블록체인 기술의 이해와 활용

Heung-No Lee
GIST, South Korea

11월 28일 (목) 14:00 ~ 17:30 주공본사 6층 대학당
부산시 남구 문현금융로40, 부산국제금융센터
11월 29일 (금) 14:00 – 17:30 남산T타워21층 주택도시보증공사회의실 1
서울 중구 소월로2길 남산T타워
Home page: https://infonet.gist.ac.kr
Facebook/Publication ID: Heung-No Lee

교육 순서

14:00-14:10 교육 및 강사소개
14:10-15:40 이장우 교수 발표
15:40-16:00 휴식
16:00-17:30 이흥노 교수 발표

강의순서

- Bitcoin
- Ethereum
- ICOs
- Policies
- Summary

고령사회, 소득양극화, 경제위기

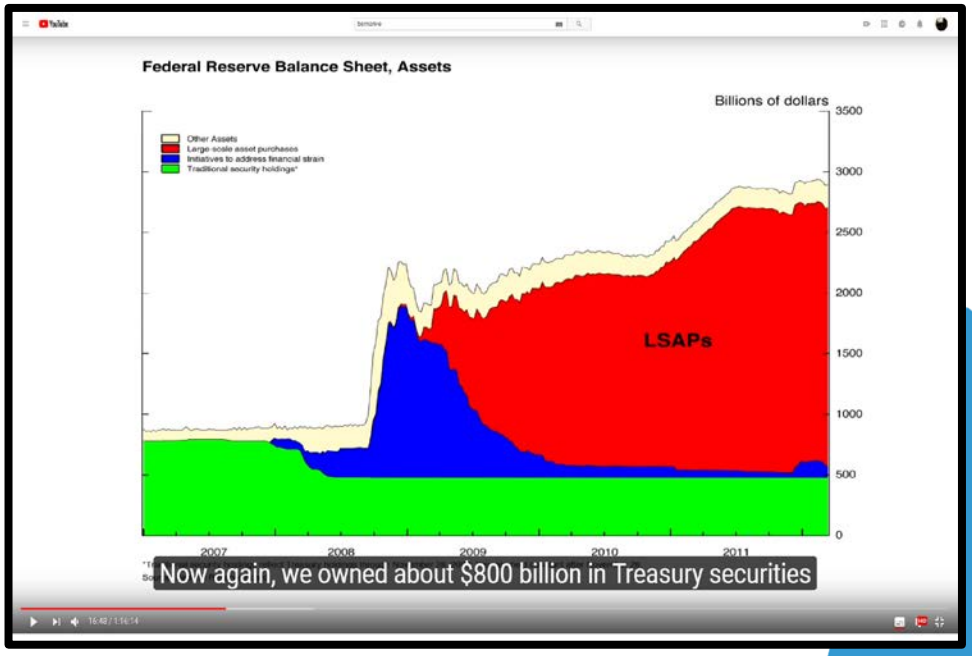
경제, 화폐, 그리고 정부

- 사람들은 누구나 과거보다 더 나은 미래(경제적 지위 및 발전된 자아)를 꿈꾼다!

- **정부는 사람들을 위해 원하는 것을 제공!**
  - 음식, 집과 같은 **의식주**
  - 전기, 물과 같은 **에너지**
  - 안정된 **치안** 환경
  - **레저**를 즐길 수 있는 좀 더 여유로운 근무환경
  - 한정된 자원에 대한 공평한 **기회**
  - 자녀들을 위한 안정된 **교육** 기회

미국의 금융위기, 연준, 그리고 양적 완화

- 2007~2008년에 미국에서 주택 담보대출 부실 로 인한 금융위기 발발!
- 리만브라더스 등 대형 은행 파산!
- 다수의 대형은행이 동시에 파산 위기로 내몰렸으나 총체적인 금융시스템의 붕괴를 막기위해 정부가 나섬!
- AIG, 골드만삭스, 모건 스탠리와 같은 금융회사를 정부가 구제해줌
- 미 연준이 금리를 대대적으로 낮추기 시작!
- 대규모 자산매입 (Large Scale Asset Purchases)를 통한 양적 완화(Quantitative easing)
  - 미연준이 국채 등의 자산을 대규모로 매입
  - 자산을 처분한 금융회사들은 돈(유동성)을 공급받음으로 유동성 공급 효과
  - 유동성 자금들은 주식, 부동산과 같은 자산에 투입됨으로 새로운 버블 형성

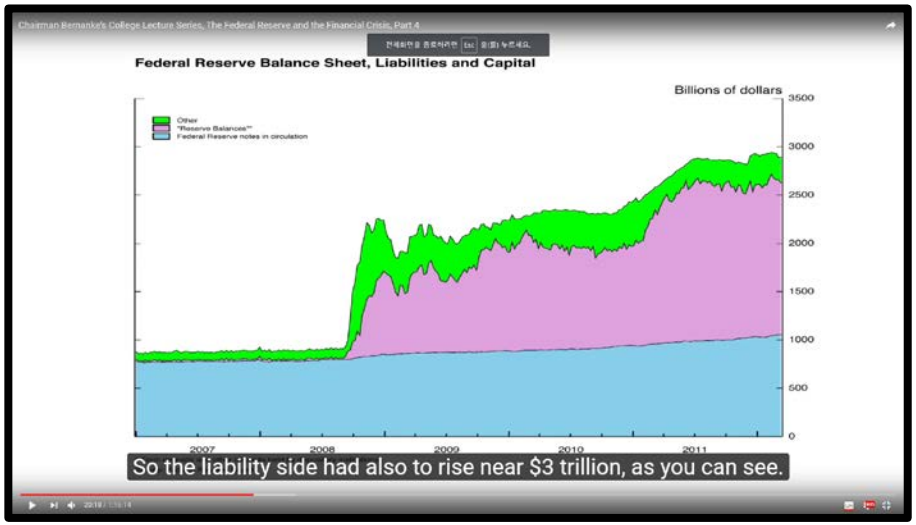


미연준은 어떻게 자산매입(LSAPs)을 하였을까?

"비전통적인 통화정책인 양적완화의 정식명칭은 대규모 자산매입(LSAP· Large-Scale Asset Purchases)인데 2007년 5.25%까지 올라갔던 연방기준금리는 2008년초 2% 대에서 그해말 0~0.25%로 떨어집니다. 이 때부터는 경기침체 상황을 막기 위해 더 이상 금리를 완화할 여지가 없습니다. 그래서 비전통적(Unconventional) 방식으로 경기 부양을 위한 통화 정책을 쓸 수밖에 없습니다. 연준이 시중은행으로부터 국채나 정부가 보증한 패니와 프레디 증권을 사들이는 것입니다. 이런 식으로 국채를 사들여 시중에 자금이 풀리는데 2009년부터 2012년까지 총 규모는 2조달러를 넘어섰습니다." 2014년 6월 현재까지 3조달러가 넘게 풀렸다.

이 돈을 미국 재무부 조폐창의 윤전기로 찍어냈을까? 버냉키 의장은 여기서 양적완화의 마술이 나온다고 주장한다. "증권을 매각한 은행은 연준에 예치하는 지급준비금(reserve balances) 계좌를 갖고 있습니다. 연준이 증권 매입 대금을 지급하는 방식은 기본적으로, 은행들이 연준에 개설하고 있는 계좌에 지급준비금 액수를 늘려주는 것입니다. 연준이 취득하는 증권의 대금 지급을 위해 돈을 찍어내고 있다는 말을 듣게 됩니다.

그러나 사실을 말하자면, 증권을 취득하기 위해 연준이 돈을 찍어내고 있는 것은 아닙니다."



벤버냉키 미연준의장 2012년 3월 조지워싱턴대 강연

http://www.hani.co.kr/arti/economy/economy_general/641160.html#csidxd73fb7e39c21cc6bdc51afa5c568217

월가에 대한 개혁요구 (버니샌더스 상원의원)

월스트리트는 그 자체적으로 계속해서 **수십억 달러에 달하는 위험한 재정적 결정**을 내릴 수는 있지만 대중은 이를 구제 할 것을 기대하고 있습니다.

나라에서 가장 큰 금융 기관을 해체 할 때입니다.

오늘날이 나라에서 **가장 큰 6 개의 금융 기관은** 국내 총 국내 생산량의 약 60 %에 해당하는 자산을 보유하고 있습니다. 이 6 개의 은행은 모든 신용 카드의 3 분의 2 이상을 발행하고 모든 모기지의 35 % 이상을 발행합니다. **모든 파생 상품의 95 %를 관리하고 미국 내 모든 은행 예금의 40 % 이상을 보유합니다**.

우리는 큰 위험을 만들어낼 수 있는 대형 금융 기관을 해체해야합니다.

이 기관들은 미국 납세자로부터 **700억달러의 구제 금융을 받았으며**, 연방 준비 은행으로부터 사실상 **16 조 달러 이상의 이자 대출을 받았습니다.** 그럼에도 불구하고, 금융 기관은 2014 년에 1,500 억 달러 이상의 수익을 올렸습니다. 기록상 가장 수익성이 높은 해이며, 4곳 중 3곳은 오늘날 우리가 파산(2008 금융위기)하기 전에 비해 80 % 더 큽니다.

우리 은행 시스템은 생산적이고 일자리 창출 경제의 일부여야합니다. 은행 산업의 엔진 역할을 하는 정부 기관인 미연준은 내부 이해 상충을 제거하고, 보다 철저한 감독을 제공하며, **은행은 극소수 아닌 모든 사람에게 혜택이 돌아가도록 서비스를 제공해야 합니다.**

신용의 진화

Scientific American **318, 38 - 41 (2018)**
Published online: 19 December 2017
| doi:10.1038/scientificamerican0118-38

Natalie Smolenski

- **은행과 정부는** 여러 가지면에서 특히 지난 수십 년간 세계 경제에 대한 **신뢰를 중개하지 못했습니다. 평범한 사람들은 중앙 집중식 권력에 경계하고 있으며 대안을 찾고 있습니다.**
- 블록 체인 기술 기반 **비트코인**은 **신뢰 중개를 기계가 대신하고 은행가와 같은 사람으로부터 멀어지게** 합니다. 이 기술을 처벌하기 보다 잘 활용할 수 있습니다.
- 블록 체인은 **인간 해방과** 전례 없는 수준의 감시 및 통제에 모두 적합합니다. 그것들이 어떻게 사용될지는 소프트웨어가 **디지털 신원**을 처리하는 방법에 달려 있습니다.

I am the 1%, Let's Talk!

- Con:
  - FED, TARPs, LSAPs.
  - Gov. deficit spending
  - Socialism
  - Regulations
- Pro:
  - Small government
  - Free market capitalism
  - Entrepreneurship
  - Making money means creating jobs with new goods and services.

- His paying 50% of his income to tax.
- If he did not pay the tax, he could have re-invested and made more jobs.

Peter Schiff at Occupy Wall Street "I am the 1%. Let's Talk"

조회수 1,265,631회 2.9만 2천 공유 저장 ...

비트코인의 탄생과 더불어 생각해봐야할 이슈들

- 오늘날에 통화 그 자체는 돈이 될 수 없다.
  - 미 달러화 조차도 그 자체로 내재적 가치는 가지고 있지 않다. (금본위제가 아니므로)
  - 통화는 누군가가 은행에 대출을 받거나 정부가 채권 (I.O.U.)을 발행 할 때 또는 FED에 정책기조에 따라 상업 은행에 대한 **전자 잔고를 증가시킴으로써** 은행에 의해 생성됩니다.

- 빈번한 금융위기로 정부의 신뢰가 크게 훼손되었음.
  - 사람들은 재정적자와 위험한 통화 확장 정책에 의문을 재기하고 있다.

- 비트코인의 이슈는...
  - 탈중앙화
  - 월가의 개혁
  - 대기업 집중식의 분산화
  - 불평등의 감소

사용자들 간의 신뢰를 기반으로 한

비트코인의 탄생

Bitcoin: A Peer-to-Peer Electronic Cash System

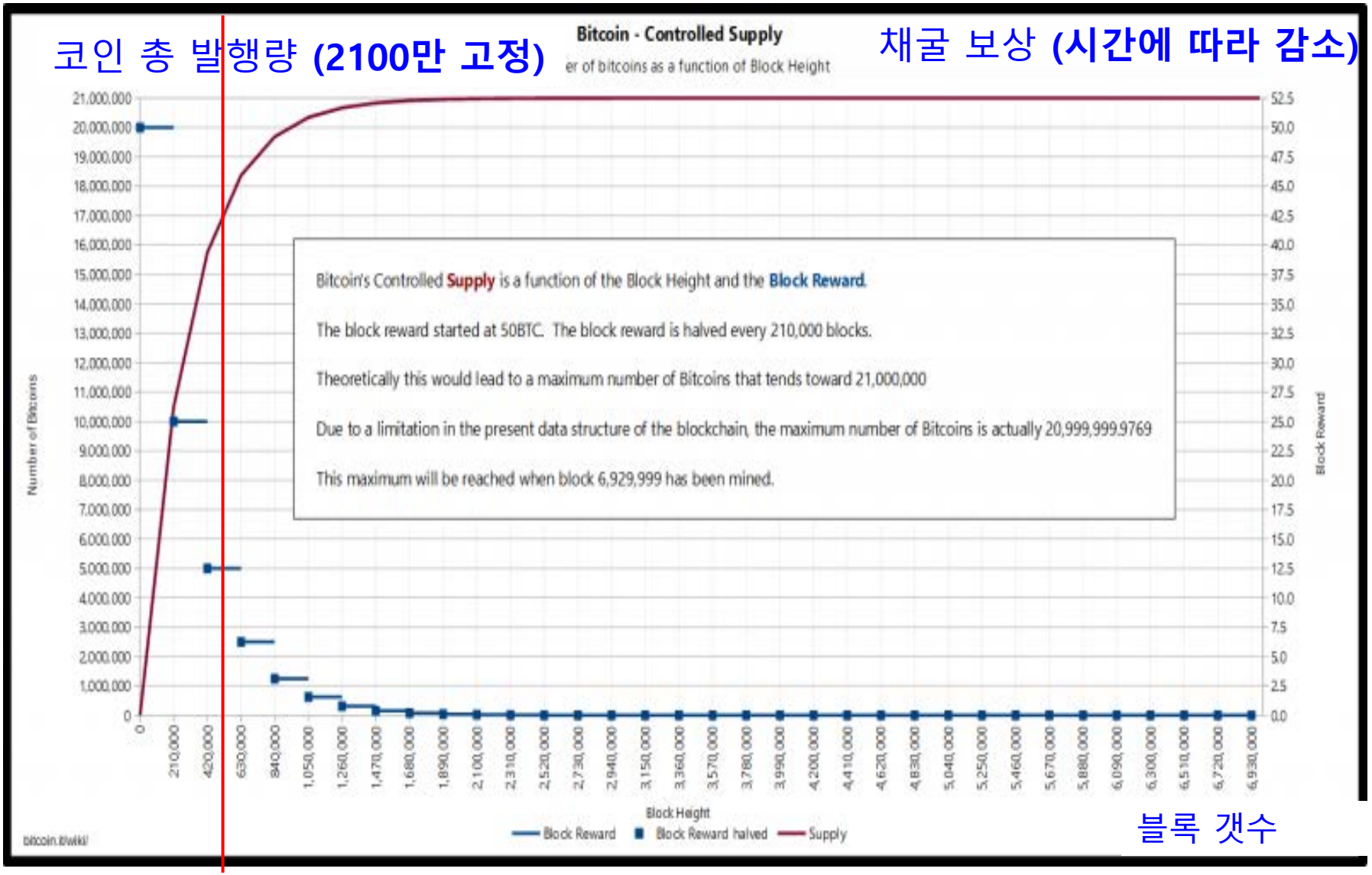
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

비트코인

- 2009년 탄생 이래로 멈추지 않고 살아 숨쉬는 통화 시스템
- 국경을 초월하는 전세계 통용 가능한 전자 화폐
- 은행과 정부의 신뢰가 바닥에 추락했을 때 이것은 태어났습니다. (2008년 미국 금융위기 전후로)
- 10분마다 계속해서 비트코인을 생성

비트코인의 채굴 스케줄



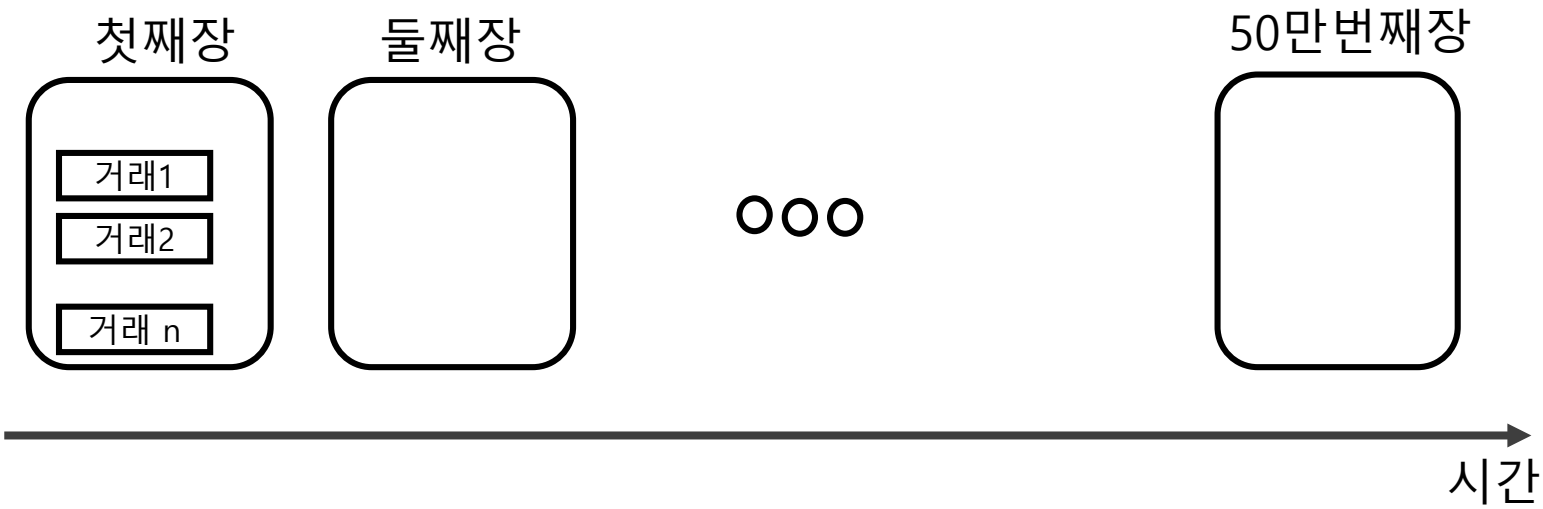
2018년

어떻게 비트코인이 작동할까요?

비트코인은 인터넷 기반 컴퓨터네트워크와 P2P 프로토콜을 기반으로 작동합니다.

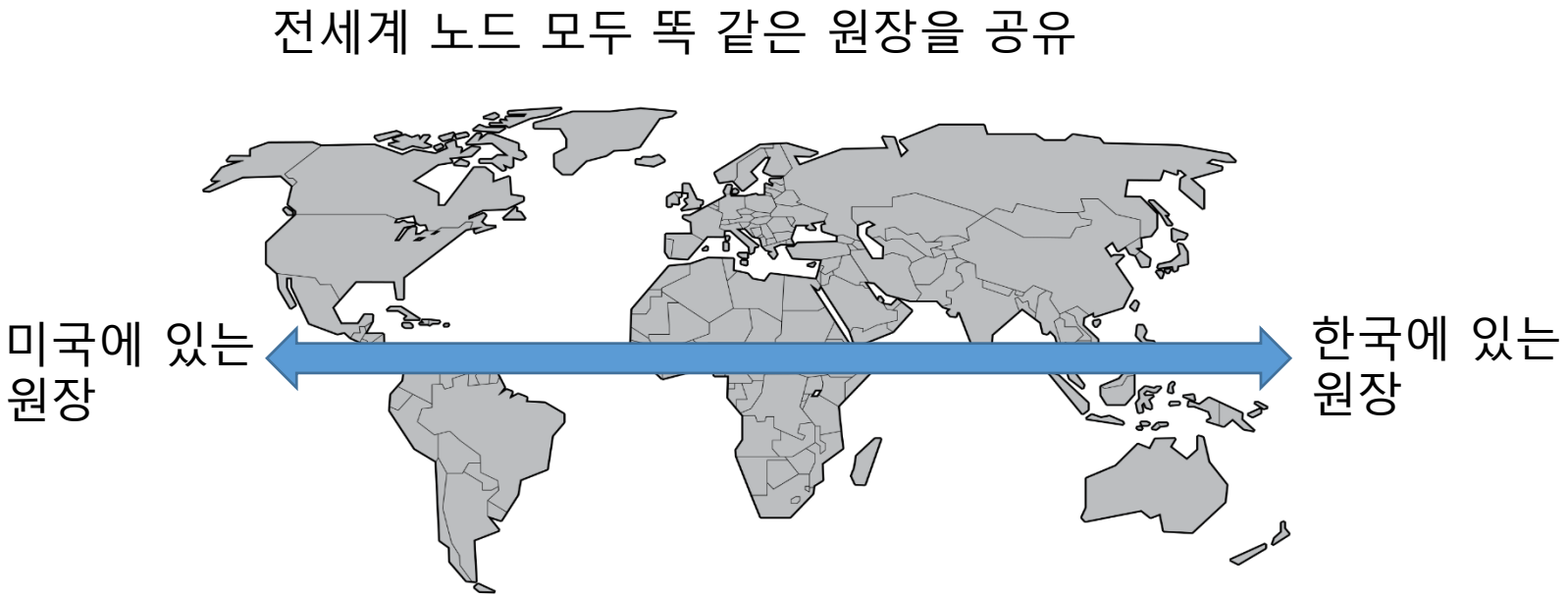
동일한 블록체인을 공유하는 P2P노드

- Blockchain의 정의:
  - *시간의 순으로* 발생하는 *모든 거래 내역을 순서대로* 그때 그 때 바로 기록한 것을 **블록체인 원장**이라고 정의할 수 있습니다.



모두에게 공개된 블록체인

- 이 원장을 **인터넷에 공개해** 놓고 거래내역을 누구나 들여다 볼 수 있게 했습니다.



어디에서나 채굴 가능한 블록체인

- 거래기록 작성은 특정인이나 단체 혹은 국가가 **독점하지 못 하도록** 하였습니다.

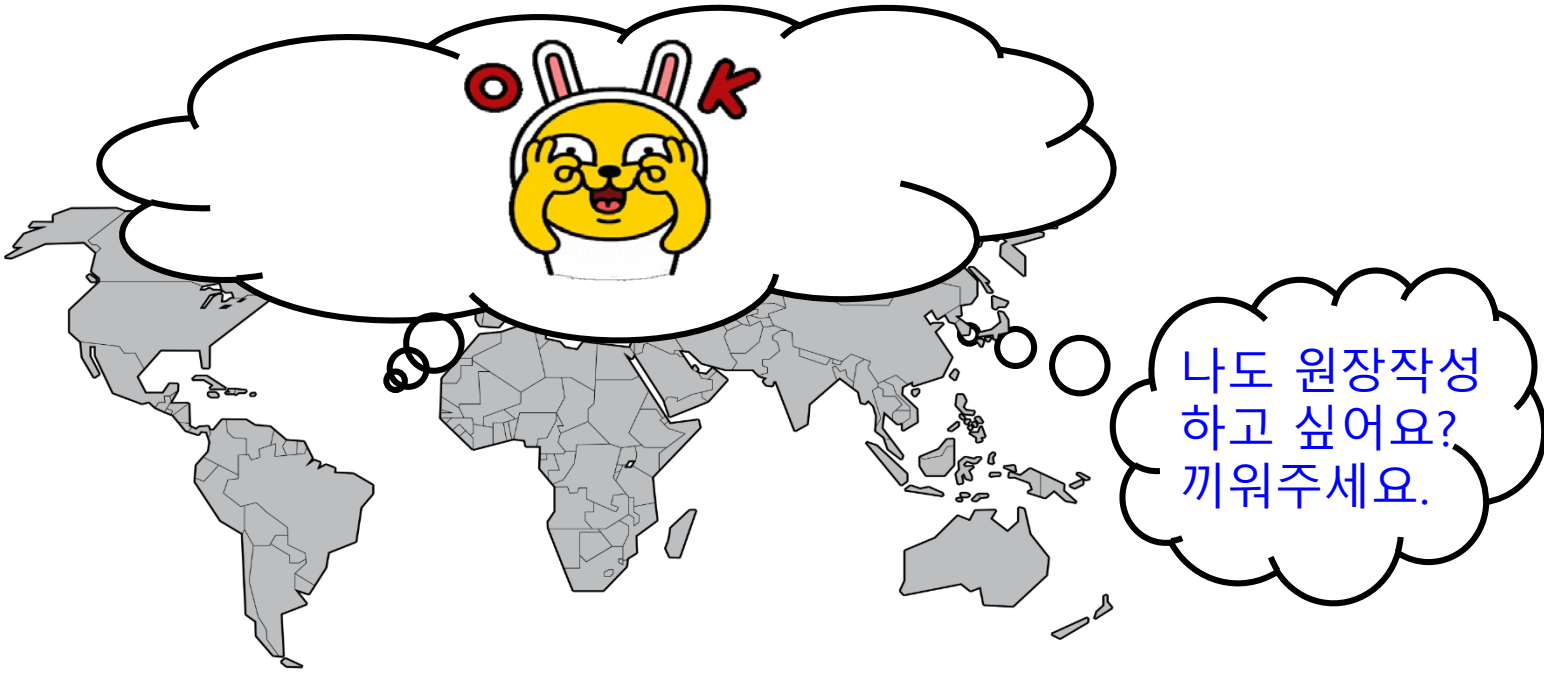
502번째 블록은 **중국**에서 작성

500번째 블록은 **미국**에서 작성

501번째 블록은 **한국**에서 작성

누구나 참여할 수 있는 블록체인

- 오히려 누구든지 거래원장 기록에 참여할 수 있도록 열어 놓은 분산 형 원장 작성 기술입니다.

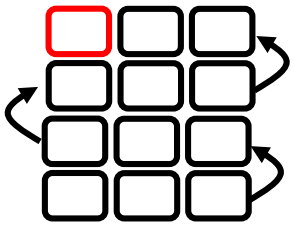


블록체인의 합의 메커니즘

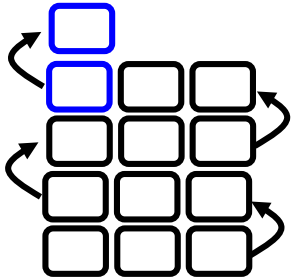
- 누구나 작성에 참여하고 인터넷에 공개된 파일임에도 불구하고 **어떤 것이 원본인지 구분할 수 있도록** 전혀 새로운 방식의 원장 동의 프로토콜을 만들었습니다.

동시에 2개의 다른 체인이 공표될 때
어떤 체인이 원장이 되나?

100번째장 작성
성공! 야호!



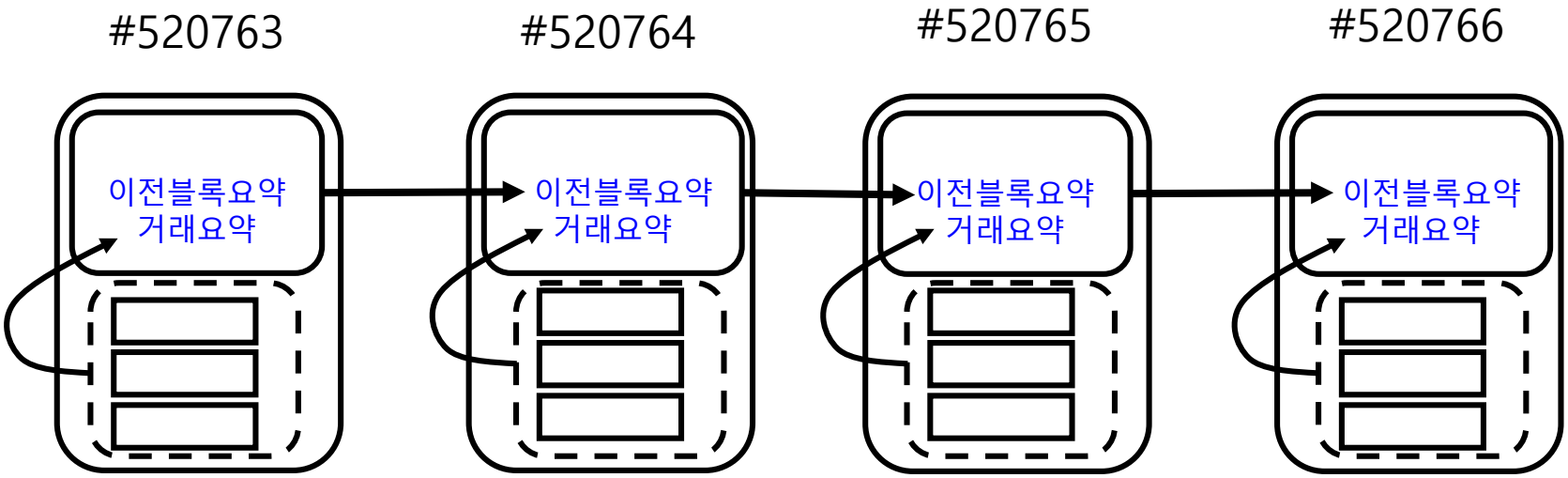
101번째장 작성
성공! 야호!



긴 체인이 승리!

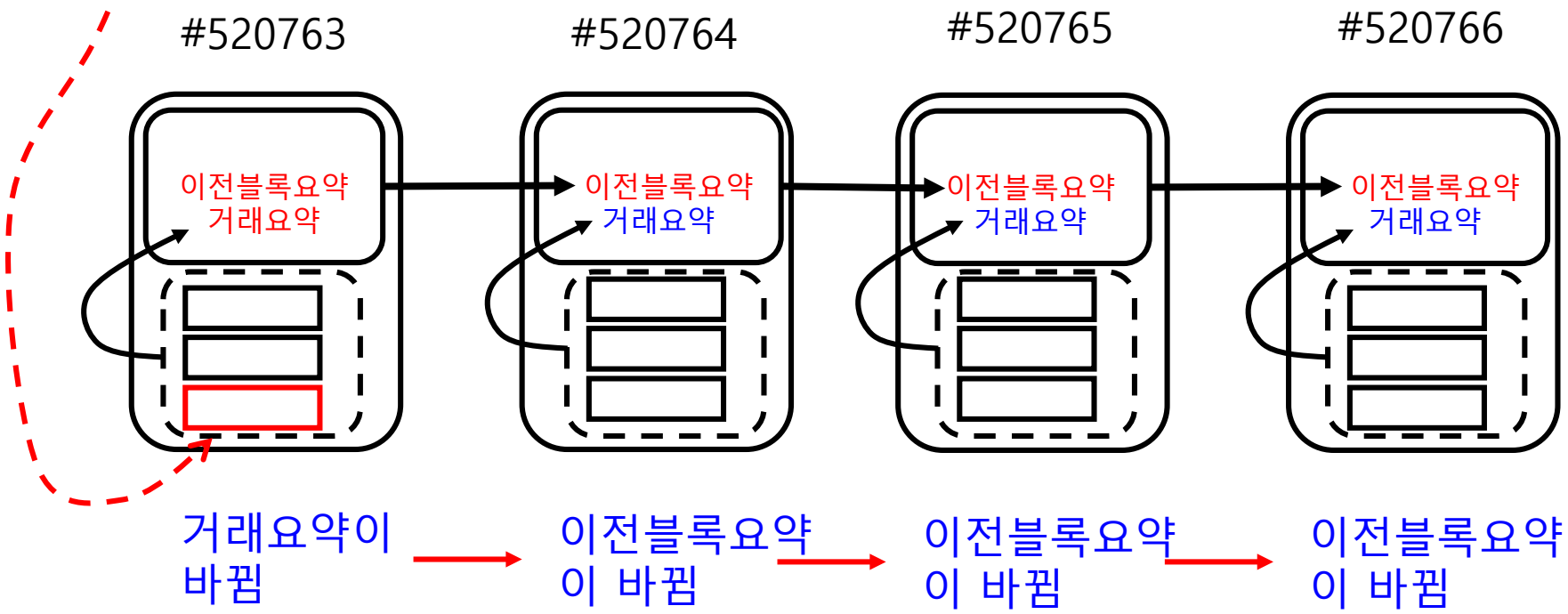
임의 변경 불가능한 블록체인

- **암호학적 설계로** 원장에 기록된 내용을 임의로 바꿀 수 없습니다.
- 임의 변경 내용은 **해시값 대조를** 통해 바로 확인이 가능합니다.



위조나 변조 시?

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



들통나지 않고 변조하려면 해당 블록 및 그 후 요약을 모두 다시 찾아서 기록하면 됨 → 불가능

프로그램 집합체인 블록체인

블록체인 구성 요소 3가지

1. 인터넷망을 기반으로 한 P2P노드들의 네트워킹

- 노드 등록, 주소 할당 및 획득
- Full 노드 또는 light 노드
- 채굴자와 지갑들 사이의 통신

2. TX 생성을 위한 지갑 어플리케이션

- 주소, 개인 및 공개 키를 만들고, UTXO를 저장하고, TX를 만들고, 서명하고, 이웃에게 알리고, TX가 블록 체인에서 지원되는지 확인

3. 블록체인 프로토콜

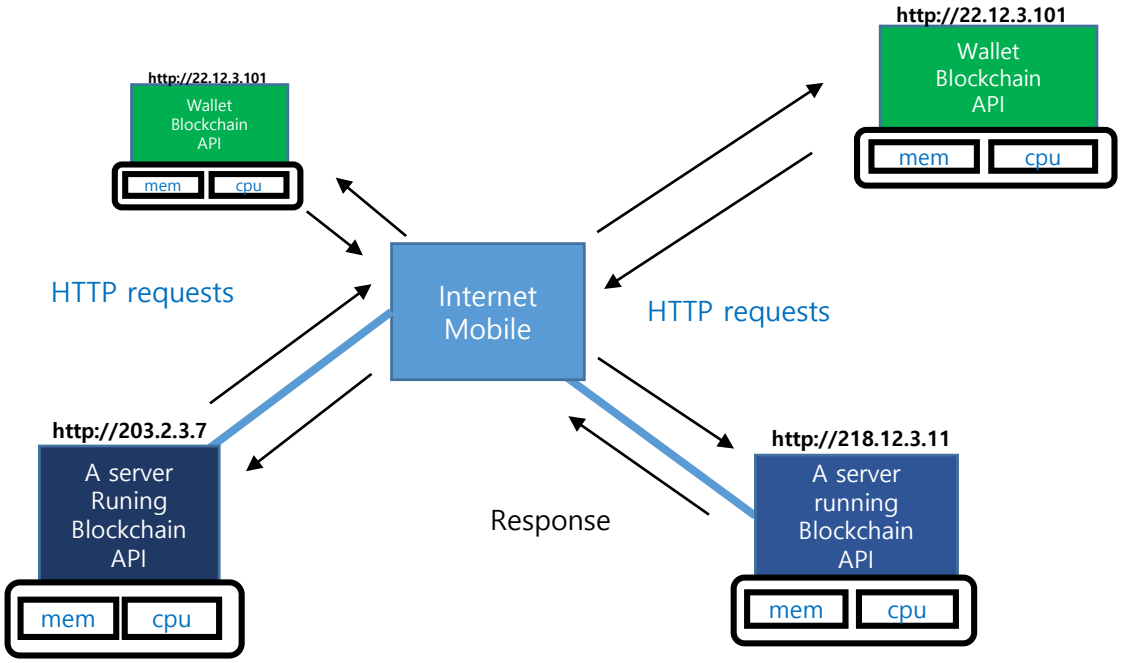
- 데이터 : 최초 블록 + 일반 블록, 1Mbyte 블록이 10분마다 생성
- 프로토콜 : 합의, 블록 헤더, 난이도 조절 등...
- 채굴 : 가장 긴 체인을 가져 와서 그 안에 있는 모든 거래를 **확인**하고 마이닝풀에서 트랜잭션을 가져와 블록을 형성하고, **좋은 해시를 찾을 때까지 SHA를 반복적으로 실행하고**, 증명을 블록 헤더에 넣고, 증명 된 블록을 가장 긴 곳에 연결 체인, 그리고 가능한 공표

프로그램 집합체

- **C++, Python, Go, Java, Flask, http**
- **다운로드 및 실행으로 블록체인 서버를 구축할 수 있음.**

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

the blockchain internet



Bitcoin Blockchain Verticals

- Decentralized
- Public
- Immutability
- Trust
- Minting coins
- Anonymity

Cryptoeconomic Design

- Master designer
  - Minting schedule, TPS, Incentive Mechanism, Master plan
- Developers
  - Maintain the system
  - SW upgrades
- Users
  - Payments, assets
- Miners

Unexpected but there are

- Exchanges
- Investors
- Crowd funding: ICO

Multiple perspectives on cryptos

- Digital currency
  - Medium of exchange, storage of value, stability of value
- Digital assets
- Commodities
- Payment methods

WEF's Perspective on Cryptocurrency

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

- May 2015 WEF Reports,
  - "By 2023, a nation will appear, collecting tax in cryptocurrencies"
  - "By 2027, 10% of World GDP will be stored in cryptocurrency"

- Cryptocurrencies Market Cap 2018 = 216B USD (0.25% of WGDP)

ICO and Ethereum

ICO

- Startups in the blockchain world use Initial Coin Offering (ICO) as a tool to raise funds.
- Reference: https://icowatchlist.com/education/history-and-evolution-of-icos

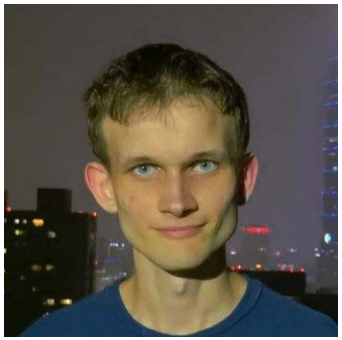
ICO, how did it get started?

- "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

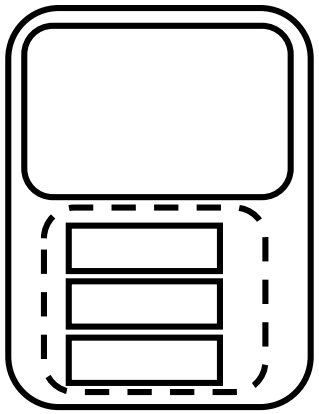
- Ethereum ICO in 2014, raising coins worth millions of dollars.



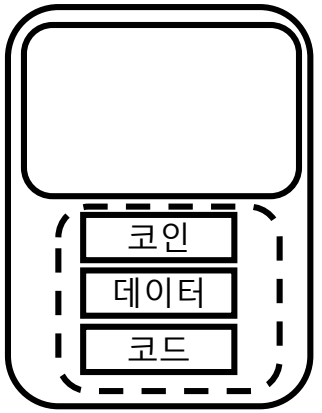
Ethereum

- 블록체인에 코인뿐만이 아니라 Smart Contract기능을 부여
- Ethereum 블록체인 Layer를 코인거래와 분리
- 나머지 블록체인 부분을 Platform화 하여, 누구나 쉽게 사용할 수 있도록 개방하고 제공함.
- Application부분을, 코인거래 뿐아니라, 데이터도 넣을 수 있고, 보다 복잡한 거래도 코딩할 수 있도록, 분리함.

Bitcoin 블록
은 코인거래만
담는 반면



Ethereum블록,
컴퓨터코드도 넣고
데이터도 넣자



Ethereum 블록에 들어간 판문점 선언문

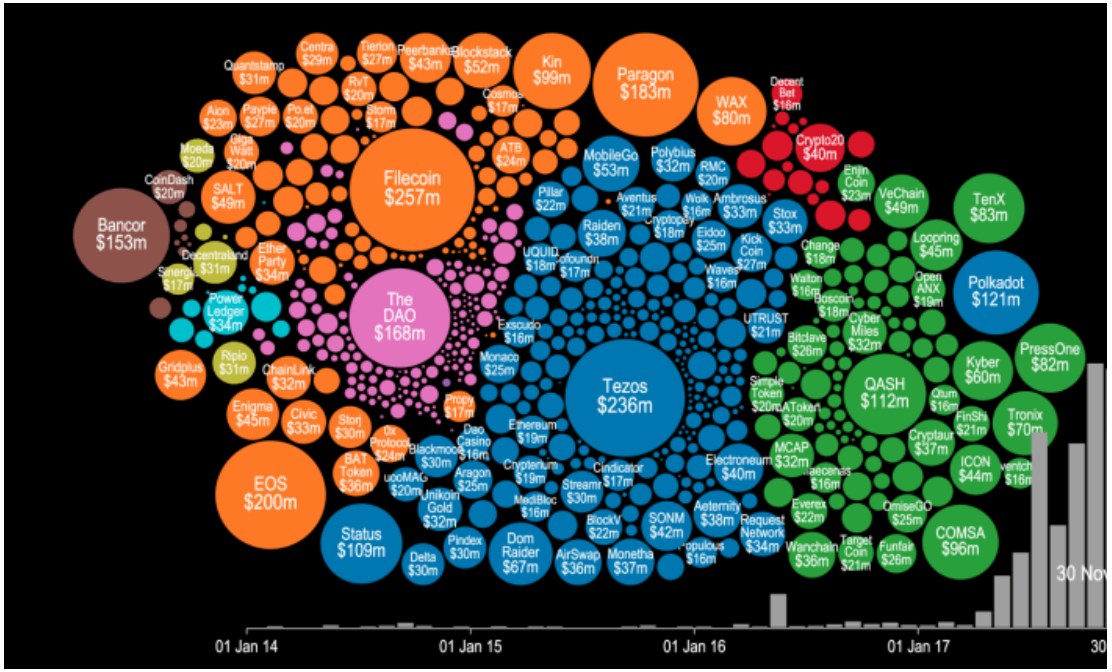
Overview | Comments

Transaction Information — Tools & Utilities

TxHash:	0xe4ee15d3f63db8464a649e3237ed83e930f9b3e40e842537a626
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>

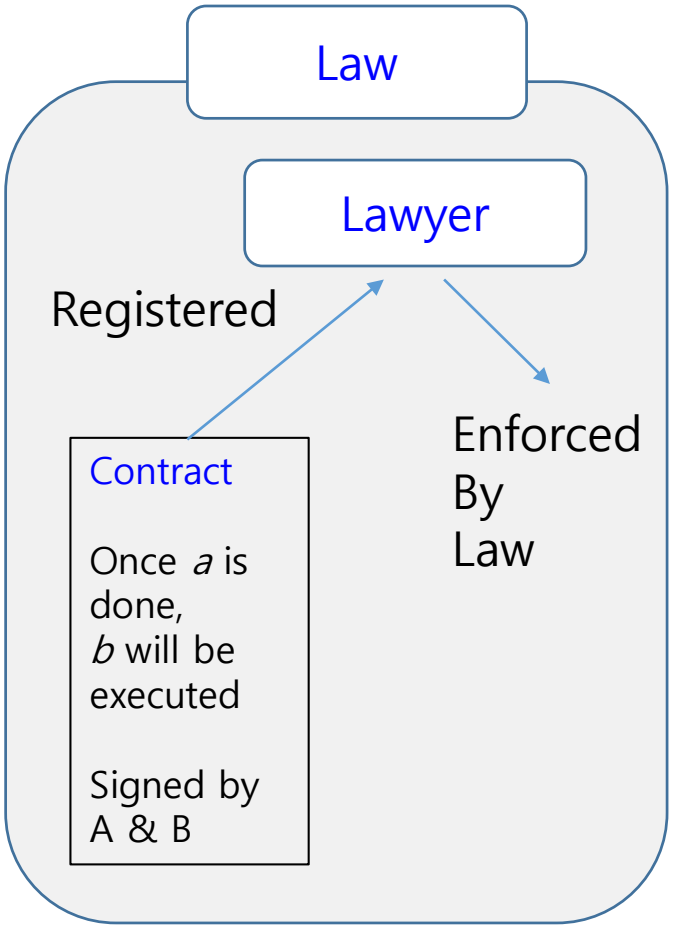
2018.04.28

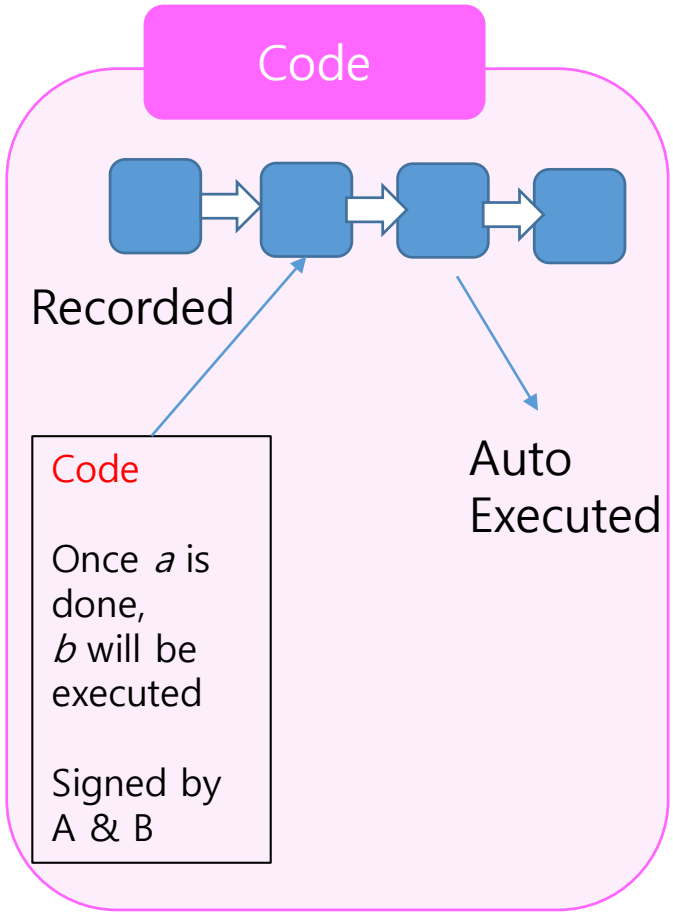
Smart Contracts



- Without lawyers, insurers, administrators, one can expect to open up a nice business relation with anyone in the internet.
- Computer codes -- smart contracts -- can be used to make contracts and expect auto execution of contractual terms.
- Programming for SCs is relatively easy.
- Thousands of ICOs have been made.

Legal Contracts vs. Smart Contracts





Sharing Economy

Insurance

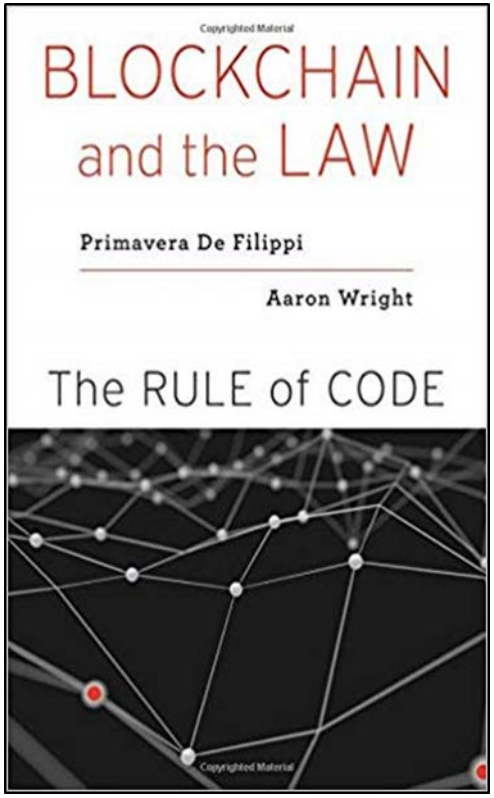
Voting

MediChain

Real Estate

Law

Lex Cryptographia



In this Article, we explore the benefits and drawbacks of this emerging decentralized technology and argue that its widespread deployment will lead to expansion of a new subset of law, which we term Lex Cryptographia*: rules administered through self-executing smart contracts and decentralized (autonomous) organizations. As blockchain technology becomes widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, could lose the ability to control and shape the activities of disparate people through existing means. As a result, there will be an increasing need to focus on how to regulate blockchain technology and how to shape the creation and deployment of these emerging decentralized organizations in ways that have yet to be explored under current legal theory.*

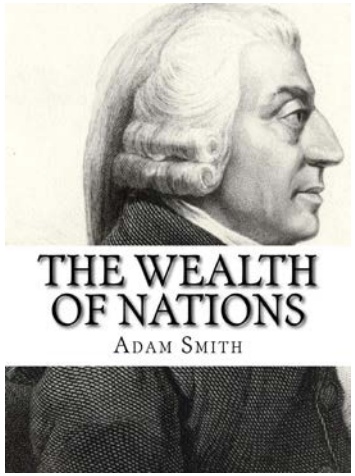
---

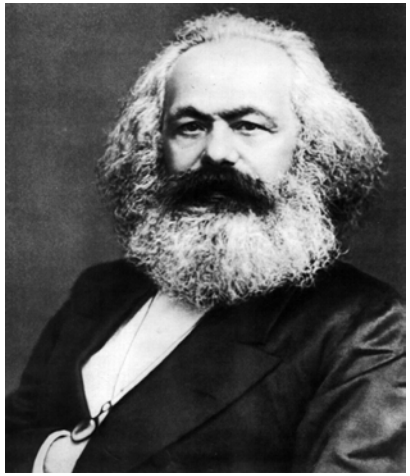
* Assistant Clinical Professor of Law and Director of the Cardozo Tech Startup Clinic, Benjamin N. Cardozo School of Law, Yeshiva University; Founder/Director of the Cryptocurrency Research Group.
** Research fellow at the Berkman Center for Internet and Society at Harvard Law School and associate researcher at the CERSA / CNRS / Université Paris II.

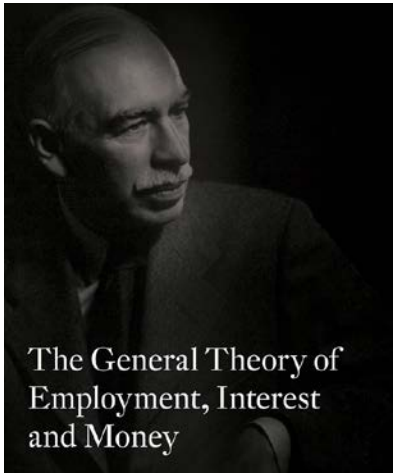
Bitcoin blockchains

- Human network.
- Computer network.
- Knowledge is wealth.
- Increased wealth is increased knowledge.
- Economy grows though learning.
- Money flows.
- It signals which area needs more work.
- Data and ideas are resource.

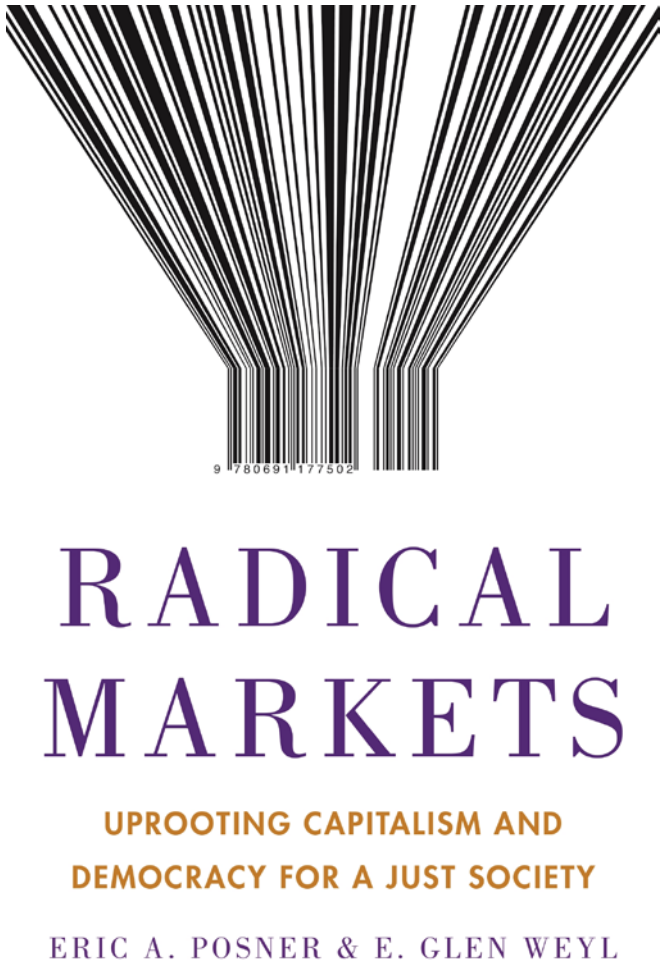
Flows of philosophy







New Capitalism?



Andrew Yang vs. D. Trump

암호화폐/블록체인 질문목록

1. 블록체인이란 게 도대체 뭔가요?
2. 세계 최초의 암호화폐는 무엇인가요?
3. 암호화폐와 블록체인의 관계는 어떻게 되나요?
4. 암호화폐와 우리가 평상시 쓰는 통화와의 차이점은 무엇인가요?
5. 암호화폐는 어떤 배경에서 탄생하게 되었나요?
6. 탄생한지 9년 된 암호화폐와 블록체인은 현재 어떤 상태입니까? 전세계적인 암호화폐 개발 동향을 알려 주십시오.
7. Ethereum이라는 암호화폐의 특징은 어떤 것인가요?
8. Smart Contract라는 것은 어떤 것 인가요?
9. 블록체인이 쓰일 수 있는 분야가 매우 많다고 하는데 예를 좀 들어 주시겠습니까?
10. Smart Contract의 응용분야는 어떤 것들이 있나요?

암호화폐/블록체인 질문목록

11. 전세계 젊은이들이 블록체인의 가능성에 집중하고 있다는데, 그이유는 무엇 인가요?
12. 블록체인은 과연 미래 기술인가요? 미래 기술이라고 한다면 어떤 이유를 들 수 있을까요?
13. 4차 산업혁명과 블록체인은 어떤 관계가 있나요?
14. 대한민국의 블록체인 산업의 현재 상태는 어떤 것입니까?
15. Initial Coin Offering이 대한민국에서 금지된 상태인데, ICO가 무엇이고, 금지된 배경은 무었입니까?
16. 대한민국 정부가 블록체인 및 암호화폐를 규제하고 있는데, 정부의 입장은 무었이라고 생각합니까?
17. 인공지능과 블록체인이 미래 핵심기술이라는데, 그 이유는 무엇이라고 생각하시는가요?
18. 대한민국이 블록체인을 육성 발전시켜야 할 방향은 어떤 것이라고 생각합니까?
19. 블록체인으로 젊은이들이 창업을 하려고 하면 어떤 것들을 조심해야 할 까요?

How to participate

- We have a number of national projects.
- Sensor intelligence and blockchain economy

- Visit home page https://infonet.gist.ac.kr/

- Blockchain 강의, 소스코드, 동영상 등
- https://infonet.gist.ac.kr/?page_id=7619

Concluding Remarks

- Bitcoin is a phenomenon of breath!

- Contact: heungno@gist.ac.kr
- Facebook ID: Heung-No Lee

Home Work

- 다음 중에서 Lex Cryptographia를 제일 적합하게 설명하는 것은?
  1. 새로운 법
  2. 전통법의 강화
  3. 코드가 법
  4. 공유경제

- 다음을 참과 거짓으로 판별 하시오.

1. Ethereum은 블록체인을 사용하지 않는다.
2. Bitcoin은 코드를 저장 하지도 실행 하지도 않는다.
3. Legal 계약서와 스마트계약서의 가장 큰 차이점은 변호사가 블록체인으로 교체된 것이다.
4. 2019년 11월 4일 시점에서 Bitcoin의 market cap은 World GDP의 1%를 넘겼다.
5. 2019년 11월 4일 Bitcoin 네트워크의 블록 당 Bitcoin 발행 량은 12.5개다.
6. Bitcoin네트워크의 평균 블록생성속도는 10분에 1블록이다.
7. Denationalization of money의 저자는 케인즈이다.
8. 아담스미스는 "국가가 계획경제를 하면 국민은 돈의 노예로 전락한다" 고 말했다.