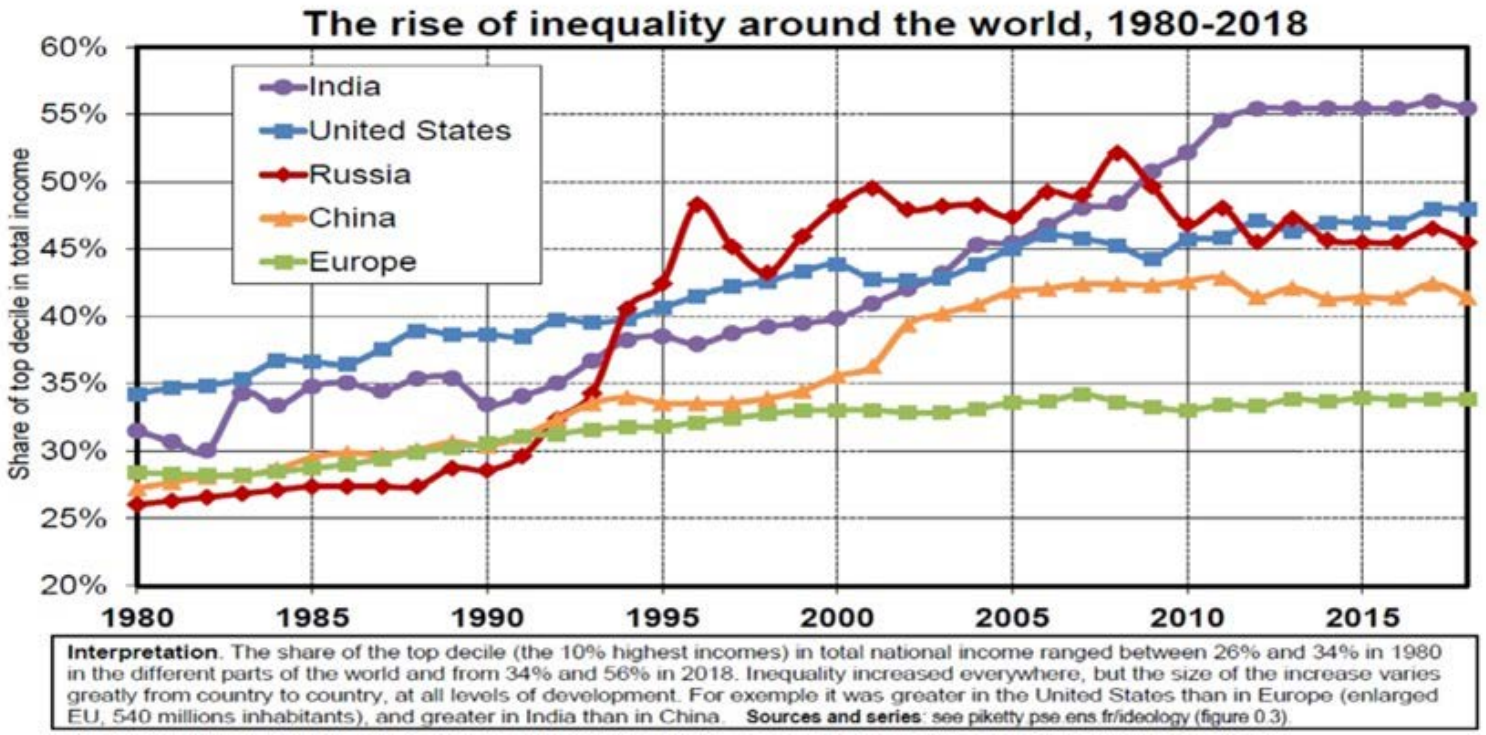
FED, Congress, Gov in Covid 19

- They bought corporate bonds as well.
- FED is aware of the consequence of QE.
- FED is more capable not to create asset bubbles.
- 중앙은행이 은행을 통해 돈은 공급하는 방법 대신에, 미국재무부가 main street에 직접 공급하는 방식으로 선회

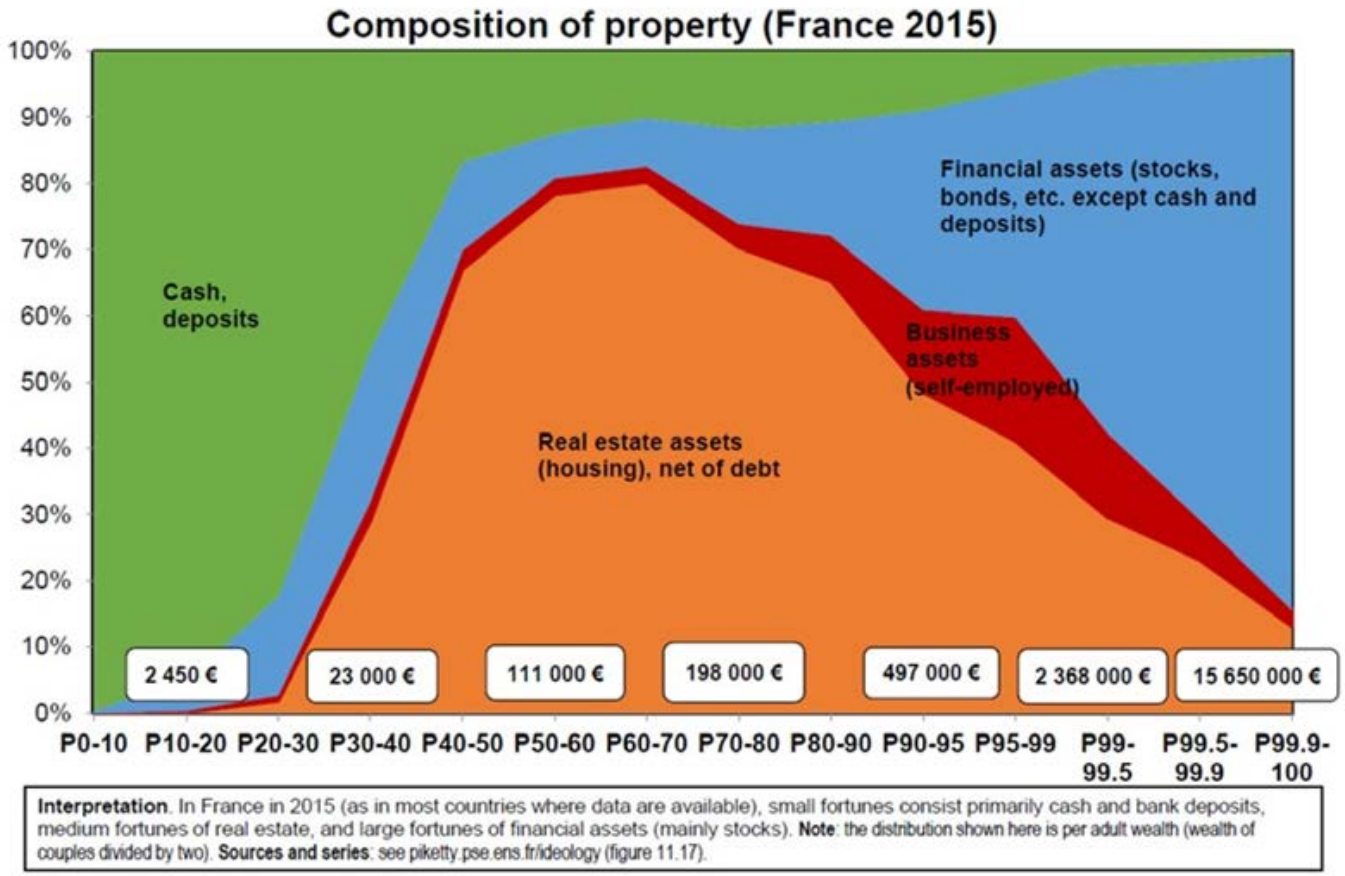
Impact of cheap money is growing inequalities.

- Capital and Ideology, Thomas Piketty, March 2020:
- Find Piketty2020SlidesLongVersion.pdf for the charts
- Piketty seems not concerned too much with cheap money.
- He's more concerned about increasing tax to rich (progressive, inheritance).

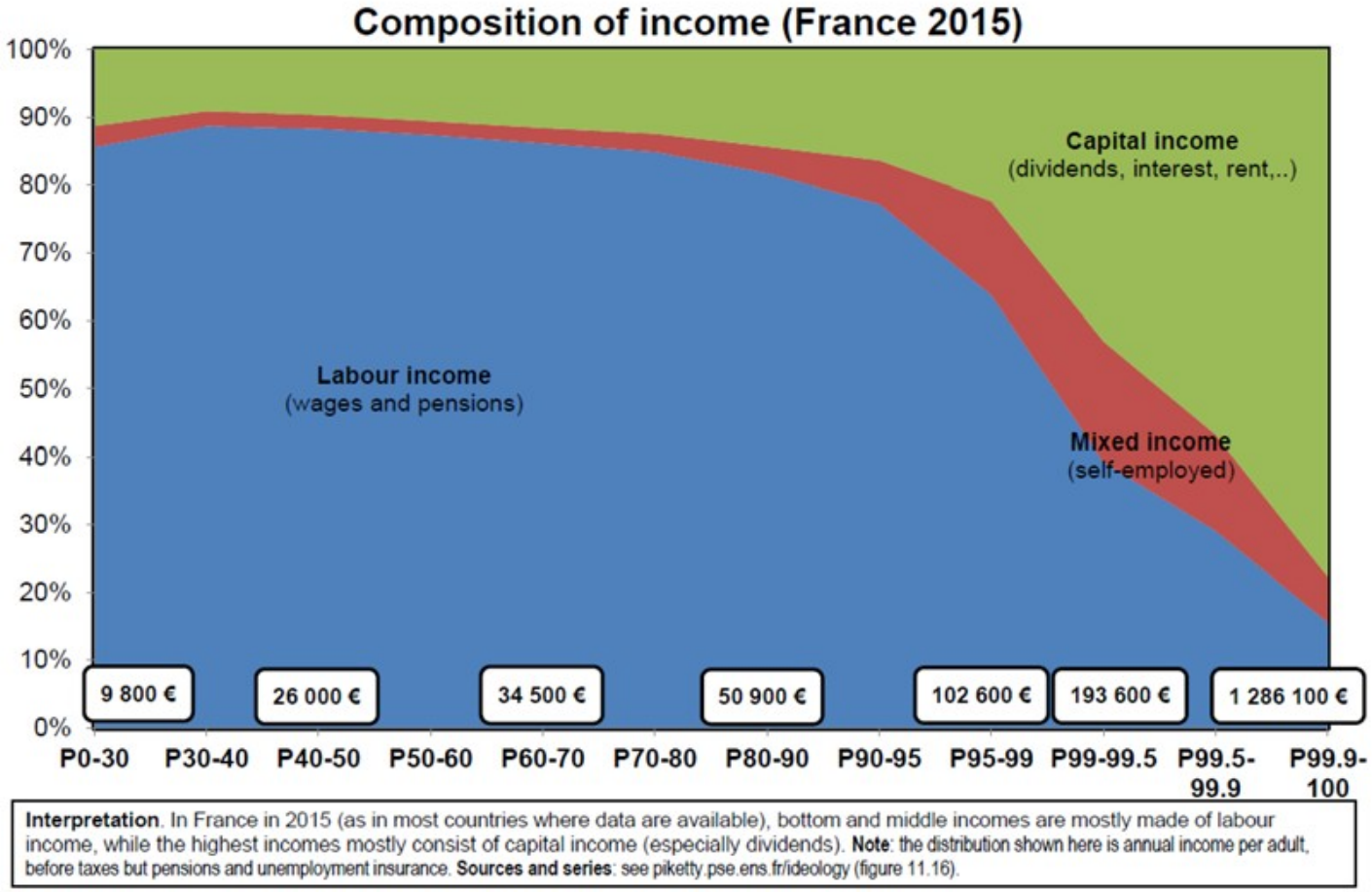
Share of top 10% in total national income has grown everywhere.



The property of the top 1% is mostly financial assets.



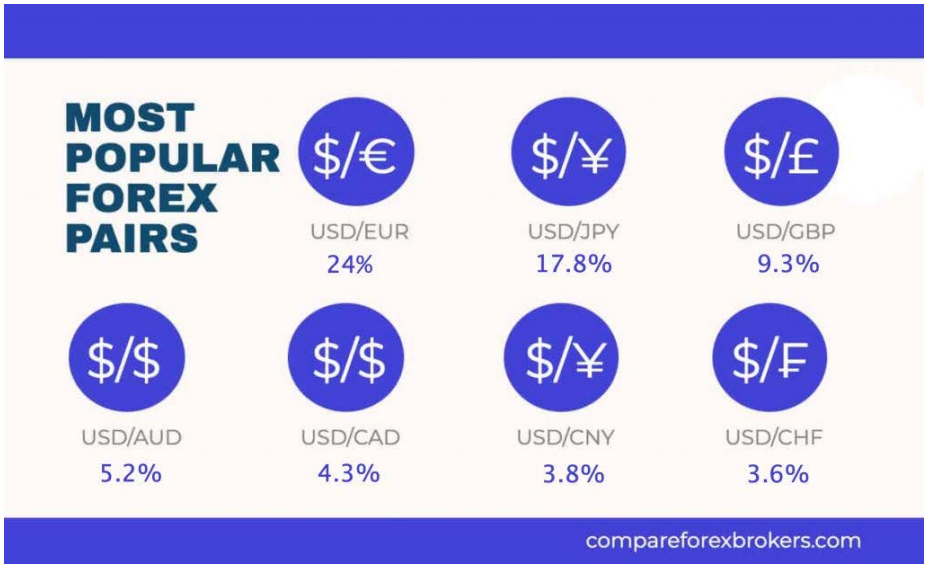
The income of the top 1% is capital income, while that of the lower 90% is labor.



Nasdaq has grown four times 2009 – 2017 (8 years), doubling every 4 year.

Forex.com

- WGDP 80 TUSD 보다 30배 더 큰 시장의 존재
  - The worldwide 2021 forex market is worth $2.409 quadrillion. $6.6 trillion on average every day is traded on foreign exchange markets.
  - 88%가 USD의 거래



Friedrich Hayek

(1899-1992, Novel laureate in Economics 1974)

De-Nationalization of Money (1976)

- Download: Denationalization of Money
  F. A. Hayek (Novel laureate in Economics, 1974) argues that money is a commodity that would be better off supplied through competition.
  - **Monopoly of government vs. competition by private issuers.**
  - **The advantages of competitive currencies are not only removing the power of government to inflate the money supply but also that they would go a long way to prevent the destabilizing fluctuations that government monopoly of money has precipitated over the last century.**
  - **In addition, it makes it difficult for government to inflate its own expenditures.**
  - **The central theme is crystal clear: government has failed, must fail, and will continue to fail to supply good money.**

De-Nationalization of Money (1976)

- Which money would public select?
- [pg66, Hayek's DeNationalization of Money]
  - Public selects a better money system.
  - The process of selection through competition is the key!
  - Four uses of money
    - Cash purchases of commodities and services
    - Holding reserves for future needs
    - Deferred payments
    - Unit of accounts
  - The prevailing currency is the one preferred by the people.

De-Nationalization of Money (1976)

- **The Practical Proposal (pg. 23)**
- The concrete proposal for the near future, and the occasion for the examination of a much more far-reaching scheme, is that
- *the countries of the Common Market, preferably with the neutral countries of Europe (and possibly later the countries of North America) mutually bind themselves by formal treaty not to place any obstacles in the way of the free dealing throughout their territories in one another's currencies (including gold coins) or of a similar free exercise of the banking business by any institution legally established in any of their territories.*
- This would mean in the first instance the abolition of any kind of exchange control or regulation of the movement of money between these countries, as well as the full freedom to use any of the currencies for contracts and accounting. Further, it would mean the opportunity for any bank located in these countries to open branches in any other on the same terms as established banks.

George Gilder

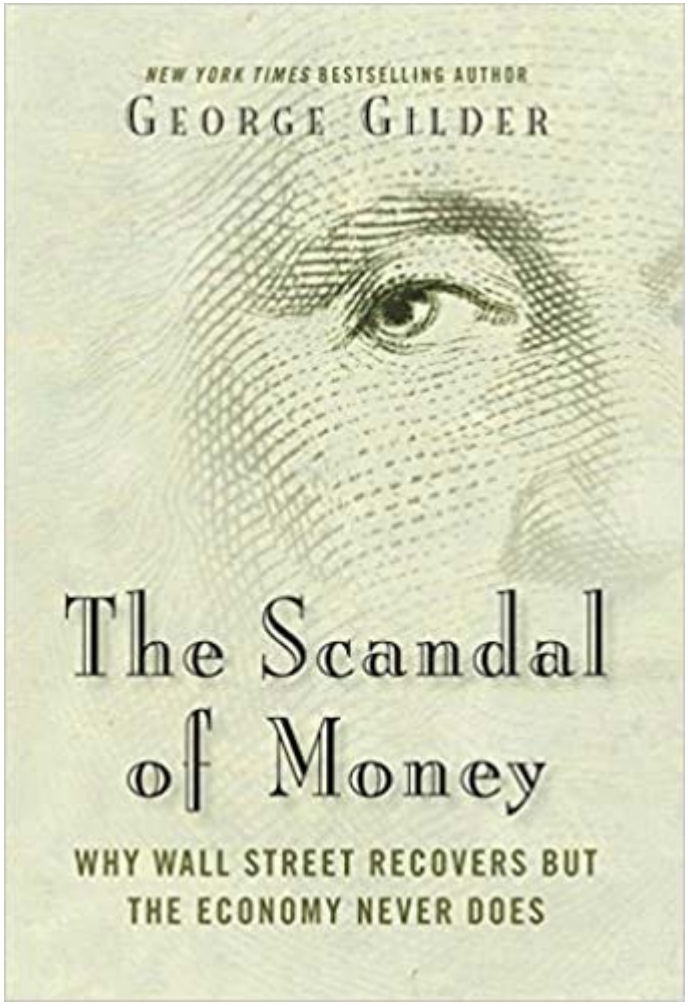
(Born 1939)

He was born in New Work City, U.S., Nov. 19, 1939. He is an investor, author, economist, techno-utopian advocate. He is the author of 1981 international best seller, Wealth and Poverty.

Scandal of Money (2016)

- *"Why do we think governments know how to create money? They don't. George Gilder shows that money is time, and time is real. He is our best guide to our most fundamental economic problem."*

  --Peter Thiel, founder of PayPal



Scandal of Money

Monopoly money: Money issued by sovereign states that block all competitive moneys in their domains, whether by regulation or by taxes not imposed on the sovereign currency. It's what we have in America and the rest of the world. Friedrich Hayek, the author of The Road to Serfdom, declared that "the source and root of all monetary evil [is] the government monopoly on the issue and control of money." Like most state-run monopolies, the money monopoly serves the interests of politicians rather than entrepreneurs, power rather than knowledge, old wealth rather than new ideas. Gold and bitcoin are the chief alternatives to monopoly money.

Scandal of Money

Hypertrophy of finance: The growth of finance beyond the rate of growth of the commerce it intermediates. For example, international currency trading is seventy-three times more voluminous than all global trading in goods and services and an estimated one hundred times as voluminous as all stock market transactions. Oil futures trading has risen by a factor of one hundred in some three decades, from 10 *percent* of oil output in 1984 to ten *times* oil output in 2015. Derivatives on real estate are now nine times global GDP. That's not capitalism, that's hypertrophy of finance.

Scandal of Money

Information theory: Based on the mathematical theories of Claude Shannon and Alan Turing, an evolving discipline that depicts human creations and communications as transmissions across a channel, whether that channel is a wire or the world. Measuring the outcome is its "news" or surprise, defined as entropy and consummated as knowledge.

Entropy is higher or lower depending on the freedom of choice of the sender. The larger the available alphabet of symbols-that is, the larger the set of possible messages-the greater the composer's choice and the higher the entropy and information of the message. Since these creations and communications can be business plans or experiments, information theory provides the foundation for an economics driven not by equilibrium or order but by falsifiable entrepreneurial surprises.

Information theory both enables and describes our digital world.

Scandal of Money

Wealth: Tested knowledge. Physical law dictates that matter is conserved: material resources have not changed since the Stone Age. All enduring economic advances come from the increase of knowledge through *learning*.

Scandal of Money

Economic growth: *Learning* tested by falsifiability or possible bankruptcy. This understanding of economic growth follows from

Karl Popper's insight that a scientific proposition must be framed

in terms that are falsifiable or refutable. Government guarantees

prevent learning and thus thwart economic growth. All expanding businesses and industries follow a *learning curve* that ordains a 20 to 30 percent decrease in costs with every doubling of total units sold.

Classical learning curves are MOORE'S LAW in SILICON VALLEY and METCALFE'S LAW in networking. Raymond Kurzweil generalized the concept as a "law of accelerating returns."

Scandal of Money

Wall Street: The symbol of the financial industry, from investment banks to insurance companies, from credit card vendors to payday lenders, from brokers to hedge funds. Today Wall Street is gorging itself on the HYPERTROPHY OF FINANCE. Ideally, finance *intermediates* transactions across time through interest rates and across space through currency-exchange rates. But today both these functions are falsified by government manipulation. They face disintermediation by gold, by a new transactions layer in the Internet software stack, and by new cryptographic blockchain currencies. In the hypertrophy of finance, Wall Street was bloated by MONOPOLY MONEY created by the Federal Reserve and channeled to the U.S. Treasury by banks, never touching MAIN STREET.

Scandal of Money

Main Street: The symbol of the real economy of workers paid hourly or monthly and sealed off from the circular loops of WALL STREET moneymaking. Perhaps the street where you live, Main Street is the site of local businesses and jobs.

Scandal of Money

Silicon Valley: A symbol of the high-tech entrepreneurial economy, centered in Santa Clara County, California, and largely funded by venture capital from SAND HILL ROAD in Palo Alto and Menlo Park. The high-tech economy is increasingly based on INFORMATION THEORY, which governs its infrastructure of communications and computing, particularly software. Silicon Valley sustains both MAIN STREET and WALL STREET by supplying them with new technology. Through Wall Street, Silicon Valley provides Main Street with opportunities for sharing in the equity of the ascendant sectors of the world economy.

In recent years, Silicon Valley has suffered from the HYPERTROPHY OF FINANCE, become bloated with MONOPOLY MONEY, and been bent by controls from the Wall Street-Washington axis.

Scandal of Money

Expansionary fiscal and monetary policy: The attempt by central banks to stimulate economic activity by selling government securities to pay for a governmental deficit. Keynesians believe that selling securities will impart a fiscal stimulus by enabling more government spending.

Monetarists, on the other hand, believe that to stimulate economic activity central banks should create money to *buy* government securities, money that supposedly is put into the economy. But this new money goes to the owners of the purchased securities, chiefly banks, which in recent years have used their money to purchase more securities from the Treasury. Thus Keynesianism and monetarism converge in expanding the government's power to spend.

In an information economy, both measures attempt to use government power to force growth. But ECONOMIC GROWTH is *learning* (accumulating tested knowledge). Learning cannot be forced.

Scandal of Money

Real money: A measuring stick, a metric of value, reflecting the scarcity and irreversible passage of time-entropy based, equally distributed, and founded on the physical limits of the speed of light and the span of life. BITCOIN and GOLD are both real money in this sense. MONOPOLY MONEY is not.

Scandal of Money

- Restoring Real Money (Chapter 14)

I am more convinced than ever that if we ever again are going to have sound money it will not come from government. It will be issued by private enterprise.

-Friedrich Hayek, 1977

Scandal of Money

- Restoring Real Money (Chapter 14)

Current state of the world diagnosed by the author:

- Government is getting bigger and bigger.
- To get re-elected, they made promises of stimulation which results in expansion of debts and currencies.
- Continuous “stimulation” produces cheap money.
- Cheap money gives wrong signals to economic entities.
- Speculative investment thrives with the booming of money exchange market.
- Lavish spending from borrowing make people lives miserable.
- Mortgage means you pay your debt through your life time. Mort is to mean dead. Gage is to mean pledge. If you don’t pay you debt, you will have to pay with your life.

Scandal of Money

- Restoring Real Money (Chapter 14)

His Proposal is Policy Change:

Existing policies based on demand-side economics by a few elites, government and central banks, suppress growth. Needed is a shift in policy. Supply-side economics can bring about an instant and sharp enhancement of all entrepreneurial assets. Real money, lower tax rates, and deregulation can open up and lengthen the time horizons of enterprise.

- To supply-side economics from demand-side economics
- To deregulate the economy from oppressive regulations
- To promote industrial innovation, manufacturing, skilled immigration, initial public offering
- To a small-entropy government from a high-entropy government
- To high-entropy private entrepreneurs with ample room for making real value creation and growth
- To expand the economy with ever cheaper and more useful goods and services with which everyone can thrive.

1. To achieve all these can be helped by the redemption of sound money (honest money)

Scandal of Money

- Restoring Real Money (Chapter 14)

- **Sound Money (Honest money)**

- Global money on the Internet
- Fixed exchange rate
- Payment methods over the Internet
- Distributed system rather than centralized.
- It is Bitcoin.

Scandal of Money

- Restoring Real Money (Chapter 14)

- **Previous attempts** (back to sound money; did not get realized).

- Greenspan (Previous FED chairman) "Shelton bonds": five year treasury notes payable in gold.

- Government has to be prudent and frugal. They now have to pay back to the borrowers with the real money.

Scandal of Money

Restoring Real Money (Chapter 14)

- **Nature of Sound Money and Consequence**

- Money is time. Money is essentially tokenized time. It allows this scarcity that applies to all economic activity ubiquitously across the economy. It allows you to translate that into transactions and prioritizations across the economy.

- With the real money, everyone cannot but be prudent!
  - No more stimulation via debts
  - By working hard to creating new value, you become rich.
  - You can share with others with what you've earned.
  - With money tied to time, money start to flow to real economic and productive activities.
  - Real economic activities produce goods and services.
  - Everyone can benefit from cheap but useful goods and services.

1st Home Work at GIST

1. Read the lecture note materials and the references.
2. Think about the following questions at least.
3. Write an essay (less than 10 page, 12 font size, Times New Romans) and submit.

- What do you like to do after reading these books so far?
- No matter what you believe in their work, but can you agree with their observation of how the world is moving and diagnosis that the money today has a problem causing inequality and crisis.
- After studying these materials, what position would you like to take?
  - 1. Use this knowledge and become rich.
  - 2. Diversify your portfolio and let others know as well.
  - 3. Do something to make a change.
- One says that you can make change by programming.
- Do you believe in these words?
- If yes, how do you think programming can change the world?

전형적인 비트코인 비평

- 누리엘 루비니(뉴욕대 스턴경영대학원 교수).
  - bitcoin is not a hedge against inflation and investors are 'feeding the bubble' …
  - bitcoin is a "pseudo-asset" that is pumped by "massive manipulation."2021. 2. 23.
  - 항상 시장을 비관, '닥터 둠'(Dr. Doom)불리움.
- 앤디 캐슬러(WSJ 기고가)
  - "비트코인 폭등의 이면에는 군중들의 광기를 이용하는 조작적인 배우들이 도사리고 있다"
  - "비트코인, 아무것도 아니고 그냥 사라질 수증기이며 아이디어일 뿐"
  - "비트코인이 실제 거래에 사용된 사례는 거의 없고 저장 수단도 아닌 단지 허공에서 가상적으로 떠다니는 신기루에 불과하다."

오래된 문제의 반복일 뿐

- In 1773 banks in England went in on a clearinghouse in London, for example, an improvement on the system of managing separate ledgers with each bank. The banks themselves took in gold coin—cumbersome to carry and verify—then created new money by offering more in loans than the gold they had on deposit.

- Bitcoin is fiat as well with no intrinsic value.
- With a new bitcoin, Bitcoin shall go back to zero.

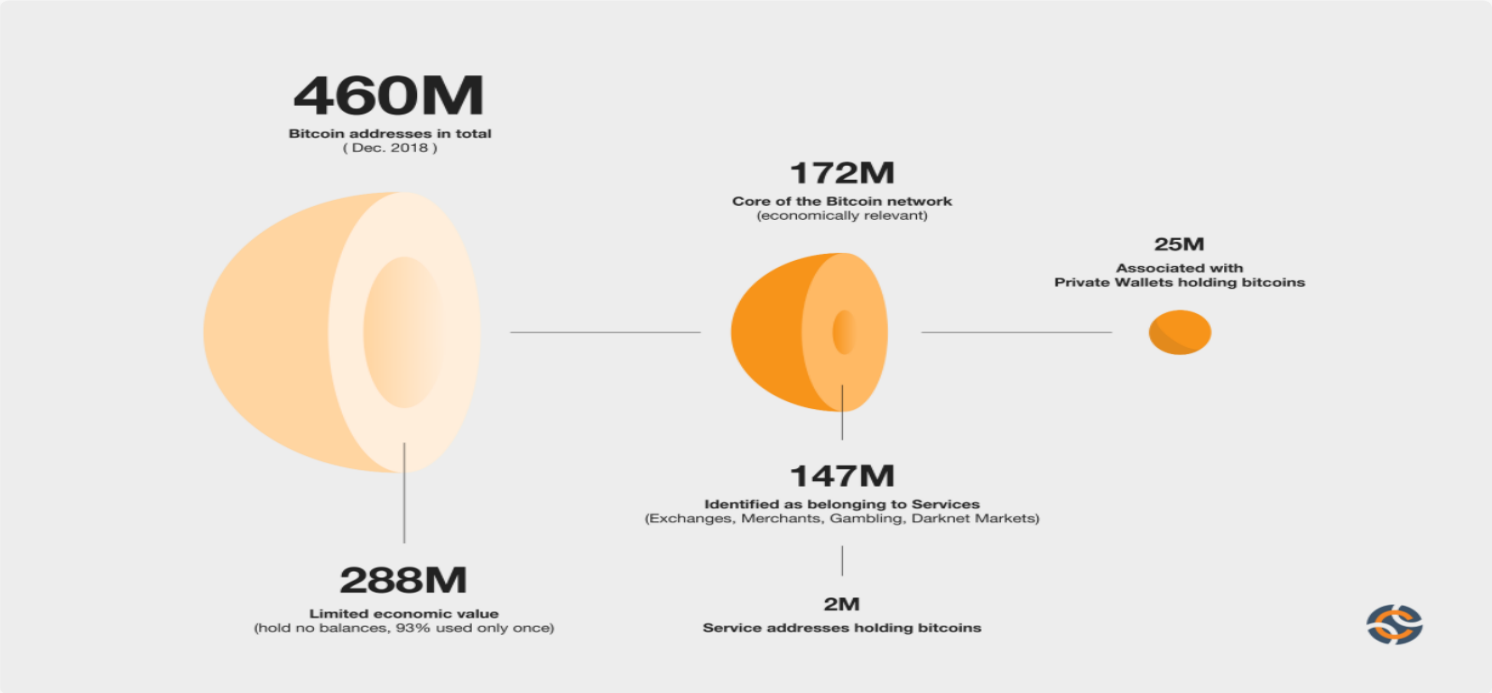
비트코인
현재의 모습을
분석해보자

Bitcoin소유자 추산 2400만명

How Many People Own Bitcoin?

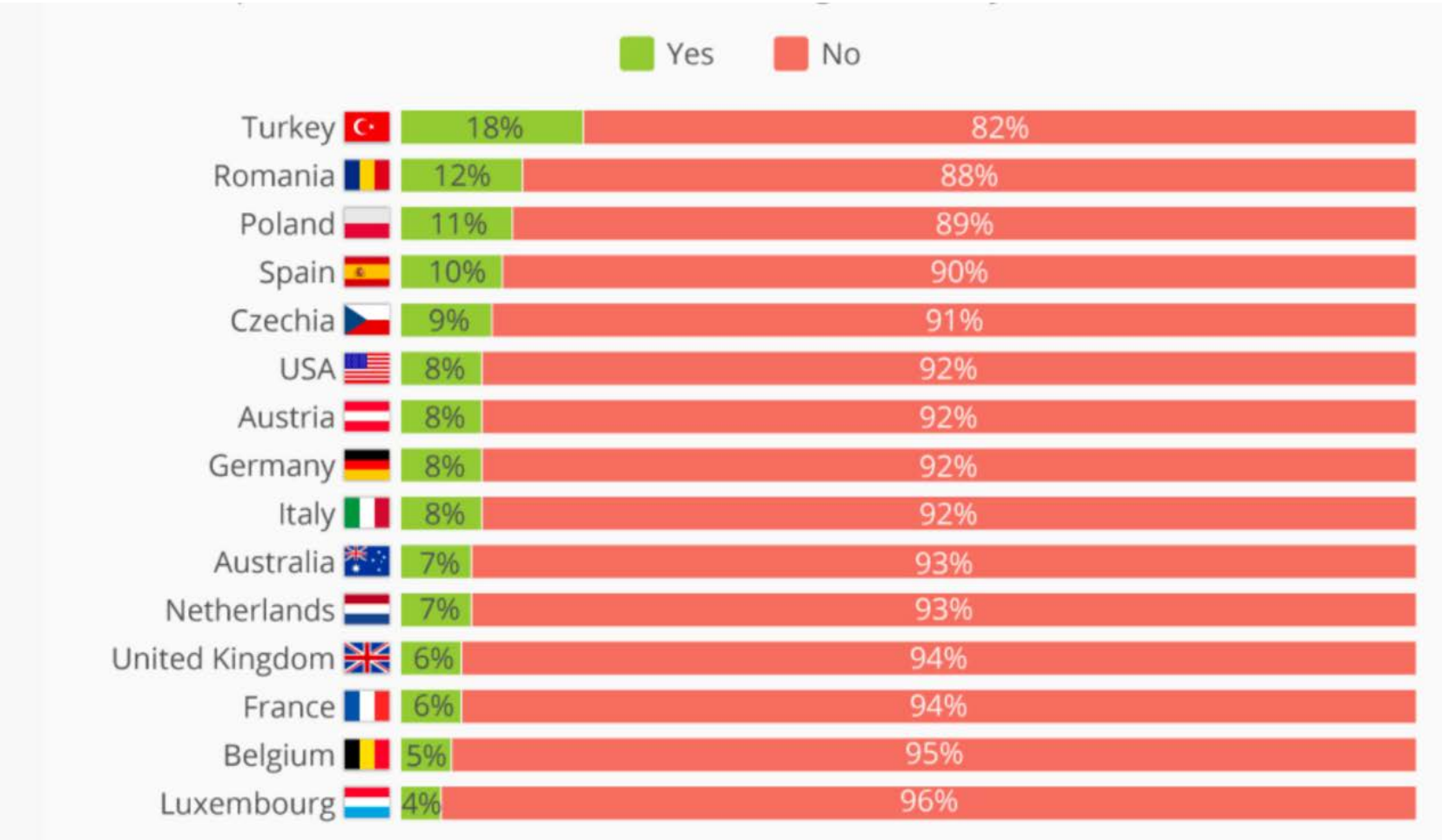
No one will ever know.

The most common method of estimating the number of Bitcoin owners is look at the amount held in different addresses.

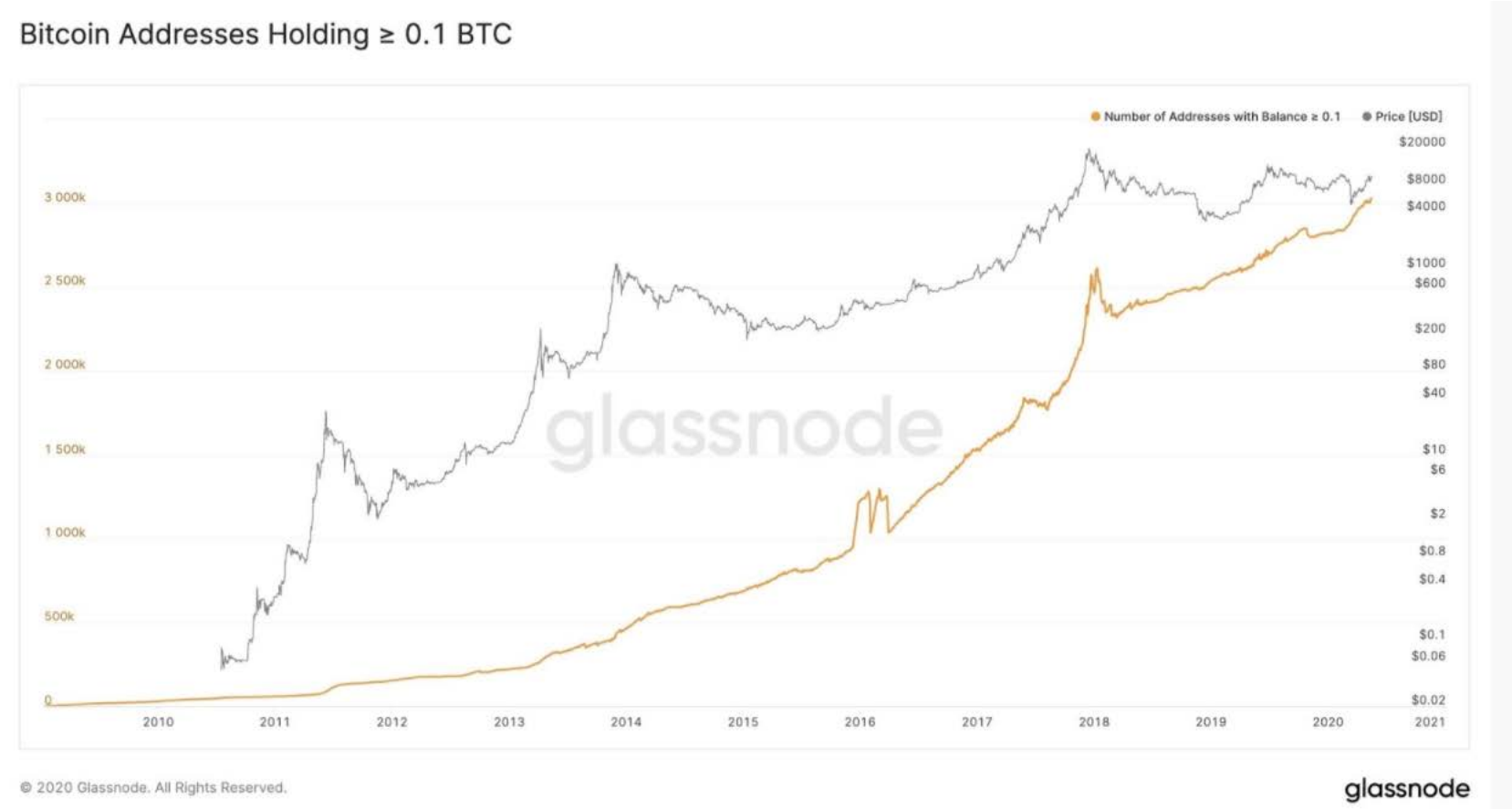


Bitcoin addresses in use - courtesy of chainalysis

국가별 비트코인 소유자 %


Yes
No
Turkey 18% 82%
Romania 12% 88%
Poland 11% 89%
Spain 10% 90%
Czechia 9% 91%
USA 8% 92%
Austria 8% 92%
Germany 8% 92%
Italy 8% 92%
Australia 7% 93%
Netherlands 7% 93%
United Kingdom 6% 94%
France 6% 94%
Belgium 5% 95%
Luxembourg 4% 96%

비트코인주소>0.1BTC ~ 3백 만



The number of addresses holding just .1 BTC is tiny.

Bitcoin Info 2021년 3월 30일

Total Bitcoin (sum of all currently existing Bitcoin)	18,667,884 BTC
Market Capitalization (market value of all currently existing Bitcoin)	**$1,069,000,935,655 USD**
Bitcoin Price	1 BTC = $ 57,264.17 USD (2021-03-30 06:12:02)
Transactions last 24h (Number of transactions in blockchain per day)	267,333
Transactions avg. per hour	11,139
Bitcoins sent last 24h	314,660 BTC ($18,018,757,796 USD) 1.69% market cap
Bitcoins sent avg. per hour (last 24h)	13,111 BTC ($750,781,575 USD)
Avg. Transaction Value	1.18 BTC ($67,402 USD)
Median Transaction Value	0.013 BTC ($755.64 USD)
Avg. Transaction Fee	0.00023 BTC ($13.03 USD) 0.00000042 BTC/byte
Median Transaction Fee	0.000092 BTC ($5.25 USD)

Bitcoin Info 2021년 3월 30일

Block Time (average time between blocks)	10m 0s
Blocks Count	676,892 (2021-03-30 05:35:39)
Block Size	876.628 KBytes
Blocks last 24h	139
Blocks avg. per hour (last 24h)	6
Reward Per Block	6.25+0.507 BTC ($386,935.95 USD) next halving @ block 840000 (in 163108 b
Reward (last 24h)	868.75+70.48 BTC ($53,784,097.21 USD)
Fee in Reward (Average Fee Percentage in Total Block Reward)	5.52%
Difficulty	21.866 T next retarget @ block 679392 (in 2500 blocks ~ 16 days 11 hours)
Hashrate	168.298 Ehash/s **-2.73%** in 24 hours
Bitcoin Mining Profitability	0.3196 USD/Day for 1 THash/s
Top 100 Richest	2,673,924 BTC ($153,120,057,754 USD) 14.32% Total
Wealth Distribution Top 10/100/1,000/10,000 addesses	5.19% / 14.32% / 33.50% / 58.61% Total
Addresses richer than 1/100/1,000/10,000 USD	32,900,480 / 15,838,148 / 6,853,416 / 2,338,104
Active Addresses last 24h (Number of unique (from or to) addresses per day)	885,381
100 Largest Transactions	last 24h: 801,142 BTC ($45,876,736,900 USD) 254.61% Total

BTC 시총, RUB 시총 추월

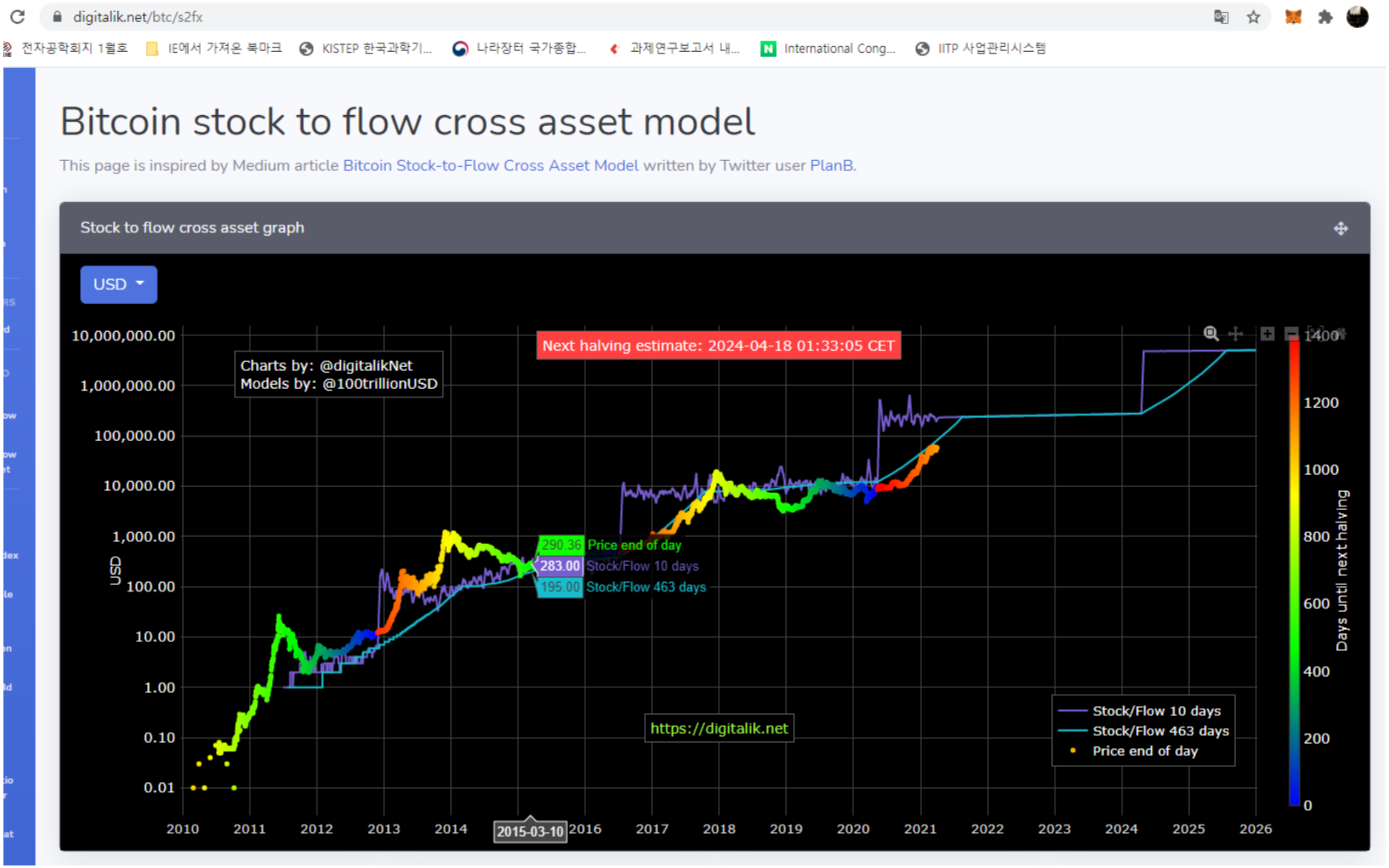
Blockcast.cc Feb. 10th, 2021

#	Currency	Market Cap	Price	Circulating Supply	Max Supply
1	CNY	726,968,545 BTC	328 sats	221,300,000,000,000 CNY	Unlimited
2	USD	410,637,587 BTC	2,113 sats	19,424,767,542,000 USD	Unlimited
3	EUR	345,851,628 BTC	2,558 sats	13,517,482,000,000 EUR	Unlimited
4	JPY	298,978,143 BTC	20 sats	1,479,242,000,000,000 JPY	Unlimited
5	GBP	95,170,645 BTC	2,916 sats	3,263,167,000,000 GBP	Unlimited
6	KRW	84,896,004 BTC	1 sats	4,462,726,000,000,000 KRW	Unlimited
7	INR	53,086,997 BTC	29 sats	183,004,000,000,000 INR	Unlimited
8	CAD	48,493,984 BTC	1,664 sats	2,913,897,000,000 CAD	Unlimited
9	HKD	42,663,902 BTC	272 sats	15,644,043,000,000 HKD	Unlimited
10	AUD	39,860,409 BTC	1,632 sats	2,441,000,000,000 AUD	Unlimited
11	TWD	37,553,782 BTC	75 sats	49,721,350,000,000 TWD	Unlimited
12	BRL	31,328,870 BTC	389 sats	8,041,803,000,000 BRL	Unlimited
13	CHF	27,030,198 BTC	2,367 sats	1,141,566,000,000 CHF	Unlimited
14	BTC	18,624,275 BTC	100,000,000 sats	18,624,275 BTC	21,000,000 BTC
15	RUB	16,746,017 BTC	28 sats	58,651,000,000,000 RUB	Unlimited

BTC 현재 모습의 시사점

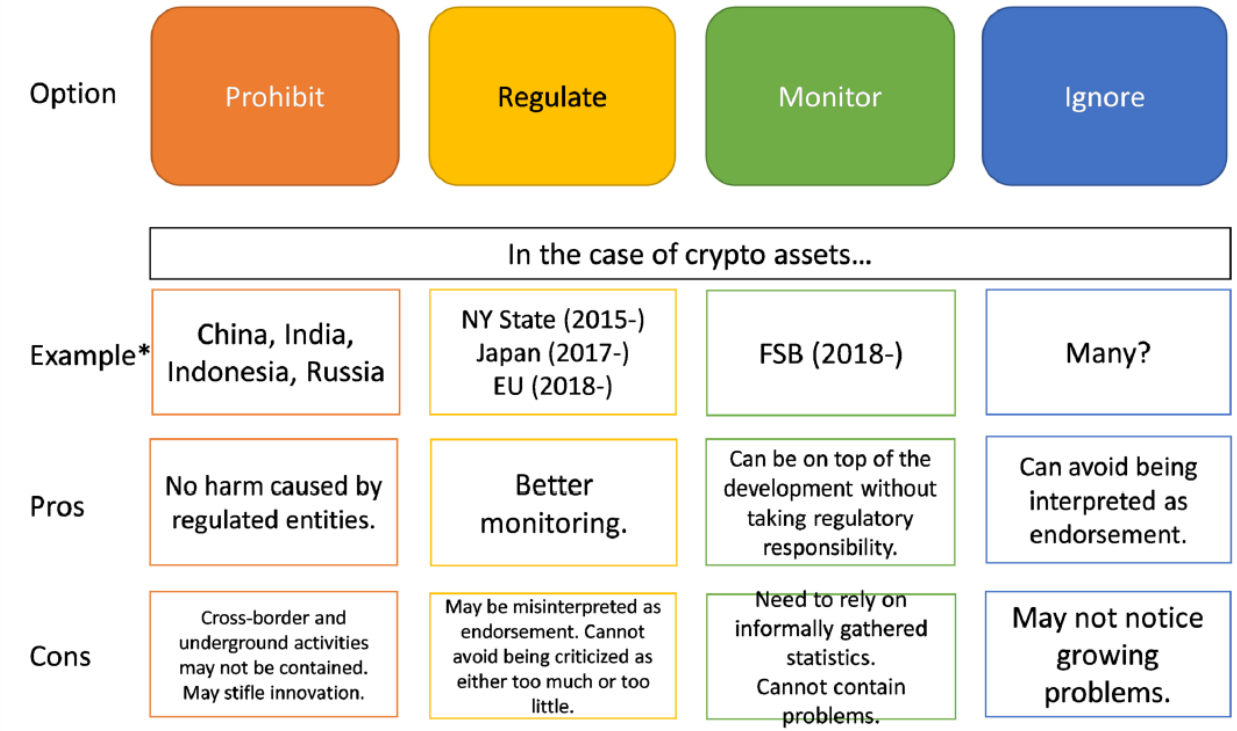
- 소유자는 60억 인구의 0.4% 인 2400만 명.
- 만 개의 주소(0.1%)가 BTC 50% 소유.
- 대부분 투자용으로 축적만 하는 상황.
- 하루 거래량은 MC의 1.69%
- 총 유통량 (Stock)= 18 M BTC
  - 하루 총 발행량 = 900 BTC/day
  - 일년 총 발행량(Flow) = 328500 BTC/year
  - S/F = 52 (cf: Gold S/F = 62)
- 이게 과연 Sound Money의 모습일까?

S2F BTC Price Model, 기하급수적 성장



FED가 BTC의 위협을 보고만 있을까?

Fragmented Regulatory Approaches



* Prohibition, regulation and monitoring refer only to certain scope of businesses or activities related to crypto-assets. For more specific descriptions, please refer to FATF, "FATF Report to G20 Finance Ministers and Central Bank Governance," July 2018.

4

INTERNATIONAL MONETARY FUND

Source: FSA Japan

재닛 옐런 "난 비트코인의 팬 아냐"

'2018 캐나다 핀테크 포럼' 연설 통해 비트코인 비판
과거에도 "비트코인, 매우 투기적 자산" 발언
"중앙은행 암호화폐 발행, 재정 안정에 부정적"

박선우 기자 | 2018-10-31 09:40:03

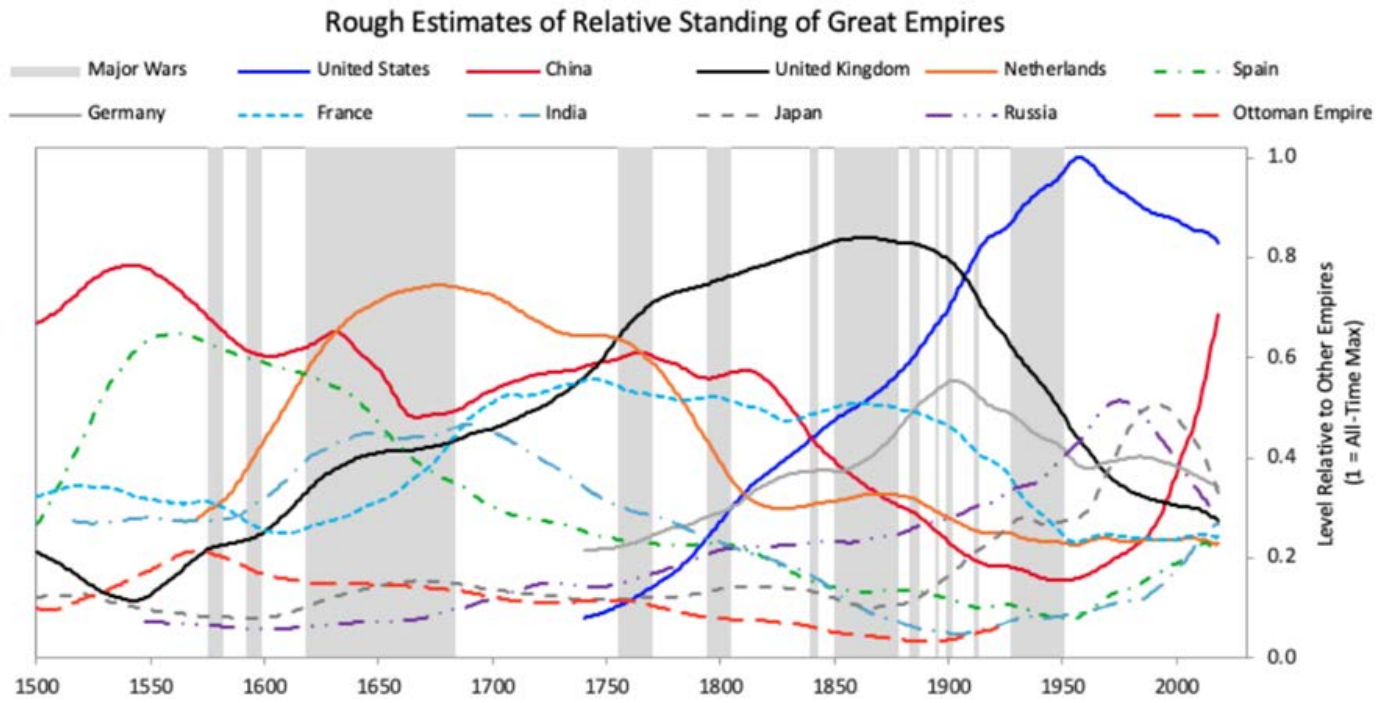
가 가

재닛 옐런 전 연방준비제도 의장/사진='2018 캐나다 핀테크 포럼' 홈페이지 캡처

미국 중앙은행인 연방준비제도(Fed·연준) 의장을 역임했던 재닛 옐런(Janet Yellen)이 비트코인에 대한 부정적인 입장을 재확인했다.

THE CHANGING WORLD ORDER

- By Ray Dalio
- https://www.principles.com/the-changing-world-order/
- **Ray Dalio** is Founder of Bridgewater Associates. He, it is known, started Bridgewater out of his two-bedroom apartment in New York in 1975 and under his leadership, the firm has grown into one of influential ($18.7 Billion) hedge funds companies in the US according to Fortune Magazine.
- This book is about how different empires such as China, Nederland, and England in the past have evolved over time from the birth to the demise to a successor. The aim of this book, or the research done, is to protect the wealth (of his companies and his followers) by provision of better understanding the nature of empires and wars, the eight stages an empire goes through, and the role of its reserve currency and finance during these stages.



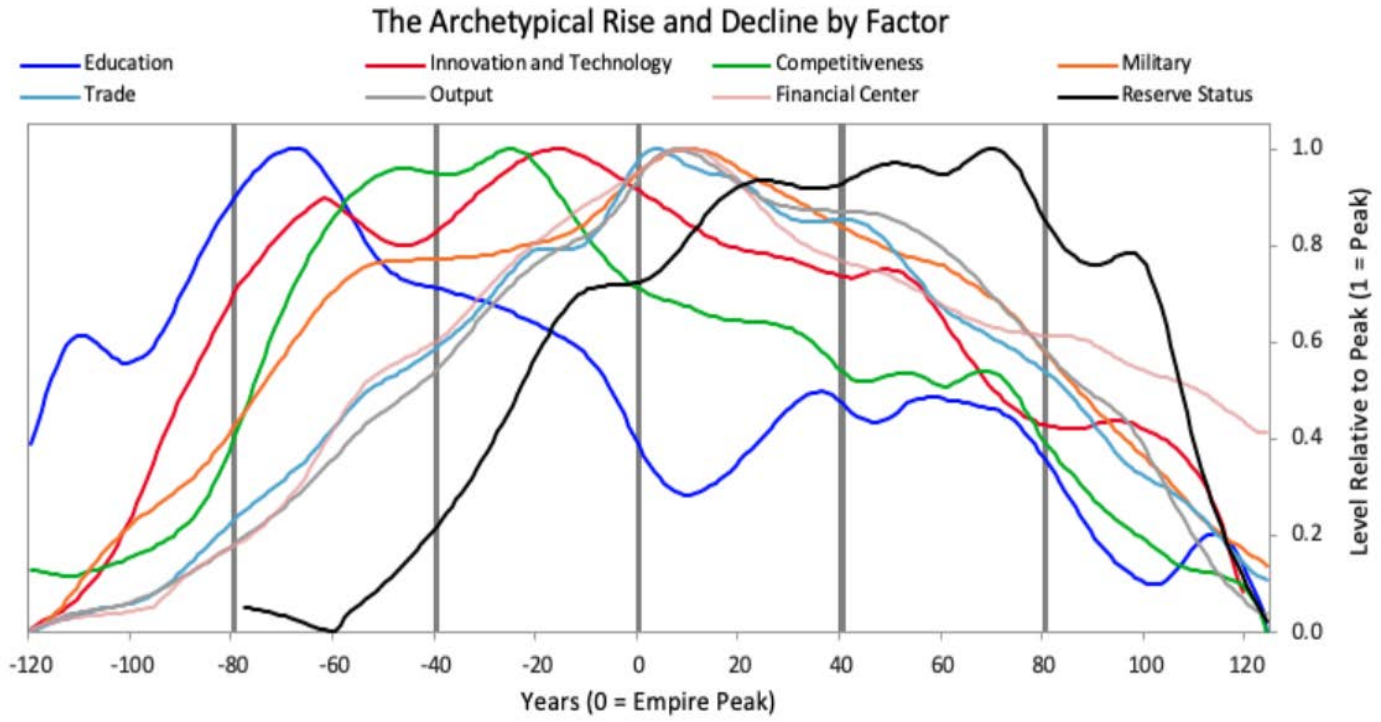
The graph above shows a level relative to other empires (1 = all time high)

- 1500 – 1600: China
- 1625 – 1750: Nederland
- 1750 – 1900: The United Kingdom

1900 – current: The United States of America, The China is rising.

8 measures of wealth and power

- Education
- Competitiveness
- Technology
- Economic output
- Share of world trade
- Military strength
- Financial center strength
- Reserve currency



- The chart above shows that the power in Education comes first and followed by Innovation and Technology.
- Education (Blue) → Innovation and Technology (Red) → Competitiveness (Green), Military(Orange), Trade (LGreen), Financial Center(Peach) → Reserve Status.
- Note that the one comes last is the status of Reserve Currency.

Questions

- Should we go back to the gold standard?
- Could Bitcoin be a solution to these problems?
- Where does the US stand in 2021?
- What do you think is the reason that the Bitcoin price getting higher and higher?

- Bitcoin is mobile, scarce, energy-binding, free, and open assets.

계속되는 통화가치 하락, 어디에 나의 자산을 둘 것인가?

- "달러의 가치는 매년 20%씩 감소"
- "금은 FED가 가격을 콘트롤 하고있고..."
- "제국의 마지막은 기축통화 지위를 남용, 엄청난 양극화를 유발, 전쟁 혹은 혁명이 일어나며 해결"
- "BTC의 가치는 매년 20%씩 상승..."
- "정부는 누진세, 재산세 인상..."
- 개인의 입장
  - 젊었을 때 일해서 모은 자산으로
  - 아이들과 가족과 함께
  - 운동하고, 그림 그리고, 노래하고, 창작활동을 하고
  - 안정되고 평화로운 노후를 설계할 수 있어야...
- BTC가 과연 Sound Money 인가?

감사합니다!

Q&A

이흥노

heungno@gist.ac.kr

Home page: http://infonet.gist.ac.kr

Facebook/Publication ID: Heung-No Lee

References

1. GIST 대학원 교과목 <Blockchain and Future Society>
   https://infonet.gist.ac.kr/?page_id=8954

2. Heung-No Lee, "DeSecure Blockchains," ETH-CON, Seoul, Reb. of Korea., May 2019.

3. Heung-No Lee, "Blockchain Consensus and Governance," July Meet-Up, Institute of Blockchan and Law, July 11th, 2019. YouTube Video Available at https://www.youtube.com/watch?v=7ujkFgsKPdY.

Selected References of GIST Blockchain Economy Center

- [Lee1] JH Jang and Heung-No Lee, "Profitable Double Spending Attacks," March 5th, 2019 submitted to IEEE Trans. Information Forensics and Securities, downloadable from https://arxiv.org/abs/1903.01711.
- [Lee2] 장재혁, 이흥노, "50%미만 이중 지불 공격", OSIA S&TR Journal, Vol. 32, No. 1, Mar. 2019. (pdf)
- [Lee3] 정현준, 이흥노, "암호화폐 투자와 규제 현황", 한국정보과학회, 정보과학회지, 제 36권, 제 12호, pp. 49-56, Dec, 2018. (pdf)
- [Lee4] 박상준, 김형성, 이흥노, "Introduction to Error-Correction Codes Proof of Work," 블록체인경제 특집호, 대한전자공학회지, June 2019.
- [Lee5] Sangjun Park, HS Kim, Heung-No Lee, "Time-Variant Proof-of-Work Using Error-Correction Codes," to be submitted to IEEE Trans. Information Forensics and Securities.
- [Lee6] Mohamed Yaseen.J, Giljun Jung and Heung-No Lee."Decentralized Framework for Medical Images Based on Blockchain and Inter Planetary File System", The 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society(EMBC 2019), Berlin, Germany, Jul. 23-27, 2019.
- [Lee7] Please visit INFONET home page https://infonet.gist.ac.kr/?page_id=14 for more references.