블록체인으로 여는 미래

2018. 4. 19 (목)
숭실대학교 형남공학관

이흥노 교수
GIST

박창기 대표
Govern Tech

김형식 교수
성균관대학교

김형중 교수
고려대학교

이두원 대표
(주)아니스트

김용대 교수
KAIST

Introduction to Bitcoin and Blockchain

Heung-No Lee

April 19th 2018

블록체인으로 여는 미래

2018. 4. 19 (목)
숭실대학교 형남공학관

이흥노 교수
GIST

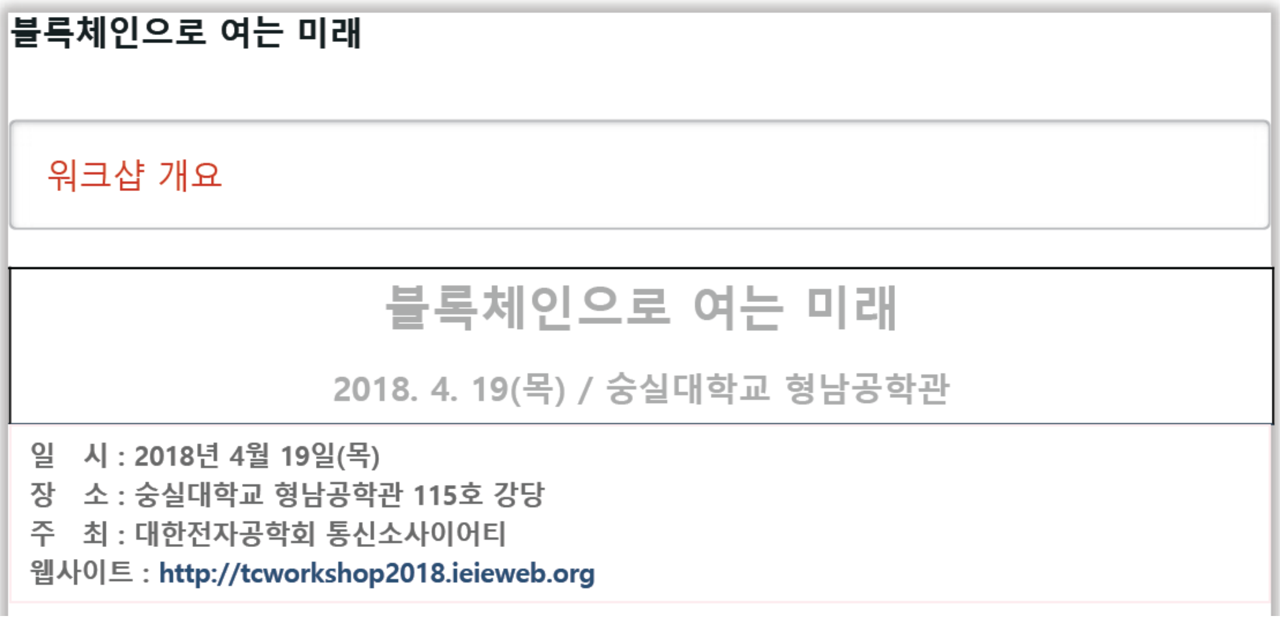
박창기 대표
Govern Tech

김형식 교수
성균관대학교

김형중 교수
고려대학교

이두원 대표
(주)아니스트

김용대 교수
KAIST



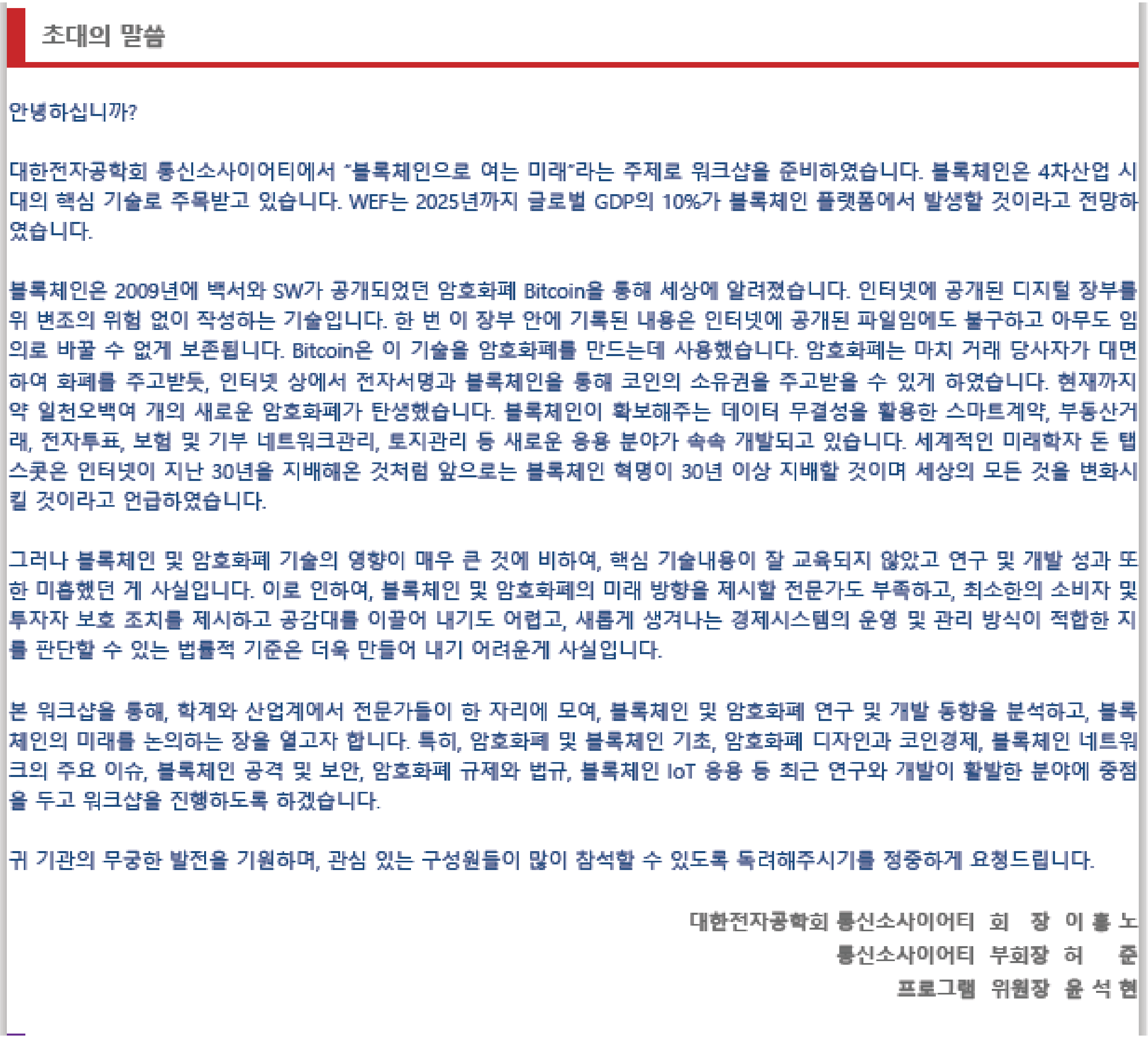
블록체인으로 여는 미래

워크샵 개요

블록체인으로 여는 미래

2018. 4. 19(목) / 숭실대학교 형남공학관

일　시 : 2018년 4월 19일(목)
장　소 : 숭실대학교 형남공학관 115호 강당
주　최 : 대한전자공학회 통신소사이어티
웹사이트 : http://tcworkshop2018.ieieweb.org



초대의 말씀

안녕하십니까?

대한전자공학회 통신소사이어티에서 “블록체인으로 여는 미래”라는 주제로 워크샵을 준비하였습니다. 블록체인은 4차산업 시대의 핵심 기술로 주목받고 있습니다. WEF는 2025년까지 글로벌 GDP의 10%가 블록체인 플랫폼에서 발생할 것이라고 전망하였습니다.

블록체인은 2009년에 백서와 SW가 공개되었던 암호화폐 Bitcoin을 통해 세상에 알려졌습니다. 인터넷에 공개된 디지털 장부를 위 변조의 위험 없이 작성하는 기술입니다. 한 번 이 장부 안에 기록된 내용은 인터넷에 공개된 파일임에도 불구하고 아무도 임의로 바꿀 수 없게 보존됩니다. Bitcoin은 이 기술을 암호화폐를 만드는데 사용했습니다. 암호화폐는 마치 거래 당사자가 대면하여 화폐를 주고받듯, 인터넷 상에서 전자서명과 블록체인을 통해 코인의 소유권을 주고받을 수 있게 하였습니다. 현재까지 약 일천오백여 개의 새로운 암호화폐가 탄생했습니다. 블록체인이 확보해주는 데이터 무결성을 활용한 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.

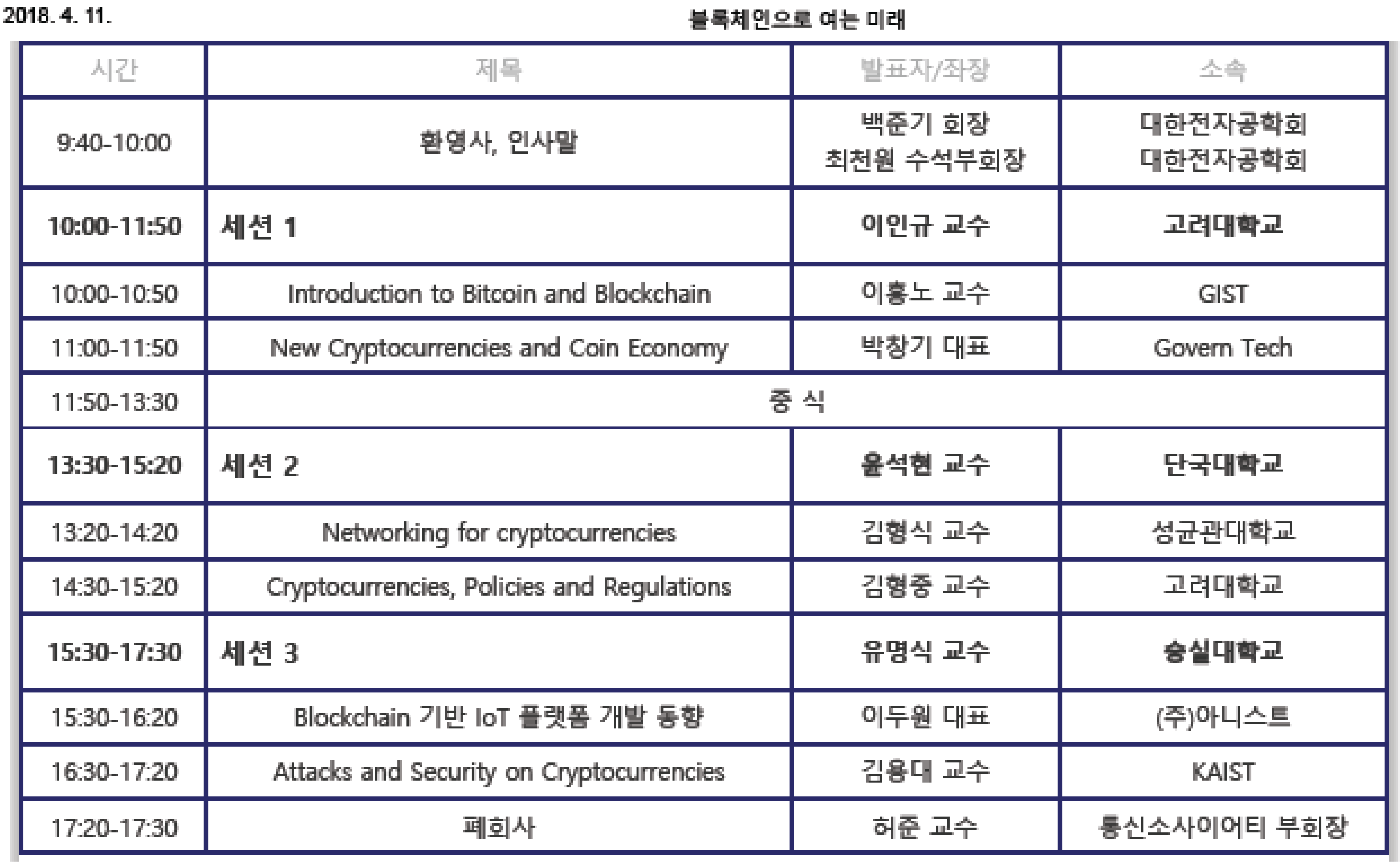
그러나 블록체인 및 암호화폐 기술의 영향이 매우 큰 것에 비하여, 핵심 기술내용이 잘 교육되지 않았고 연구 및 개발 성과 또한 미흡했던 게 사실입니다. 이로 인하여, 블록체인 및 암호화폐의 미래 방향을 제시할 전문가도 부족하고, 최소한의 소비자 및 투자자 보호 조치를 제시하고 공감대를 이끌어 내기도 어렵고, 새롭게 생겨나는 경제시스템의 운영 및 관리 방식이 적합한 지를 판단할 수 있는 법률적 기준은 더욱 만들어 내기 어려운게 사실입니다.

본 워크샵을 통해, 학계와 산업계에서 전문가들이 한 자리에 모여, 블록체인 및 암호화폐 연구 및 개발 동향을 분석하고, 블록체인의 미래를 논의하는 장을 열고자 합니다. 특히, 암호화폐 및 블록체인 기초, 암호화폐 디자인과 코인경제, 블록체인 네트워크의 주요 이슈, 블록체인 공격 및 보안, 암호화폐 규제와 법규, 블록체인 IoT 응용 등 최근 연구와 개발이 활발한 분야에 중점을 두고 워크샵을 진행하도록 하겠습니다.

귀 기관의 무궁한 발전을 기원하며, 관심 있는 구성원들이 많이 참석할 수 있도록 독려해주시기를 정중하게 요청드립니다.

대한전자공학회 통신소사이어티 회 장 이 흥 노
통신소사이어티 부회장 허 준
프로그램 위원장 윤 석 현

Program



2018. 4. 11.

블록체인으로 여는 미래

시간	제목	발표자/좌장	소속
9:40-10:00	환영사, 인사말	백준기 회장 최천원 수석부회장	대한전자공학회 대한전자공학회
10:00-11:50	**세션 1**	**이인규 교수**	**고려대학교**
10:00-10:50	Introduction to Bitcoin and Blockchain	이흥노 교수	GIST
11:00-11:50	New Cryptocurrencies and Coin Economy	박창기 대표	Govern Tech
11:50-13:30	중 식		
13:30-15:20	**세션 2**	**윤석현 교수**	**단국대학교**
13:20-14:20	Networking for cryptocurrencies	김형식 교수	성균관대학교
14:30-15:20	Cryptocurrencies, Policies and Regulations	김형중 교수	고려대학교
15:30-17:30	**세션 3**	**유명식 교수**	**숭실대학교**
15:30-16:20	Blockchain 기반 IoT 플랫폼 개발 동향	이두원 대표	(주)아니스트
16:30-17:20	Attacks and Security on Cryptocurrencies	김용대 교수	KAIST
17:20-17:30	폐회사	허준 교수	통신소사이어티 부회장

금융공학과 블록체인

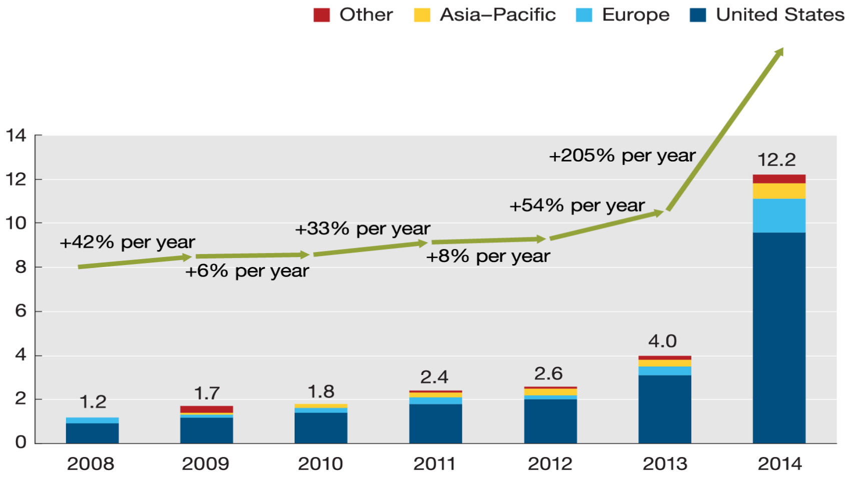
왜 금융공학인가?

우리가 할 수 있나?

어디로 투자가 되고 있는지 봐라!

The level of venture-capital investment in financial technology has recently accelerated.

Global investment in financial technology,
$ billion

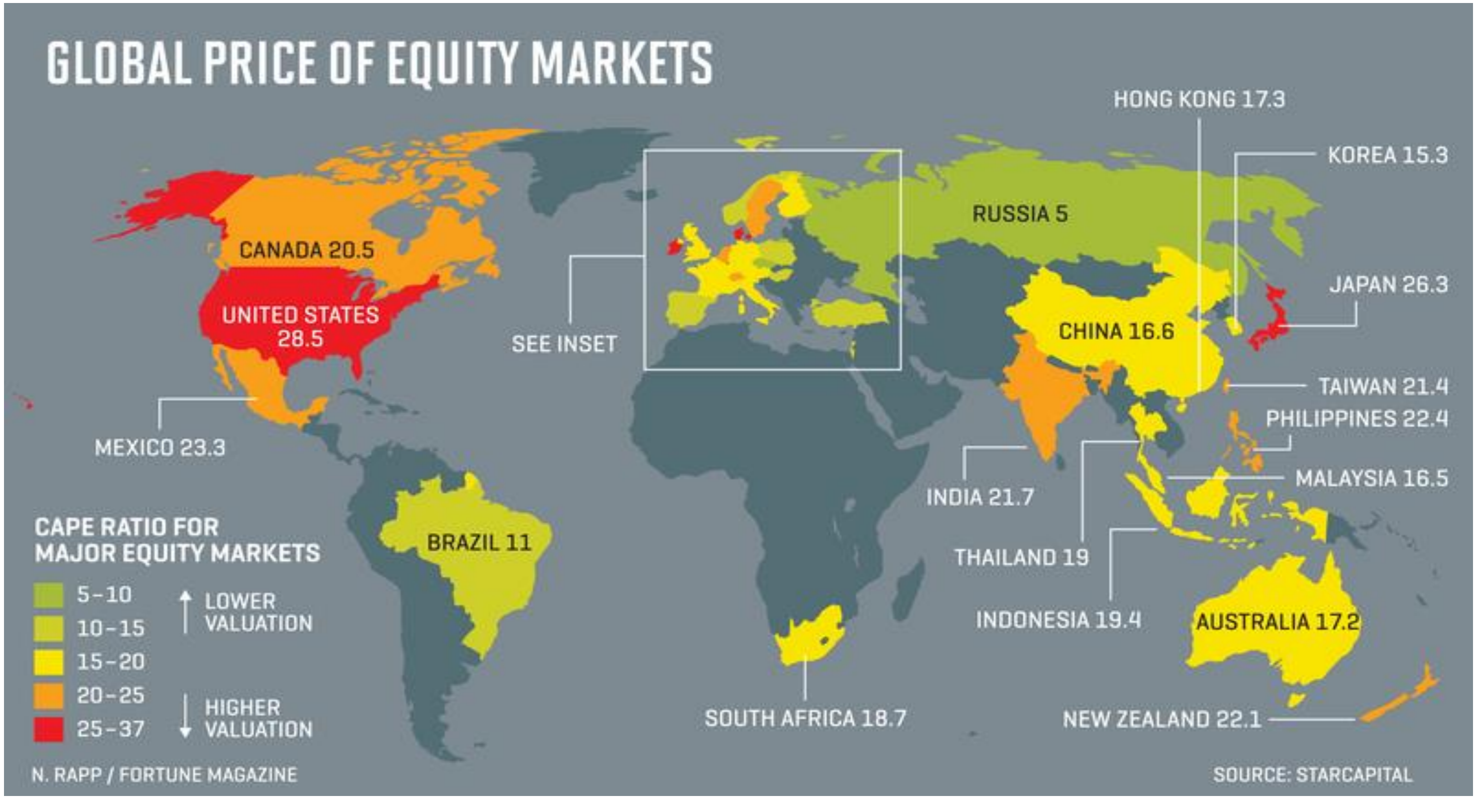


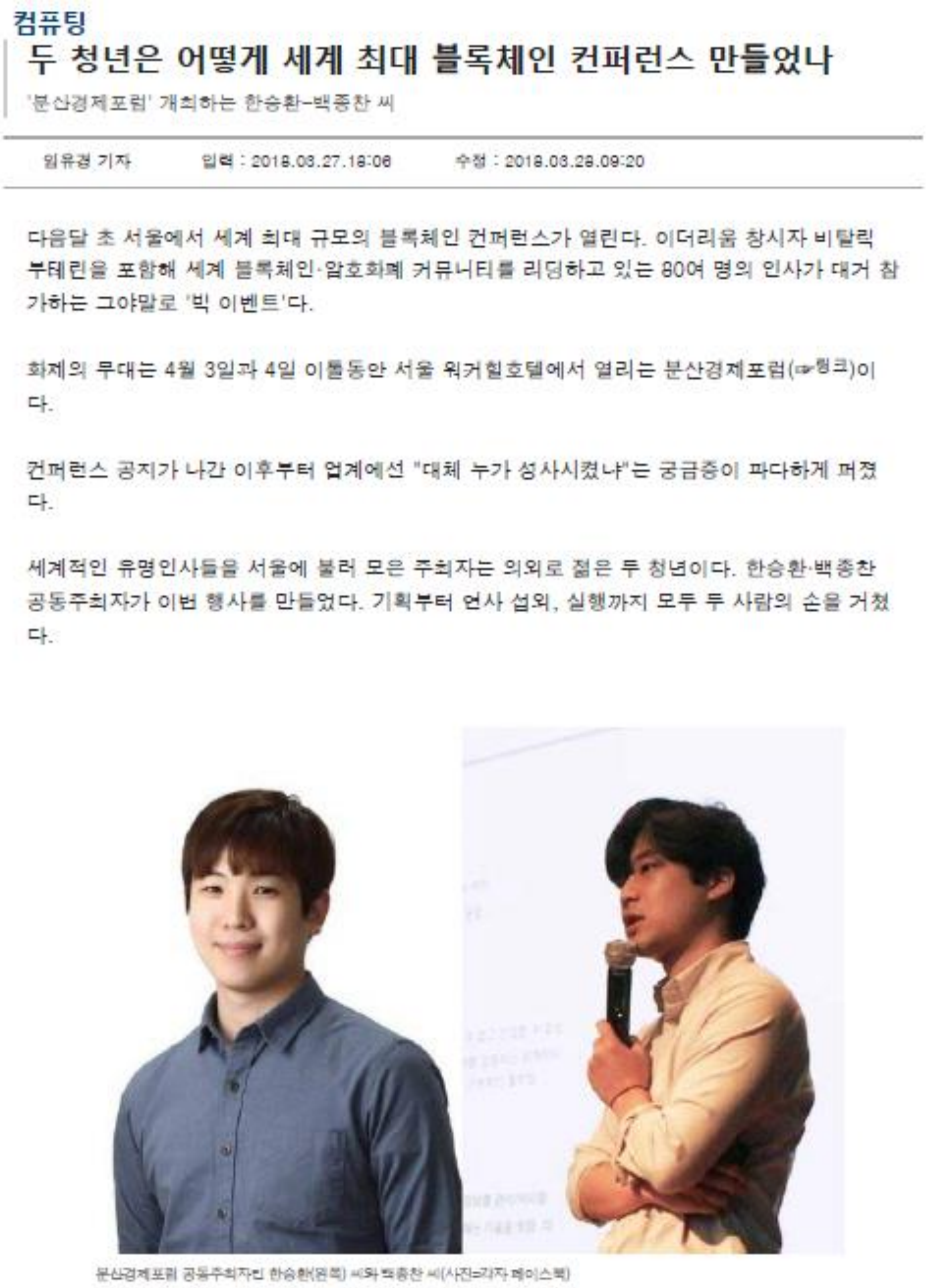
Source: CB Insights; analysis of data provided by McKinsey Panorama (a McKinsey Solution)

McKinsey&Company

This Map Will Show You the World's Most Expensive Stock Markets
FORTUNE, 2017/08/18

Cyclically Adjusted Price/Earnings ratio





컴퓨팅

두 청년은 어떻게 세계 최대 블록체인 컨퍼런스 만들었나

'분산경제포럼' 개최하는 한승환-백종찬 씨

임유경 기자　　입력 : 2018.03.27.18:06　　수정 : 2018.03.28.09:20

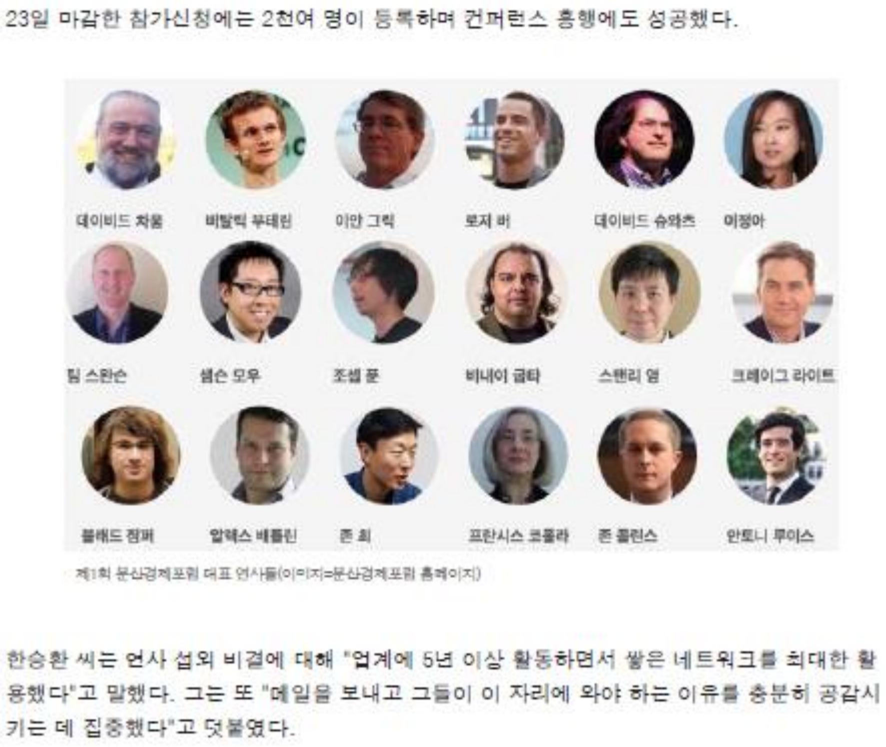
다음달 초 서울에서 세계 최대 규모의 블록체인 컨퍼런스가 열린다. 이더리움 창시자 비탈릭 부테린을 포함해 세계 블록체인·암호화폐 커뮤니티를 리딩하고 있는 80여 명의 인사가 대거 참가하는 그야말로 '빅 이벤트'다.

화제의 무대는 4월 3일과 4일 이틀동안 서울 워커힐호텔에서 열리는 분산경제포럼(☞링크)이다.

컨퍼런스 공지가 나간 이후부터 업계에선 "대체 누가 성사시켰냐"는 궁금증이 파다하게 퍼졌다.

세계적인 유명인사들을 서울에 불러 모은 주최자는 의외로 젊은 두 청년이다. 한승환·백종찬 공동주최자가 이번 행사를 만들었다. 기획부터 연사 섭외, 실행까지 모두 두 사람의 손을 거쳤다.

분산경제포럼 공동주최자인 한승환(왼쪽) 씨와 백종찬 씨(사진=각자 페이스북)



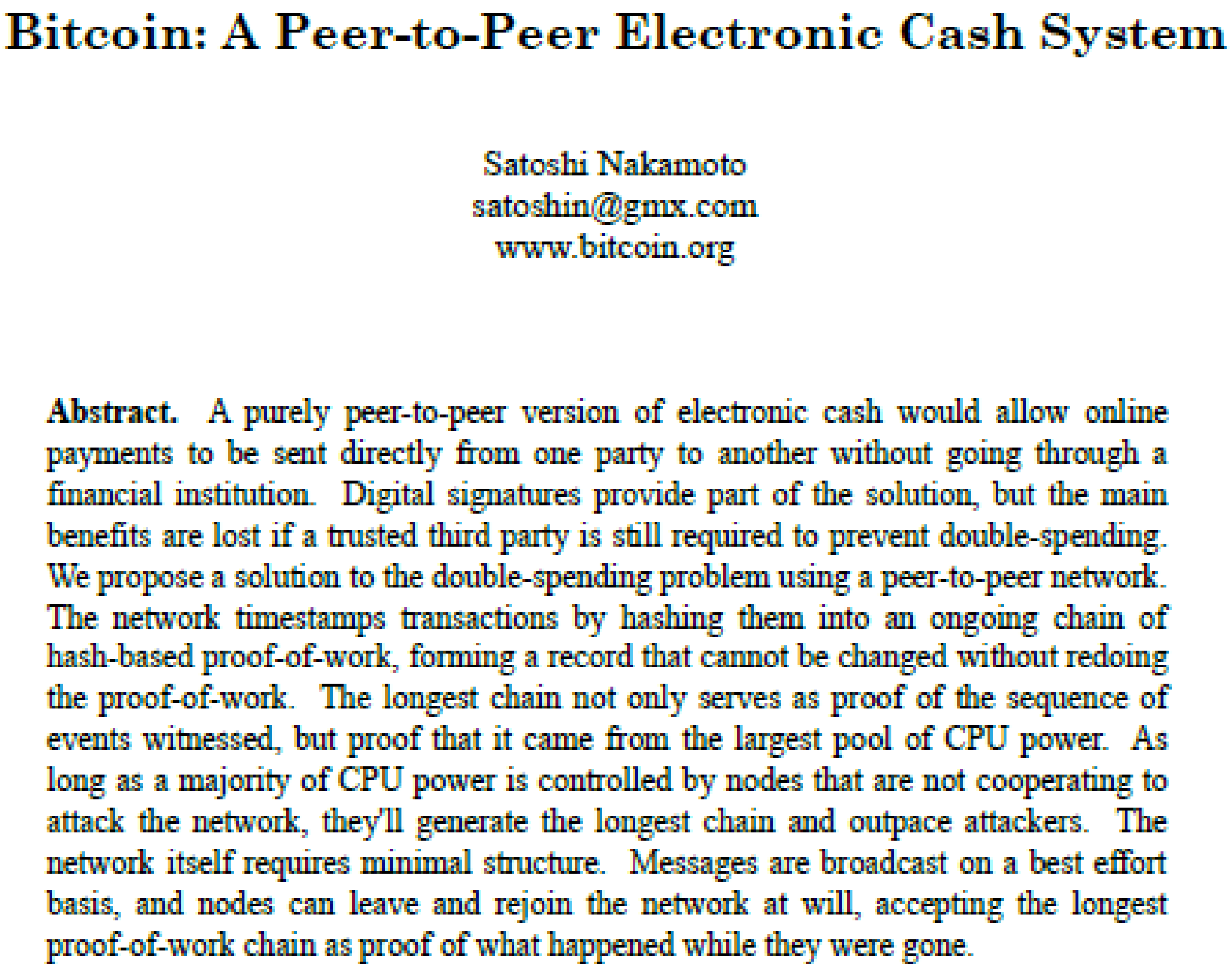
23일 마감한 참가신청에는 2천여 명이 등록하며 컨퍼런스 흥행에도 성공했다.

제1회 분산경제포럼 대표 연사들(이미지=분산경제포럼 홈페이지)

한승환 씨는 연사 섭외 비결에 대해 "업계에 5년 이상 활동하면서 쌓은 네트워크를 최대한 활용했다"고 말했다. 그는 또 "메일을 보내고 그들이 이 자리에 와야 하는 이유를 충분히 공감시키는 데 집중했다"고 덧붙였다.

Bitcoin?

The first paper



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.

Satoshi Nakamoto

- Anonymous person or group of people who designed the original Bitcoin and goes by the pseudonym Satoshi Nakamoto.
- Released the ground-breaking White Paper “Bitcoin: A Peer-to-Peer Electronic Cash System” in 2008.
- The smaller unit of Bitcoin, 1/100,000,000 has been named “Satoshi” in homage.
- Likely has a lot of Bitcoin, maybe 1,624,250 Bitcoin, or close to a $1 Billion USD.

Bitcoin

Bitcoin is digital currency!

Currency works based on trust. You have the currency, then you can exchange it to get goods and services.

- **Today, money is simply numbers in our bank account. When a number is lowered in my account, the same amount of number appears in the other account when I spend them.**

Value of a currency lies in a government who issues it and enforces wrong usages.

- **Making counterfeits are caught.**
- **Fraud is punished.**

Currency with high demands is valued high in the market.

Bitcoin has gained the position of currency in the market without the support of any government.
Very high market value based on high demand has been created for Bitcoin.
This is a fact.
It gives a reason why Bitcoin is important for us to study.
It is the first digital currency made it to such a level.
It is an important invention of the humanity.

Brief history on bitcoin markets

Source https://thenextweb.com/insider/2015/03/29/a-brief-history-of-bitcoin-and-where-its-going-next/

~2010 : M. value created, Pizza Day

October 2009

- Bitcoin receives an equivalent value in traditional currencies. The New Liberty Standard established the value of a Bitcoin at $1 = 1,309 BTC. The equation was derived so as to include the cost of electricity to run the computer that created the Bitcoins in the first place.

February 2010

- The world’s first Bitcoin market is established by the now defunct dwdollar.

May 2010

- A programmer living in Florida named Laslo Hanyecz sends 10,000BTC to a volunteer in England, who spent about $25 to order Hanyecz a pizza from Papa John’s. Today that pizza is valued at £1,961,034 and stands as a major milestone in Bitcoin’s history.

November 2010

- Bitcoin reaches $1 million. Based on the number of Bitcoins in circulation at the time, the valuation leads to a surge in Bitcoin value to $0.50/BTC.

2013: Regulation started, “Bitcoin is money”

February 2011

- Bitcoin reaches parity with the US dollar for the first time. By June each Bitcoin is worth $31 giving the currency a market cap of $206 million.

March 2013

- The US Financial Crimes Enforcement Network (FINCEN) issues some of the world’s first bitcoin regulation in the form of a guidance report for persons administering, exchanging or using virtual currency. This marked the beginning of an ongoing debate on how best to regulate bitcoin.

March 2013

- Bitcoin market capitalization reaches $1bn.

August 2013

- **Federal Judge Mazzant** claims: “It is clear that Bitcoin can be used as money” and “It can be used to purchase goods or services” in a case against Trendon Shavers, the so-called ‘Bernie Madoff of bitcoin’. Bloomberg begins testing bitcoin data on its terminal. Although alternative tickers exist, endorsement from Bloomberg gives bitcoin more institutional legitimacy.

December 2013

- China’s central bank bars financial institutions from handling bitcoin transactions. This ban was issued after the People’s Bank of China said bitcoin is not a currency with “real meaning” and does not have the same legal status as fiat currency. The ban reflects the risk bitcoin poses to China’s capital controls and financial stability. Today China remains the world’s biggest bitcoin trader, with 80% of global bitcoin transactions being processed in China.

2014 : Taxation, Regulations, Funds

January 2014

- Bitcoin custodians Elliptic launch the world's first insured bitcoin storage service for institutional clients. All deposits are comprehensively insured by a Fortune 100 insurer and held in full reserve. This means Elliptic never re-invests client assets; instead they secure them in deep cold storage. Overstock.com becomes the first major online retailer to embrace bitcoin, accepting payments in the US. Overstock was the first in what is now an expeditiously growing list of large businesses that accept bitcoin.

February 2014

- HMRC classifies bitcoin as assets or private money, meaning that no VAT will be charged on the mining or exchange of bitcoin. This is important as it is the world's first and most progressive treatment of bitcoin, positioning the UK government as the most forward thinking and comprehensive with regard to bitcoin taxation.

July 2014

- The 'Bit Licence' edges towards reality as the New York State Department of Financial Services releases the first draft of the agency's proposed rules for regulating virtual currencies. The European Banking Authority publishes its opinion on 'virtual currencies'. Their analytical report recommends that EU legislators consider declaring virtual currency exchanges as 'obliged entities' must comply with anti-money laundering (AML) and counter-terrorist financing requirements.
- The EBA report is important as it acts as a catalyst to launch bitcoin into the financial mainstream by highlighting the fact that virtual currencies require a regulatory approach to strive for an international coordination to achieve a successful regulatory regime.
- Also that month GABI (Global Advisors Bitcoin Investment Fund) launches the world's first regulated Bitcoin Investment fund. This is important to the bitcoin ecosystem as the launch of this investment vehicle adds further legitimacy to bitcoin in addition to allowing regulated investors a way to invest in bitcoin.

2015: Derivatives, Assets, Payments

August 2014

- The Chancellor of the Exchequer, George Osborne, demonstrates his and HM Treasury's positive outlook on bitcoin when he purchases £20 worth of bitcoin and announces HM Treasury's Call for Information on digital currencies, offering digital currency businesses the chance to comment on the risks and benefits and potentially influence future government policy.

October 2014

- TeraExchange announces that the first bitcoin derivative transaction was executed on a regulated exchange, adding a new hedging instrument to bitcoin and instilling credibility and institutional confidence in the entire bitcoin community.

December 2014

- Tech giant Microsoft begins accepting bitcoin payments.

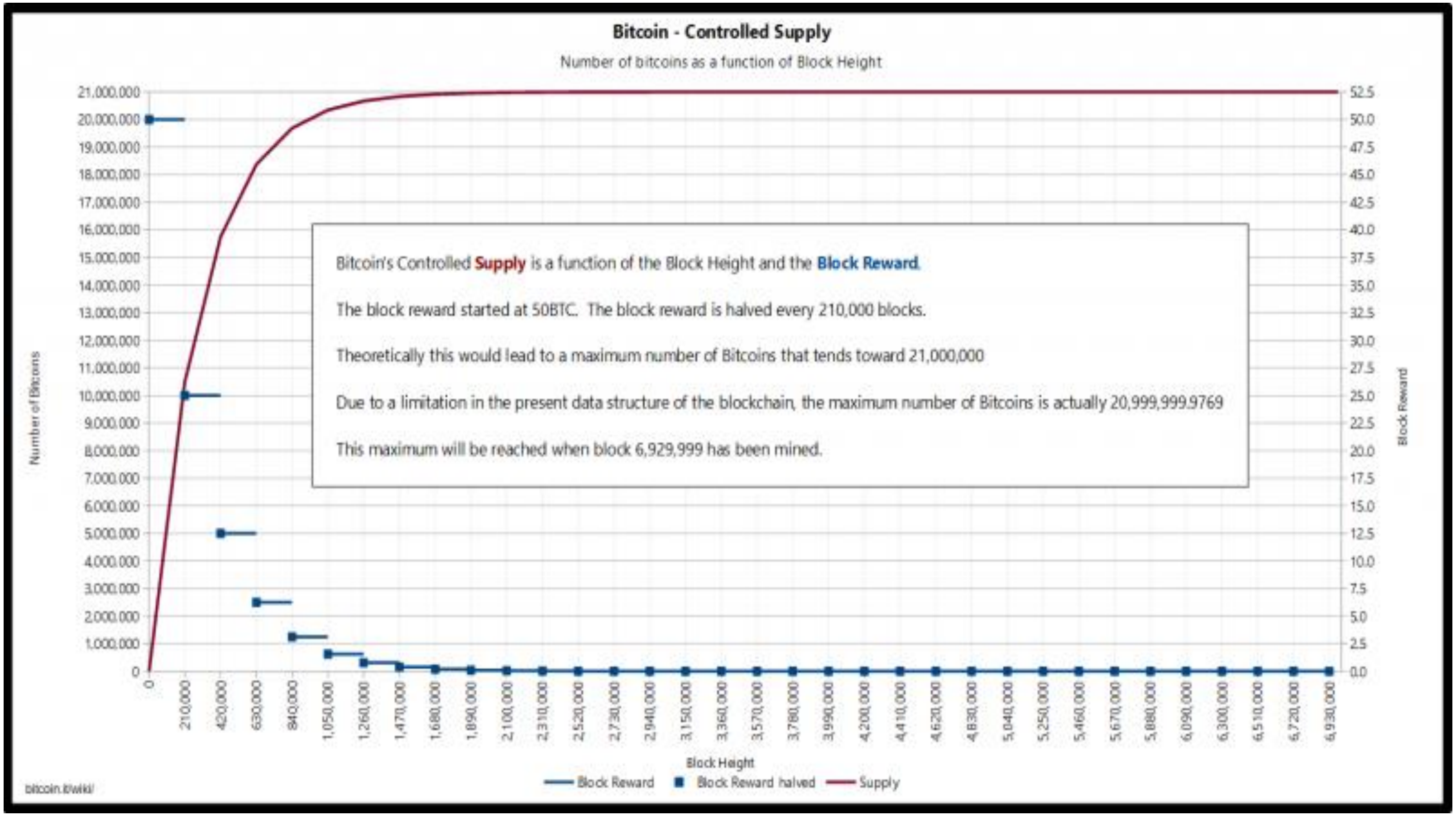
January 2015

- The New York Stock Exchange is a minority investor in Coinbase's $75M funding round. The NYSE aims to tap into the new asset class by bringing transparency, security and confidence to bitcoin.

March 2015

- The results of the UK Treasury's call for information on digital currency are announced.

Bitcoin Issuance Schedule



Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height

Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

Seigniorage Effect

- Seigniorage is the difference between the value of money and the cost to produce it — in other words, the economic cost of producing a currency within a given economy or country. If the seigniorage is positive, then the government will make an economic profit

Seigniorage and the Federal Reserve

- While the basic principle behind seigniorage suggests that a country can profit from the production of new bills, there can be other factors affecting the entire transaction. Within the United States, if the Federal Reserve agrees to increase the number of dollars available within the U.S. economy, it will purchase a Treasury Bill in exchange for permitting the production of more dollars. While the government may appear to profit when the cost of production is lower than the face value of the bills, it is important to note that Treasury Bills require interest payments to the Federal Reserve in addition to the original investment placed when the Treasury Bill was purchased.

https://www.investopedia.com/terms/s/seigniorage.asp

Bitcoin

Bitcoin protocol runs on a P2P network.
All computers in the network, cooperates and verifies the coin transaction.

It is designed to keep out faulty transactions such unproven ownership and double spending transactions.

This protocol enables, a digital message such as "A gives B a single coin" works as an in-person transfer of money if the message is verified, recorded and kept unaltered.

Without the involvement of a third party such as banks and middle man,
anybody can open up a transaction with anyone in the internet.

How can such an invention be possible?

The answer was in fact very simple.

Namely, transactions are recorded in a book with time stamped, the content of the book is kept in an immutable way that can not be altered, and the book is published in the internet so that anybody can open it up and refer to it.

Bitcoin and Blockchain

Each transaction is verified, verified transactions are recorded in the ledger, every record in the ledger is kept in an immutable way that the content cannot be altered unnoticed.

There are three parts to this:
1st Verification of ownership
2nd Double spending free
3rd Verified transactions are scribed into the blockchain (a digital file whose contents cannot be altered once recorded)

How?

- As the ledger is openly published and shared in the p2p network of computers, any transaction can be verified for valid ownership and free of double spending problem.
- Blockchain means a new cryptographic technology which is to resolve the issue of how to determine and maintain the original content of the digital ledger unaltered once recorded.

Blockchain is believed to have many usages beyond currency.

Blockchain

A file of size 1Mbyte is called a block.
Written inside this file are the transactions with content and time.
A series of such files connected in the order of time is called Blockchain.

Namely, a blockchain is a digital ledger with many bound pages.

Time 1: A gives B two coins. A's Sign.
Time 2: B gives C one coin. B's Sign.
Time 3: C gives D 0.5 coin. C's Sign.

As given above, coin transactions are recorded with time.
Taking a look inside this ledger, one can always verify who owns how much coin, how much coin has been transferred from whom to whom.
This ledger is openly published in the internet and anybody can download it.
Opening up the ledger, anybody can see how much money is belong to a person.

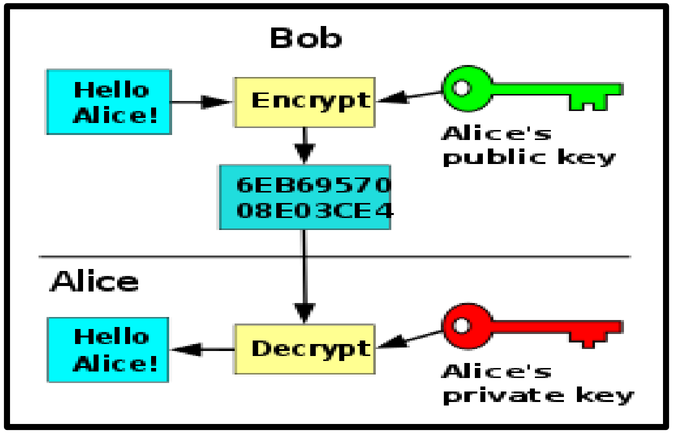
But please make no mistake.
This ledger however uses cryptographic hash values.
The coin ownerships are given to cryptographically made addresses.
Only the person who has the private key to the public address can claim the ownership of the coin.

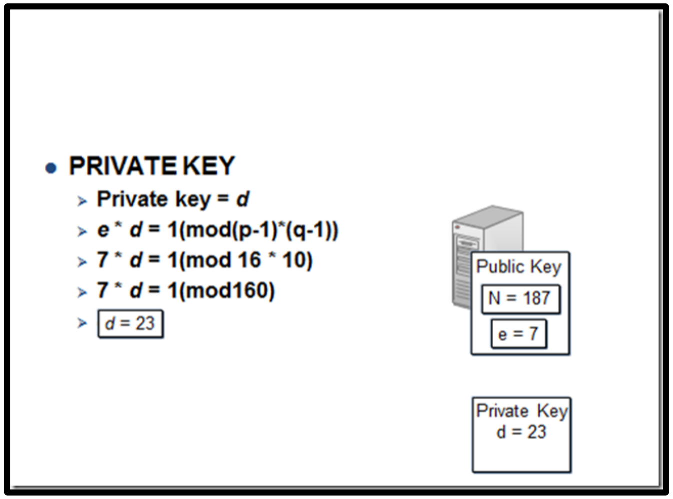
How to do Digital Signature (RSA example)

- A pair of *private and public key generated to each individual is given.*
- *Bob* wants to send a private message *m* to *Alice.*
- *Bob encrypts m* with *Alice's public key Pub_a.*

  y = ENC(m, Pub_a)
- *Alice receives y and decrypts it using its private key.*

  message = DEC(y, Pri_a)
- *ENC* and *DEC* are given and known functions.





- **PRIVATE KEY**
  - **Private key = *d***
  - ***e* * *d* = 1(mod(p-1)*(q-1))**
  - **7 * *d* = 1(mod 16 * 10)**
  - **7 * *d* = 1(mod160)**
  - *d* = 23

Google pictures

Elliptic Curve Digital Signature Algorithm

Alice sends a signed message to Bob (Curve equation, G, n)

Public domain

1. Use a designated hash function *H*(*)
2. A curve : y^2 = x^3 + 7 over Fq, q ~ prime.
3. G = (x, y), a point on the curve
4. *n* the multiplicative order of G

KeyGenerate

Out: *k* (private key), *K* (public key)

1. Select an integer *k* in [0, *n*-1].
2. Compute *K* = *k G*.
3. *K* and *G* ~ points on the curve.
4. *The* key-pair is (k, K).

Results: Alice's pair (k_A, K_A) and Bob's pair (k_B, K_B)

SignGenerate

In: m the message, Alice's private key k_A

Out: Alice' signature (r, s)

1. Calculate the message hash $e=H(m)$
2. Let z be the L_n leftmost bits of e where L_n is the bit length of the group order n.
3. Select an integer d from $[1, n-1]$.
4. Calculate the curve point (x_1, y_1)=dG.
5. Calculate $r=x_1$ mod n. If r=0, go to step 3.
6. Calculate $s=k^{-1}(z+rk_A)$ mod n. If s=0, go to step 3.
7. The signature is the pair (r, s).

https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Elliptic Curve Digital Signature Algorithm

Alice sends a signed message to Bob (Curve equation, G, n)

isSignatureValid

In: m the message,

Alice' signature (r, s), and K_A

Out: Valid or invalid

1. Verify if K_A is a valid curve point as follows:
    1. Check to see if K_A is not equal to the identity element O
    2. Check to see if K_A lies on the curve
    3. Check that n × $K_A = O$
2. Verify that r and s are integers in [1, $n-1$]. If not, the signature is invalid.
3. Calculate $w = s^{-1}$ mod n.
4. Calculate $u_1 = z$ w mod n and $u_2 = r^* w$ mod n.
5. Calculate the curve point $(x_1, y_1) = u_1{}^* G + u_2{}^* Q_A$. If $x1, y1 = O$, then the signature is invalid.
6. The signature is valid if $r \equiv x1$ mod n, invalid otherwise.

Reference https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Blockchain

An internet published and connected digital file.
Also refers to the pertinenent cryptographical techniques.

A digital file?
Can't the content be forged or altered easily?

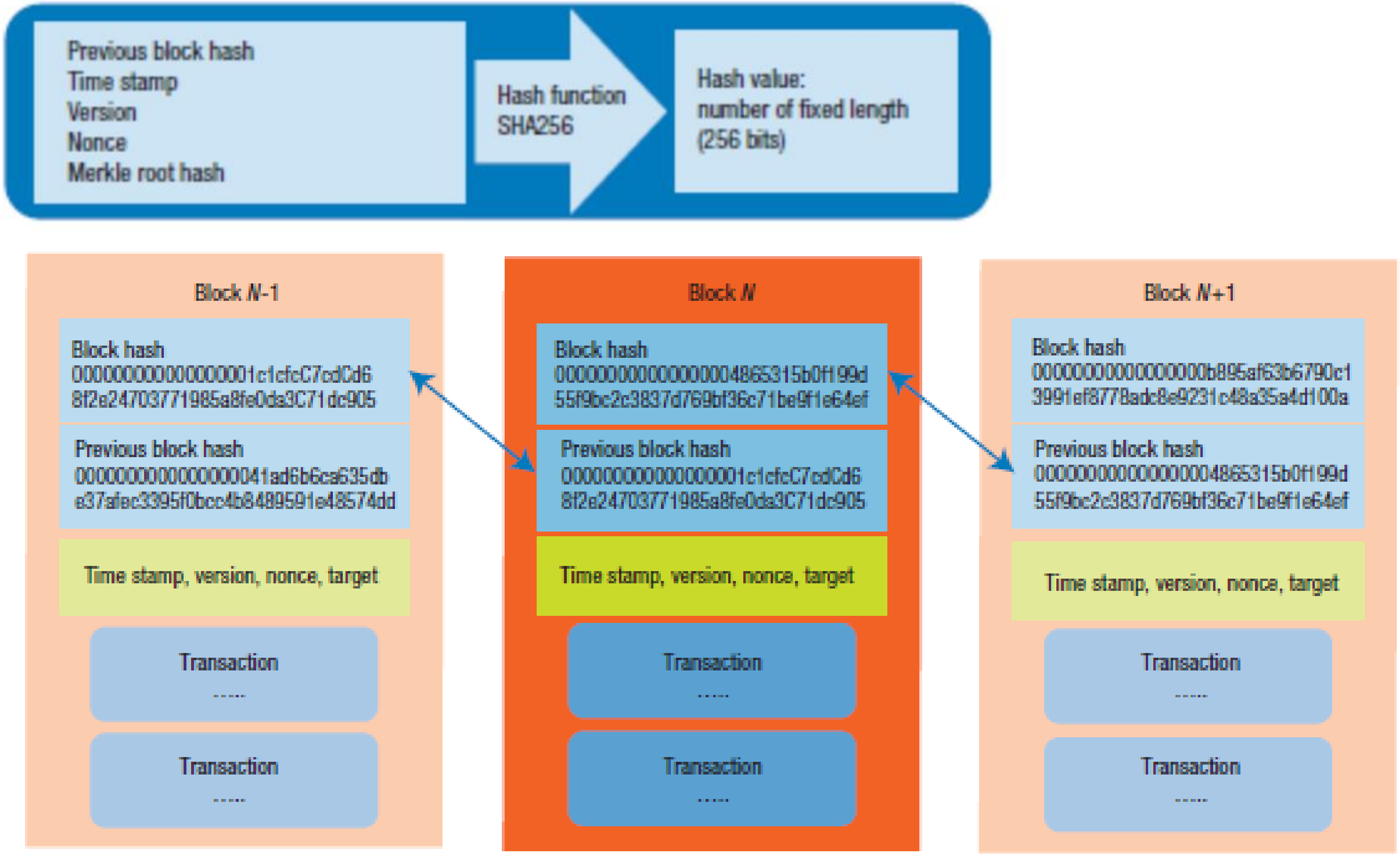
Novel way to resolve the problem of forgery and unwanted alterations.

- Each block should include a block summary.
- Block summary should be good enough, the block with a good enough summary attached is connected to the existing chain of blocks.

Revolutionary new idea!

- Any single computer cannot find a good block summary within a given amount of computing time.
- If the number of computers is large enough and all are simultaneously working on finding a good summary for a block, a single computer among them can become successful in finding a good summary.
- A reward is given to the computer which has found a good block summary.
- Once completed, a new race begins again for a new block.
- The more computers are gathered and the safer the system becomes.

Bitcoin Blockchain



Previous block hash
Time stamp
Version
Nonce
Merkle root hash

Hash function
SHA256

Hash value:
number of fixed length
(256 bits)

Block *N*-1

Block hash
000000000000000001c1cfcC7cdCd6
8f2e24703771985a8fe0da3C71dc905

Previous block hash
00000000000000000041ad6b6ca635db
e37afec3395f0bcc4b8489591e48574dd

Time stamp, version, nonce, target

Transaction
.....

Transaction
.....

Block *N*

Block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

Previous block hash
000000000000000001c1cfcC7cdCd6
8f2e24703771985a8fe0da3C71dc905

Time stamp, version, nonce, target

Transaction
.....

Transaction
.....

Block *N*+1

Block hash
0000000000000000b895af63b6790c1
3991ef8778adc8e9231c48a35a4d100a

Previous block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

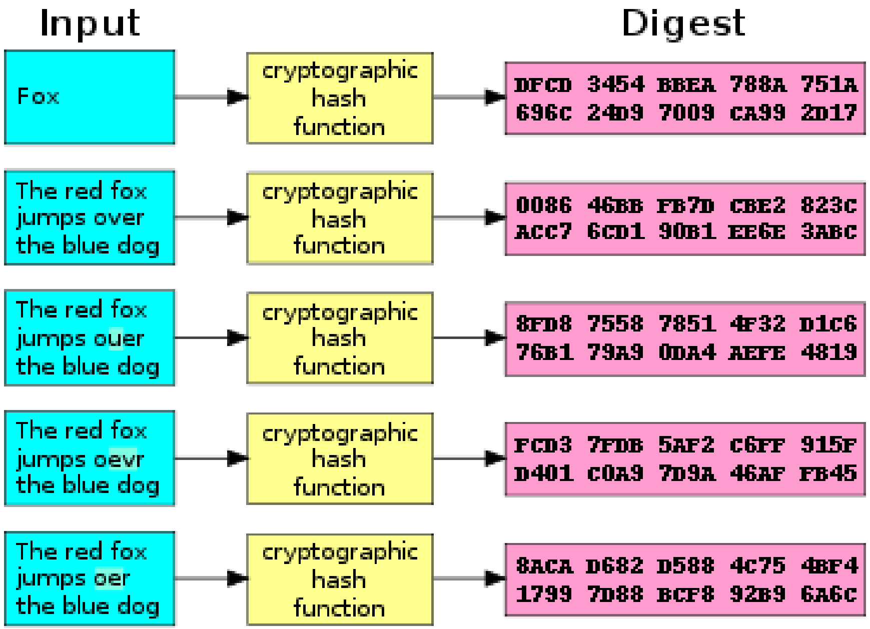
Time stamp, version, nonce, target

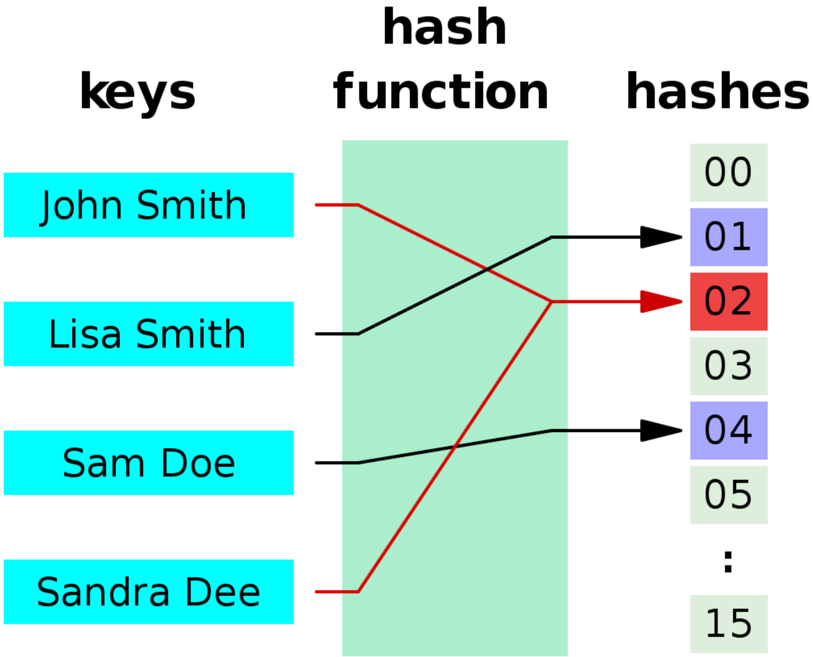
Transaction
.....

Transaction
.....

FIGURE 2. Bitcoin blockchain. The blockchain consists of text blocks containing records of transactions that are linked through consecutive hash numbers generated from the content of the previous block plus a random part.

Secure Hash Function I/O


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C



Pictures from google image

What is Hash Function?

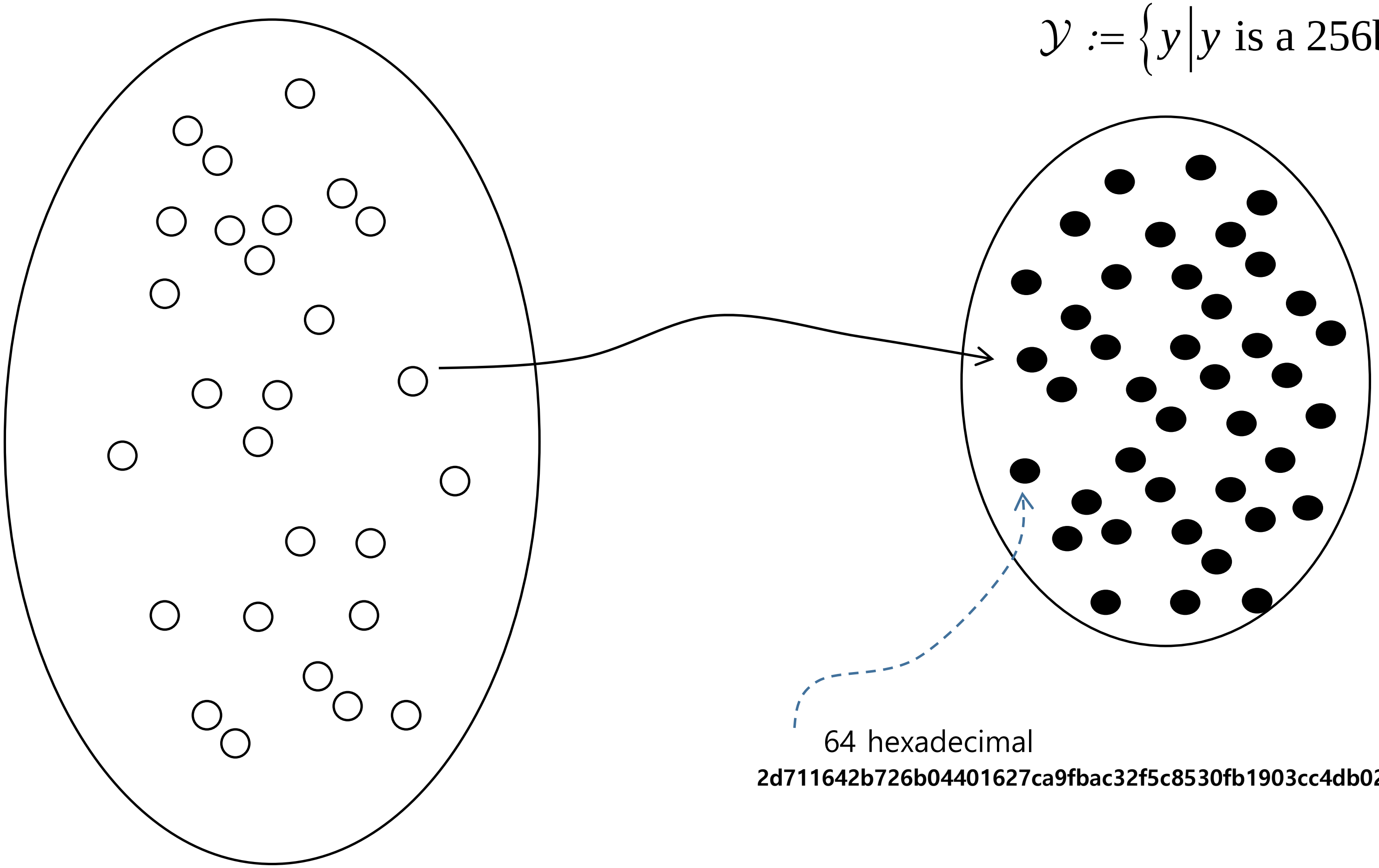
- Bitcoin uses SHA256.
- The input to the hash function is a text message or a file.
- The output of the hash function is 256 bit string.
- Conditions for Good Hash Function
  - (One way) With a little change in the input, the output is completely different.
    - Input distance has no relation to output distance.
  - (Collision free) Given y = H(x), finding x1 such that H(x1) = y shall be almost impossible!
  - (Collision free stronger) Finding an input pair x and x1 which leads to H(x) = H(x1) shall be almost impossible!

- See examples in MIT blockchain Demo, http://blockchain.mit.edu/how-blockchain-works/

SHA256, F(x) = y

$\mathcal{X} := \left\{ x \middle| x \text{ is a message up to 1 Mbyte in size} \right\}$

$\mathcal{Y} := \left\{ y \middle| y \text{ is a 256bit string} \right\}$



64 hexadecimal

2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

Finding Good Block Summary

- Let H(*) be the Hash Function

- Function F takes an input x and gives output y

  y = F(x)

- F(block) = block summary (hash value)

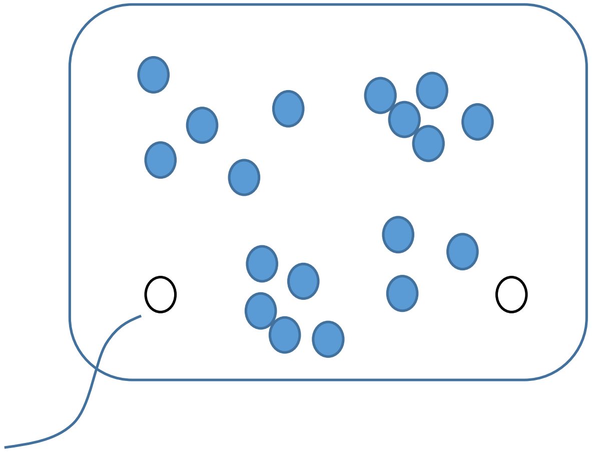
- Finding good block summary can be written as.

  F(block, *nonce*) < a certain value (PoW)

- Given a block, find nonce which satisfies the above inequality.

- Once *nonce* found, record it in the block header.

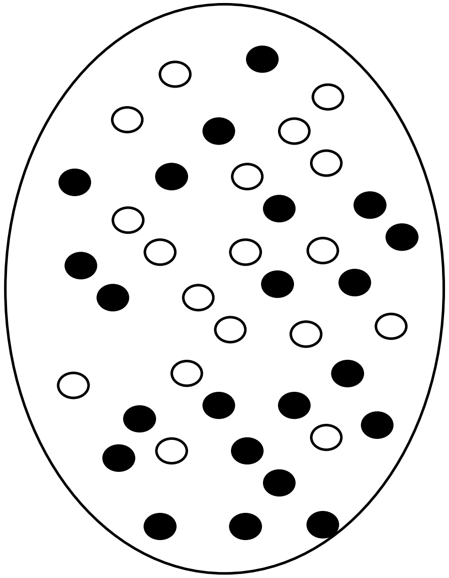
What is the probability to select a white ball?



Function Output

The probability a cpu solves (PoW) in a single cycle, given the first four strings are zeros?

$$\mathcal{Y} := \{ y \mid y \text{ is a 256bit string} \}$$



256/4 = 2^8/2^2 = 2^6 = 64

256 bit is 64 hexadecimal string

A hash value
2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

A good hash value which passes the condition that the first four digits are 0s.
0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

c = the set of any hash values = 2^256
a = the set of wanted hash values= 2^(256 – 16) = 2^240

P1 = a/c = 2^-16 = 1/(2^16) ~ 1/64000

Proof of Work is a ALone IMpossible Together Possible (Al-IM-To-Po) Problem!

- The input set C can be divided into two sets.
  Set A of elements each of which gives a wanted output.
  Set B = Complement of A.
  Let the size of each set be a, b, c.

- a = 2^10 ~ 10^3
  c = 2^32 ~ 10^9
  b = c – a

- Let there be a cpu which can take one input and gives one output.

- What is the probability that this cpu gives a good summary?

- P_1 = a/c
  = 10^-6
  = 0.000001

- How many hash cycles do you need in the average sense to find a good summary?

- A hash cycle is defined as give an input to the hash function and obtain the output from it.

Difficulty

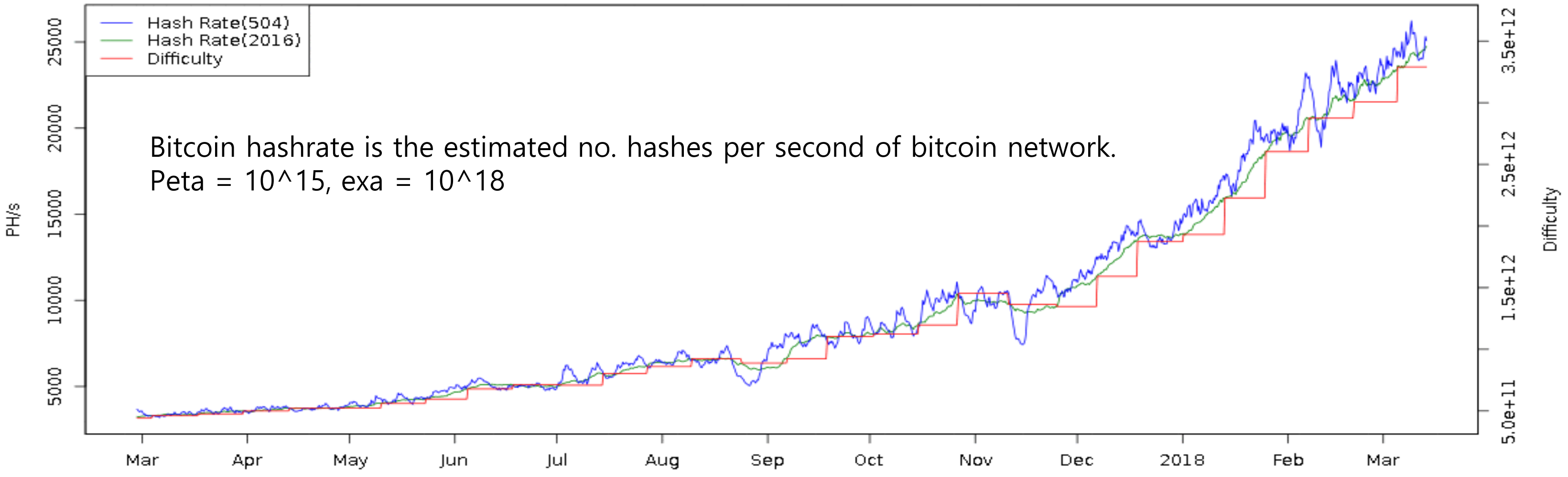
- The lower the target is, the more difficult the puzzle is.
- Recall our lecture note set 1. If target is a hash with 10 starting hexadecimal zeros, it would take on the average 2^40 trials to find a good hash.
- Among the network participants, your chance of winning a mining game is your hash power, i.e., the hash rate percentage of your mining network.
- The target value is adjusted every 2016 blocks so that one block is mined every 10 minutes. On the average, it takes 2 weeks to mine 2016 blocks.
- The new target is thus given by $\boxed{T_{new} = T_{old} \dfrac{\text{actual time taken to mine 2016 blocks}}{2016 \cdot 10 \,\text{min}}}$
- In Bitcoin, the difficulty is used to indicate how difficult it is to find a hash below a given target.
- Difficulty is defined as the ratio of the maximum allowed target to the current target.
- The maximum allowed target value is 2^224 at which difficulty is 1.
  - 256-224 = 32 bits or 32/4 = 8 hexadecimals.
  - Target with 32 leading zero bits is the minimum difficulty!

Difficulty today = 3.5e12

- Block #516447
- **BlockHash** 0000 0000 0000 0000 0006 082b 0352 8b8d d578 fa70 b5f5d1b1af62930a139a89b6
- **Difficulty** 3,511,060,552,899.7197 = 3.5e12
  - Notice from difficulty that target = 2^floor(log2(2^224/diff)) = 2^182.
  - Thus, the target hash has 256 – 182 = 74 leading zero bits.
  - Thus, the probability of successful mining per hash is 2^-74.
  - On the average, it would take 2^74 ~ 1.8e22 hashes to mine a single block.
- The hash rate of the bitcoin network should be

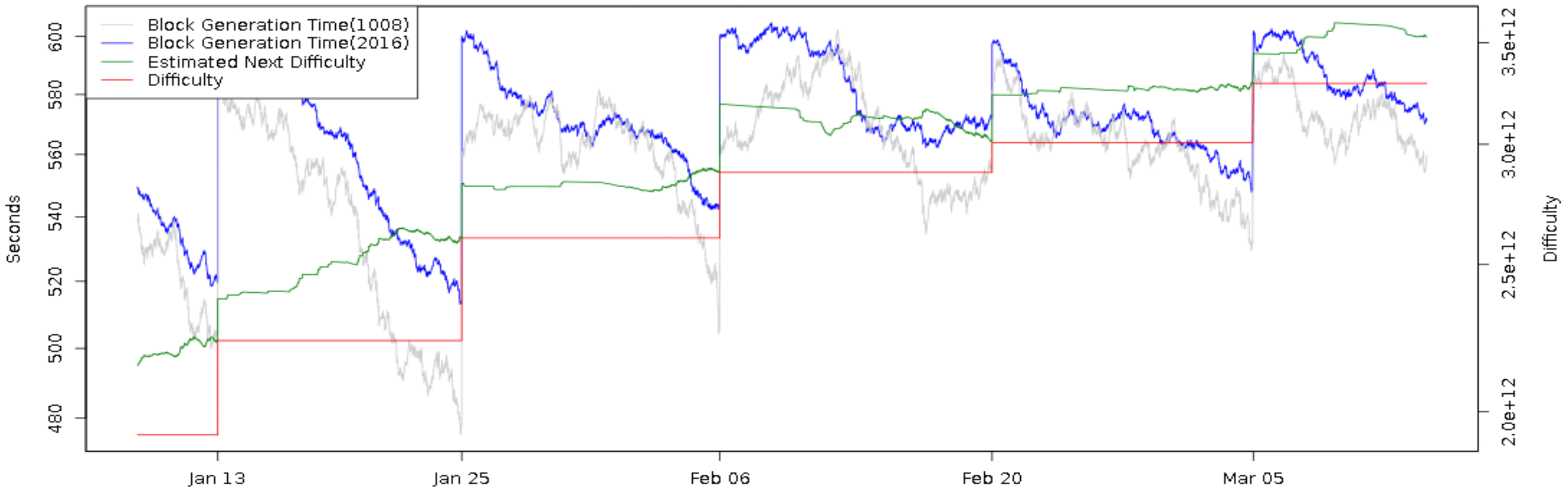
  1.88e22/600 = 3.14 e19 [hashes/sec] = 31.4 [exa H/sec].

- Today's hash rate at blockchain.info is 30 exaH/sec. https://blockchain.info/ko/charts/hash-rate



Bitcoin Hash Rate vs Difficulty (9 Months)

Bitcoin hashrate is the estimated no. hashes per second of bitcoin network.
Peta = 10^15, exa = 10^18



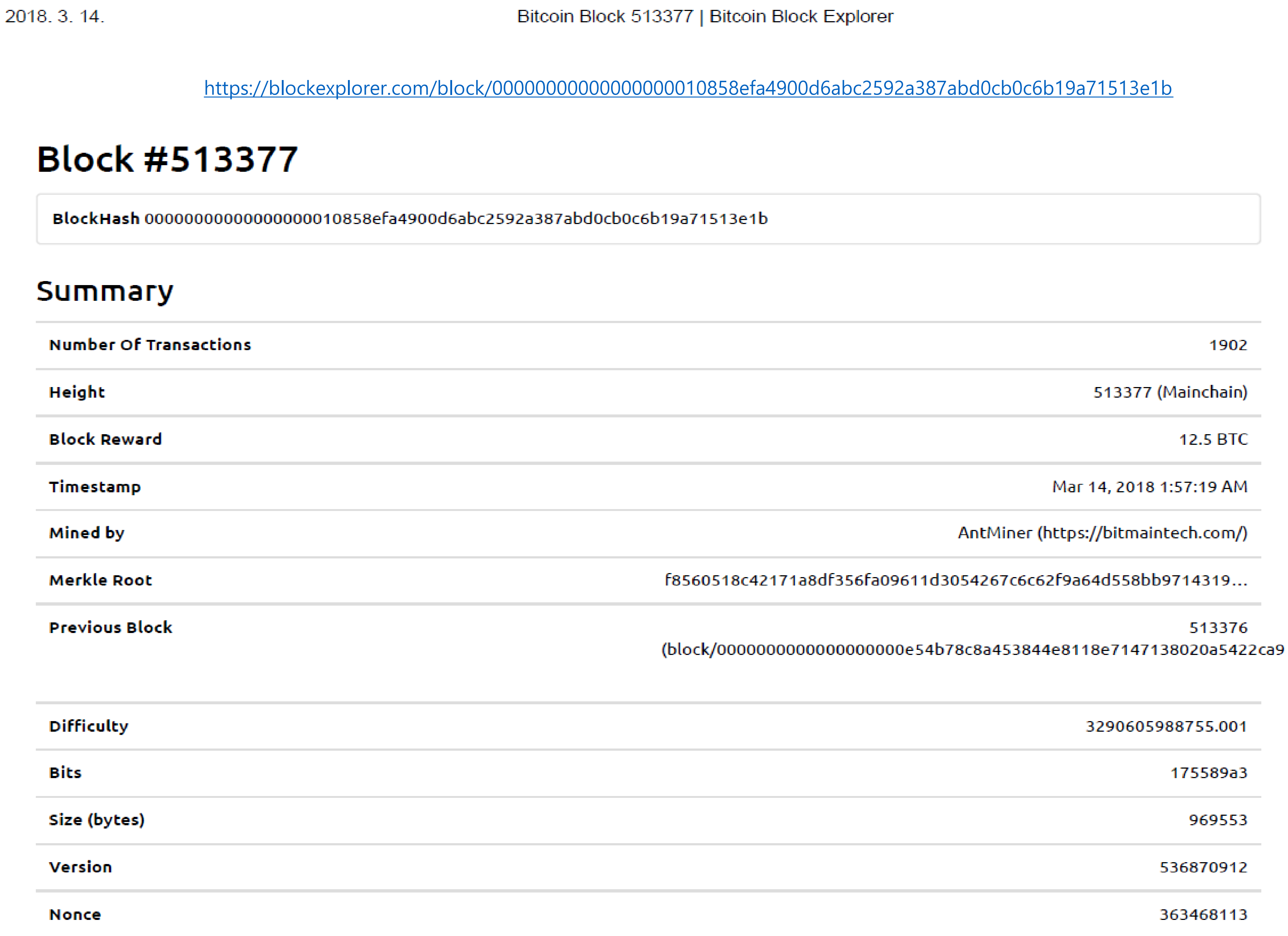
Bitcoin Block Generation Time vs Difficulty

https://bitcoinwisdom.com/bitcoin/difficulty

ASIC Mining Hardware

Bitcoin double SHA256 ASIC mining hardware

Product	Advertised Mhash/s	Mhash/J	Mhash/s/$	Watts	Price (USD)	Currently shipping	Comm ports	Dev-friendly
AntMiner S1 [1]	180,000	500	800	360	299[2]	Discontinued	Ethernet	GPL infringement
AntMiner S2 [3]	1,000,000	900	442	1100	2259	Discontinued	Ethernet	GPL infringement
AntMiner S3 [4]	441,000	1300	1154	340	382[2]	Discontinued	Ethernet	GPL infringement
AntMiner S4 [5]	2,000,000	1429	1429	1400	1400	Discontinued	Ethernet	GPL infringement
AntMiner S5 [6]	1,155,000	1957	3121	590	370	Discontinued	Ethernet	GPL infringement
AntMiner S5+ [7]	7,722,000	2247	3347	3,436	2,307	No	Ethernet	GPL infringement
AntMiner S7 [8]	4,860,000	4000	2666	1,210	1,823	No	Ethernet	GPL infringement
AntMiner S9 [9]	14,000,000	10182	5833	1,375	2,400	Yes	Ethernet	GPL



2018. 3. 14. Bitcoin Block 513377 | Bitcoin Block Explorer

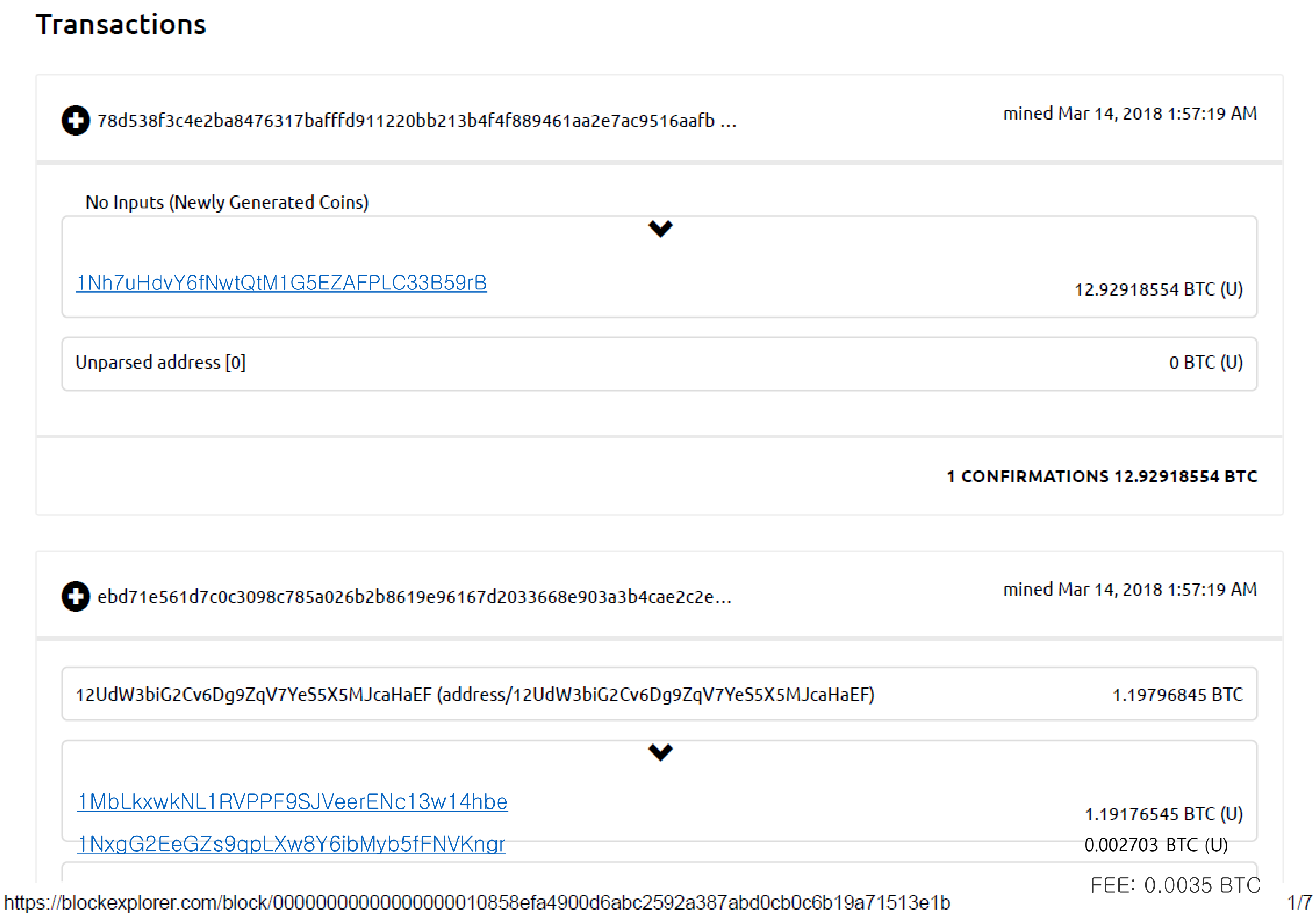
https://blockexplorer.com/block/000000000000000000010858efa4900d6abc2592a387abd0cb0c6b19a71513e1b

Block #513377

BlockHash 000000000000000000010858efa4900d6abc2592a387abd0cb0c6b19a71513e1b

Summary

Number Of Transactions	1902
Height	513377 (Mainchain)
Block Reward	12.5 BTC
Timestamp	Mar 14, 2018 1:57:19 AM
Mined by	AntMiner (https://bitmaintech.com/)
Merkle Root	f8560518c42171a8df356fa09611d3054267c6c62f9a64d558bb9714319...
Previous Block	513376 (block/000000000000000000e54b78c8a453844e8118e7147138020a5422ca9
Difficulty	3290605988755.001
Bits	175589a3
Size (bytes)	969553
Version	536870912
Nonce	363468113



Transactions

78d538f3c4e2ba8476317bafffd911220bb213b4f4f889461aa2e7ac9516aafb ... mined Mar 14, 2018 1:57:19 AM

No Inputs (Newly Generated Coins)

1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB	12.92918554 BTC (U)
Unparsed address [0]	0 BTC (U)

1 CONFIRMATIONS 12.92918554 BTC

ebd71e561d7c0c3098c785a026b2b8619e96167d2033668e903a3b4cae2c2e... mined Mar 14, 2018 1:57:19 AM

12UdW3biG2Cv6Dg9ZqV7YeS5X5MJcaHaEF (address/12UdW3biG2Cv6Dg9ZqV7YeS5X5MJcaHaEF)	1.19796845 BTC

1MbLkxwkNL1RVPPF9SJVeerENc13w14hbe	1.19176545 BTC (U)
1NxgG2EeGZs9qpLXw8Y6ibMyb5fFNVKngr	0.002703 BTC (U)

FEE: 0.0035 BTC

https://blockexplorer.com/block/00000000000000000010858efa4900d6abc2592a387abd0cb0c6b19a71513e1b 1/7

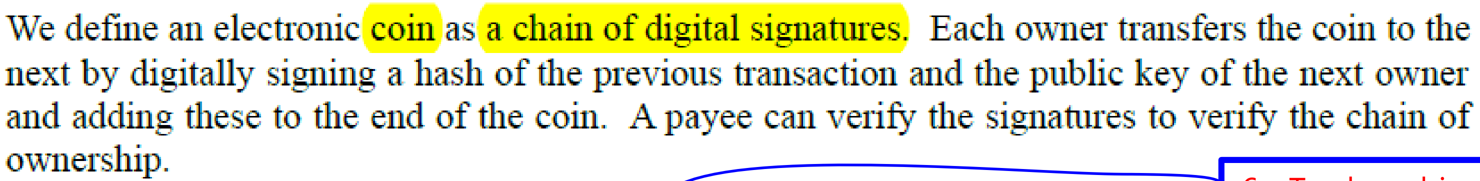
Proof of Work and Data Immutability

- Proof of work(작업증명 in Korean) is to have a large set of miners find a solution satisfying (PoW). The first miner which succeed in solving it obtains the right to produce a certain amount of new coins to himself.
- It is the key mechanism for enforcing data integrity stored inside the blockchain.
- Blockchain is a very large stone!
- Each and every transaction is checked for validity and scribed into the stone.
- How can it be done with digital file?
- Answer is simple!
- Let a large number of computers work together simultaneously. Let the first computer which is successful at finding a good answer get rewarded. Have a new race begin by having the computers work on a new problem (new block) and reward another winner at the end of this new race. The proof of work that a large number of computers have worked together is written into the block. If any computer, or a group of computers, aims to change the block content, then the same amount of work needs to be redone.
- How is the proof of work done?
  Use a Secure Hash Function(SHA).
  Characteristics of this function is that it is a forward-only function. That is, given the output value of this function, one cannot make any good guess about what the input value was. Thus, the only way to find a good answer to (PoW) problem is to try repeatedly with different input values as fast as possible until run across a satisfying one.
- Once a good answer is found, the input value which produces this good output value is scribed into the block (more specifically, into the blockheader).
- Anybody can figure out if it is a good answer or not. How?

Bitcoin

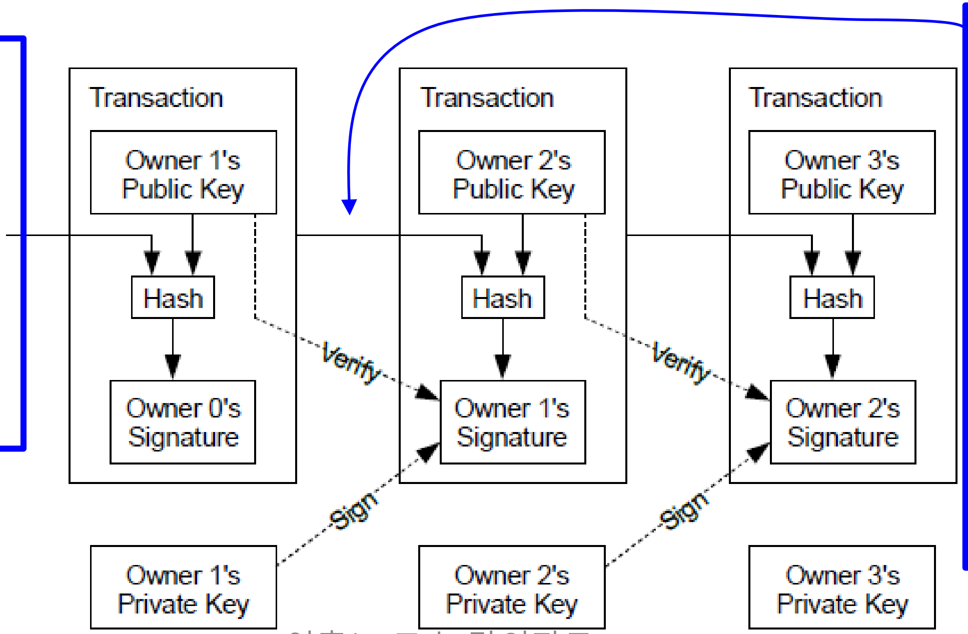
- Bitcoin is a chain of signatures.
  - Digital money with the effect of in-person transfer of money

An e-coin is a chain of signatures.



We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

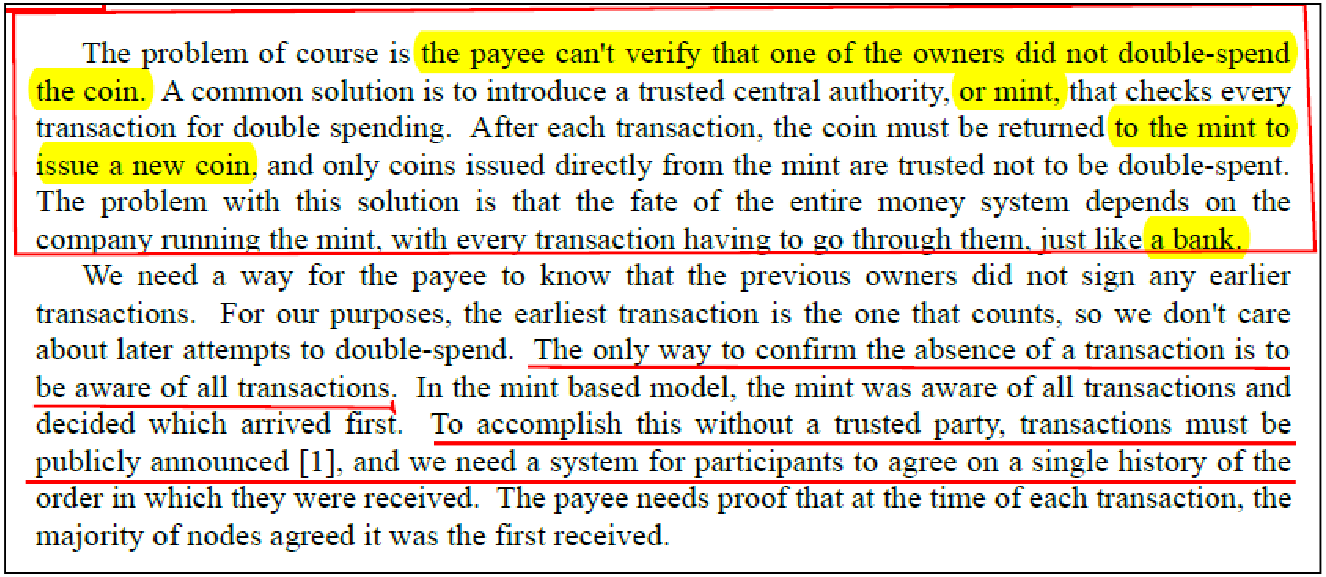
2nd Tx scene
1. The first TX shows that O1 owns the coin.
2. O1 can transfer it to anybody, say O2.
3. O1 writes TX 2.
4. O1 asks Owner2, the new owner, for his public key.
5. O1 hashes the received public key and TX1, and writes down the hash value in TX2.



6. To show his ownership status, O1 signs the hash value and leaves the signature in TX2.
7. Now, anybody can verify O1's signature with O1's pubic key written in Tx1.

Once TX 2 recorded and published, anybody can easily see TX2 and knows that O1 has transferred his coin ownership to O2.

Double Spending Problem

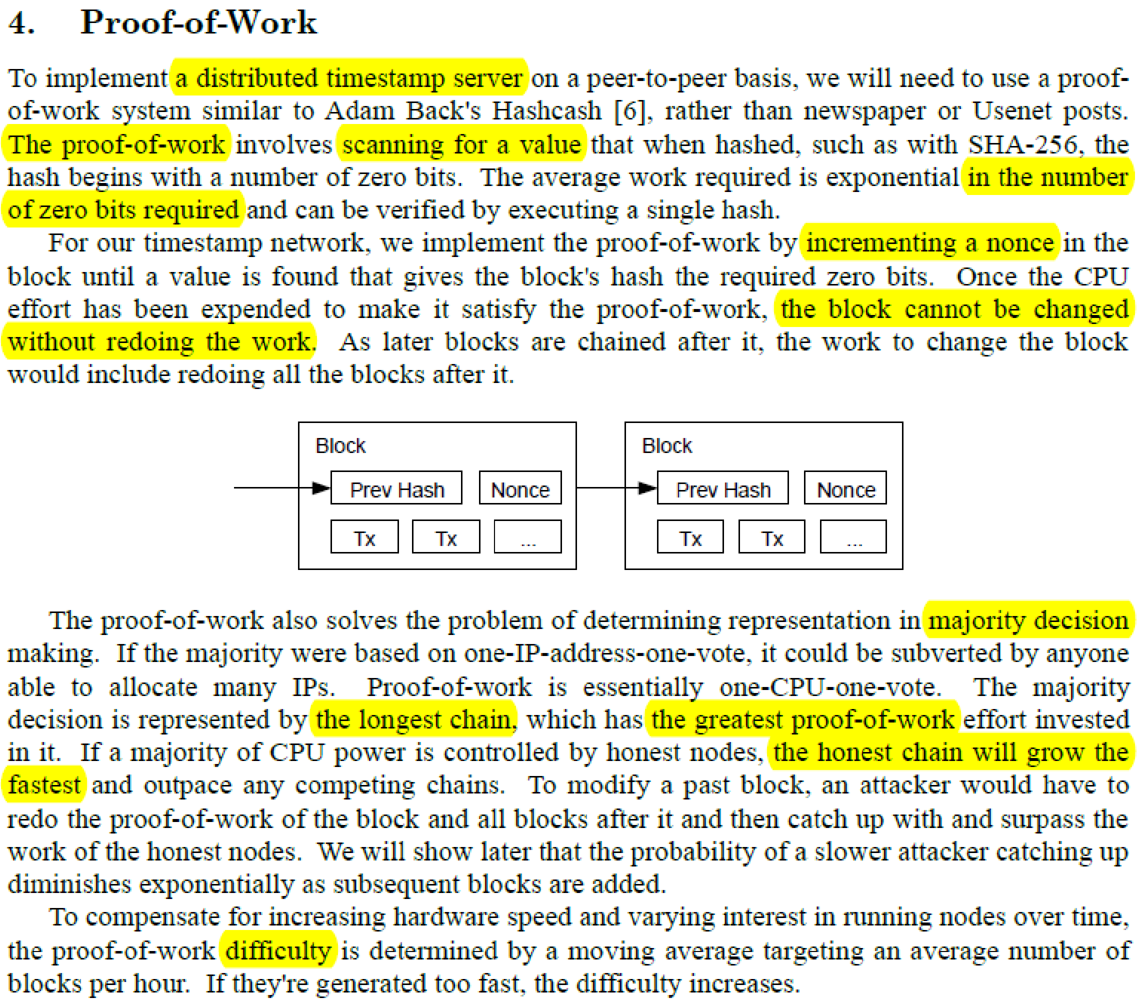


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

Blockchain & Proof-of-Work

- Aim to make a timestamp server in a P2P network.
  - Why?
  - Not to rely on the central authority.
  - Central authority such as banks and states
  - Within a nation, the state government can run the timestamp server
  - But for trades overseas, P2P across different nations would be needed.
- Solution?
  - Distributed timestamp P2P network
  - Distributed, thus, it is difficult to maintain the integrity of data.
  - To keep the integrity of data, PoW system is proposed!



4. Proof-of-Work

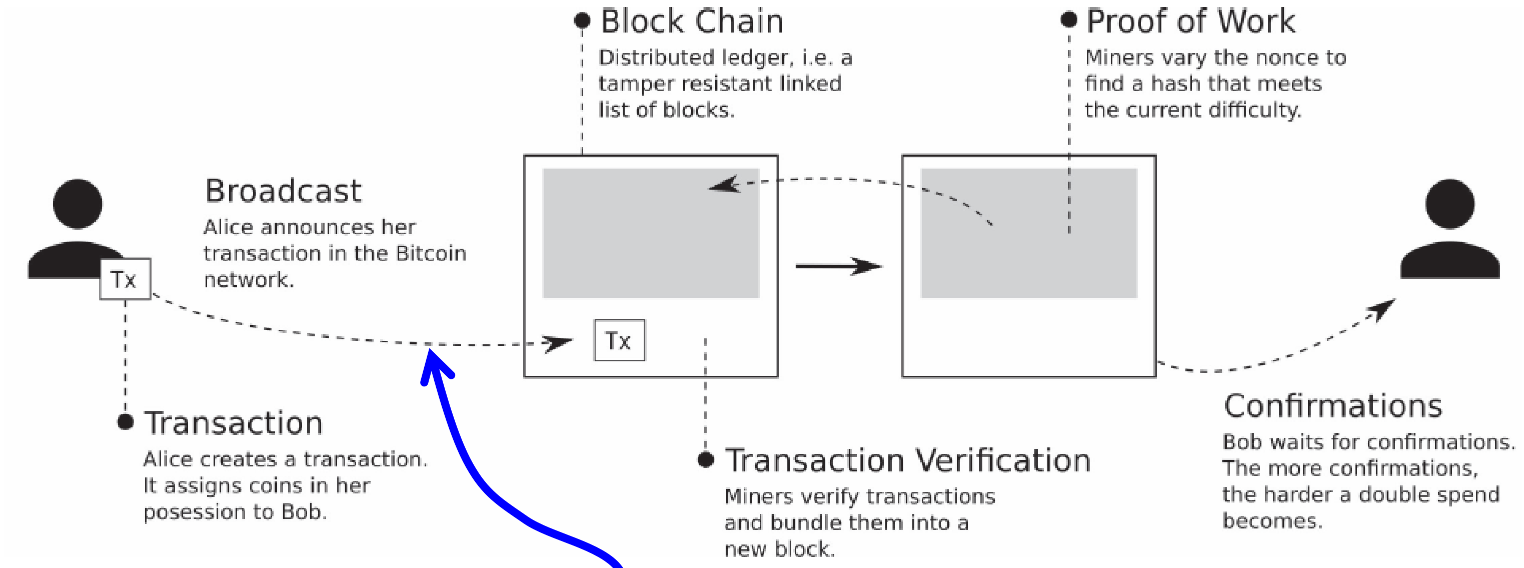
To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

TSCHORSCH AND SCHEUERMANN: BITCOIN AND BEYOND: TECHNICAL SURVEY ON DECENTRALIZED DIGITAL CURRENCIES 2091



Block Chain
Distributed ledger, i.e. a tamper resistant linked list of blocks.

Proof of Work
Miners vary the nonce to find a hash that meets the current difficulty.

Broadcast
Alice announces her transaction in the Bitcoin network.

Transaction
Alice creates a transaction. It assigns coins in her posession to Bob.

Transaction Verification
Miners verify transactions and bundle them into a new block.

Confirmations
Bob waits for confirmations. The more confirmations, the harder a double spend becomes.

Fig. 4. Bitcoin's building blocks explained.

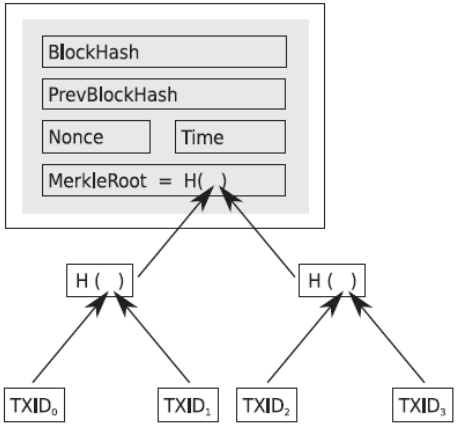


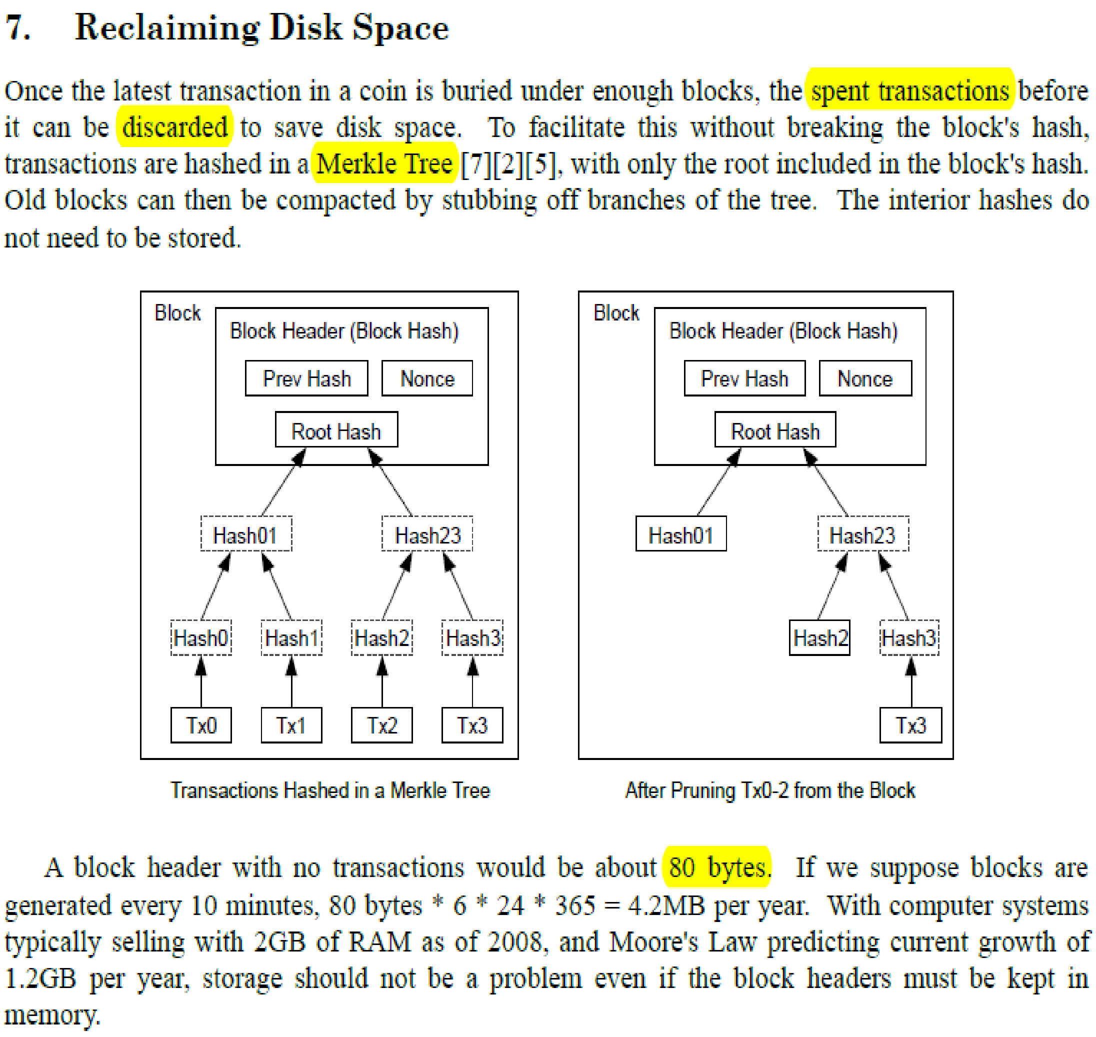
Fig. 8. Merkle tree.

Blockheader

- Use Merkle tree and save disk space
- Save the blockhash in the header.
- Those tree branches recording past transactions are erased but the hash values.
- 80 byte Blockheader

.

1. Prev hash: 256 bit = 2^8 = 2^5*(2^3) = 2^5 Bytes = 32 Bytes
2. Roothash = 32 Bytes
3. Nonce = 4 Bytes = 32 bit
4. Time
5. Difficulty
6. version



7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

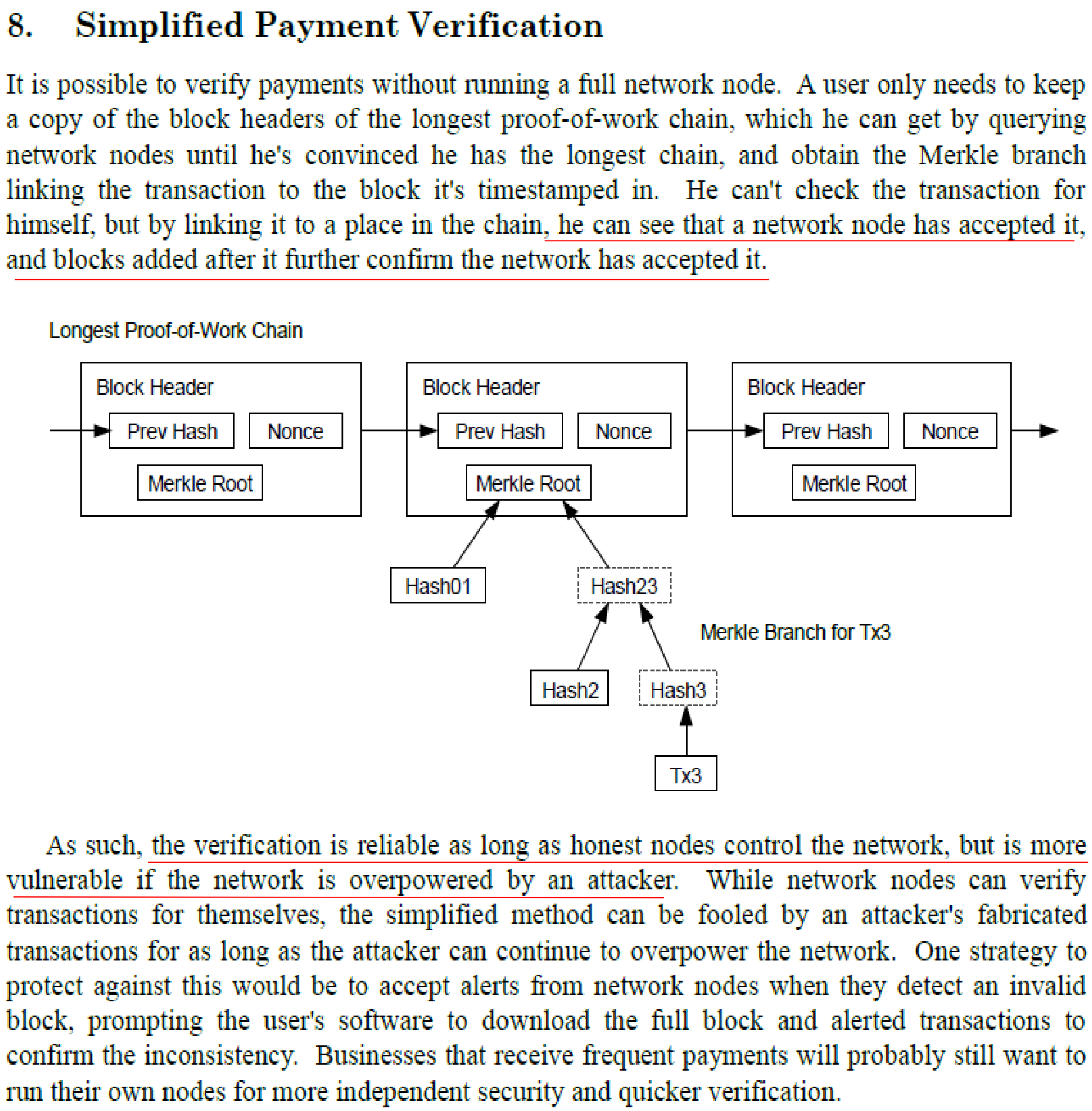
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

Longest chain is trusted, why?

- A headers-only chain use can be used for simplification!
- For full verification, one can download the full chain with full transaction record.
- But there is no guarantee with regard to chain's validity even for the full chains are used, as attacks are possible at any time and thus the network is vulnerable whenever network is overpowered by attackers.
- There is no guarantee that one obtains the longest chain by querying either.
- But when one has been around for sufficiently long time, then it shall not be difficult for one to obtain the longest chain.
- Things work as long as honest nodes control the network.
- But when there are nodes complaining inconsistencies and discontinuities, it becomes the time to stop believing the integrity of even the longest status-quo chain.



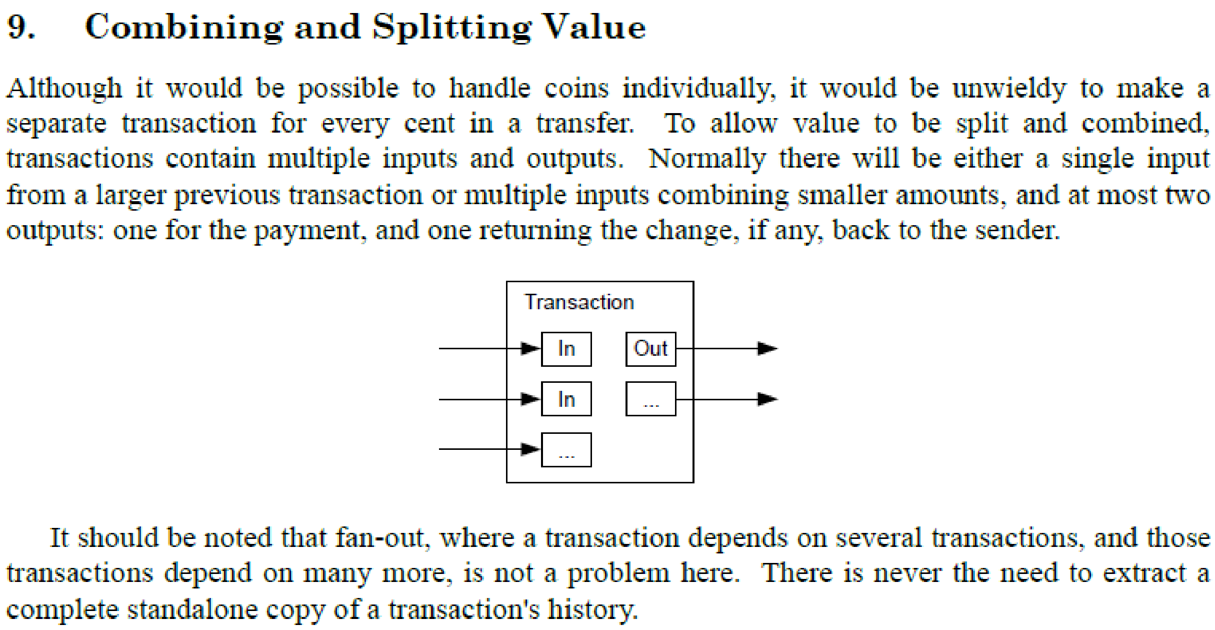
8. Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

Payment and changes

- How to get the change?



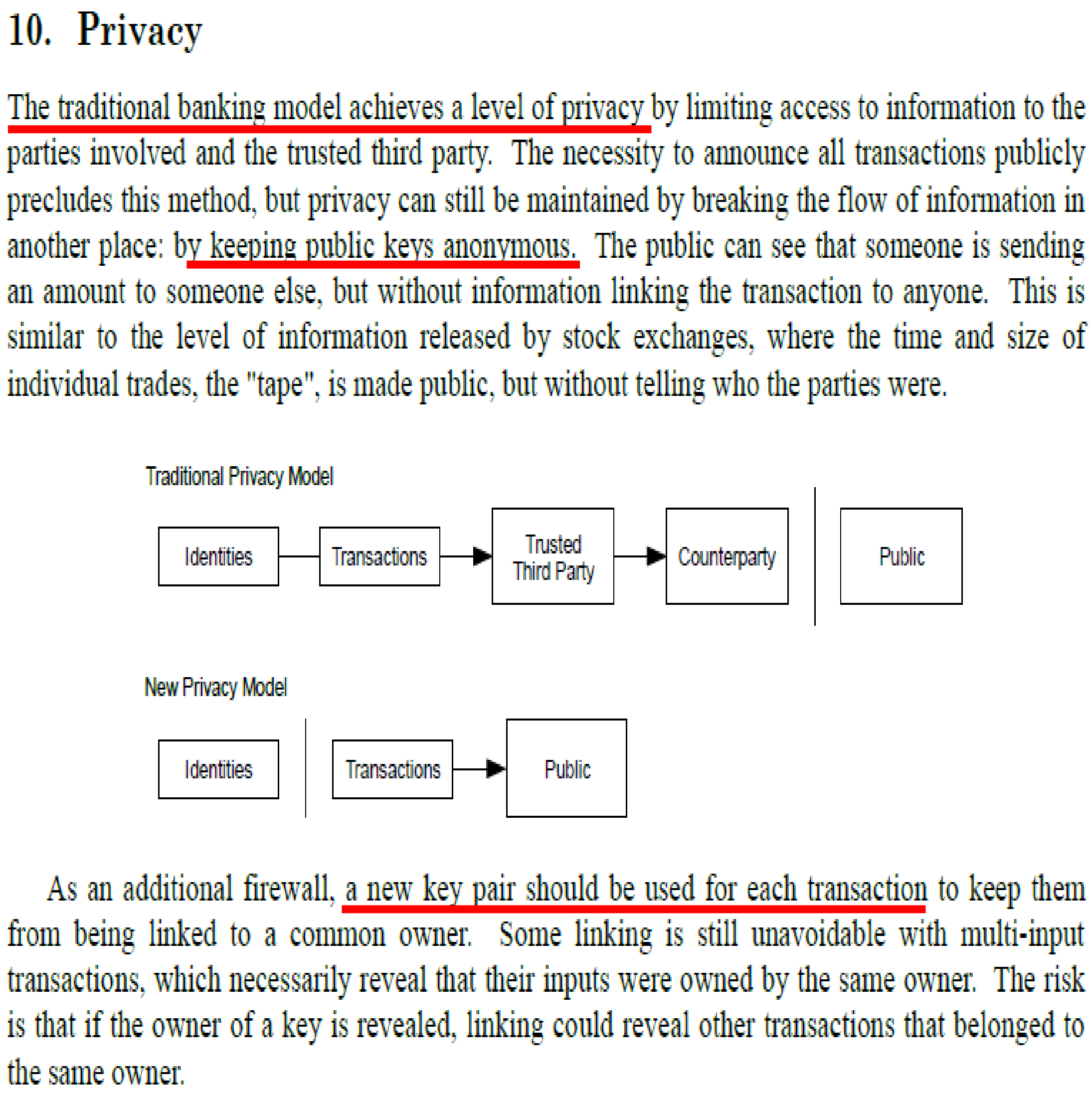
9. Combining and Splitting Value

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

Privacy, by Anonymous Pub Key

- Blockchain is published.
- Privacy is maintained by keeping public key anonymous!
- Additional privacy by using new public key per transaction!



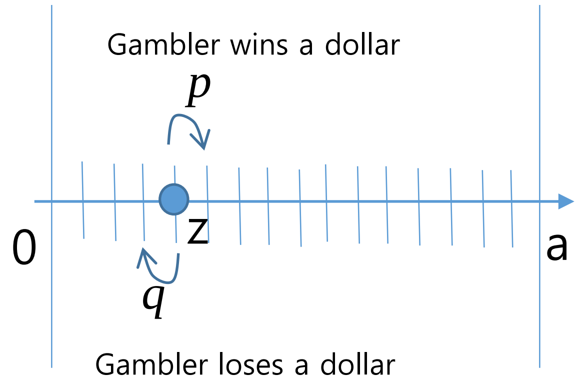
10. Privacy

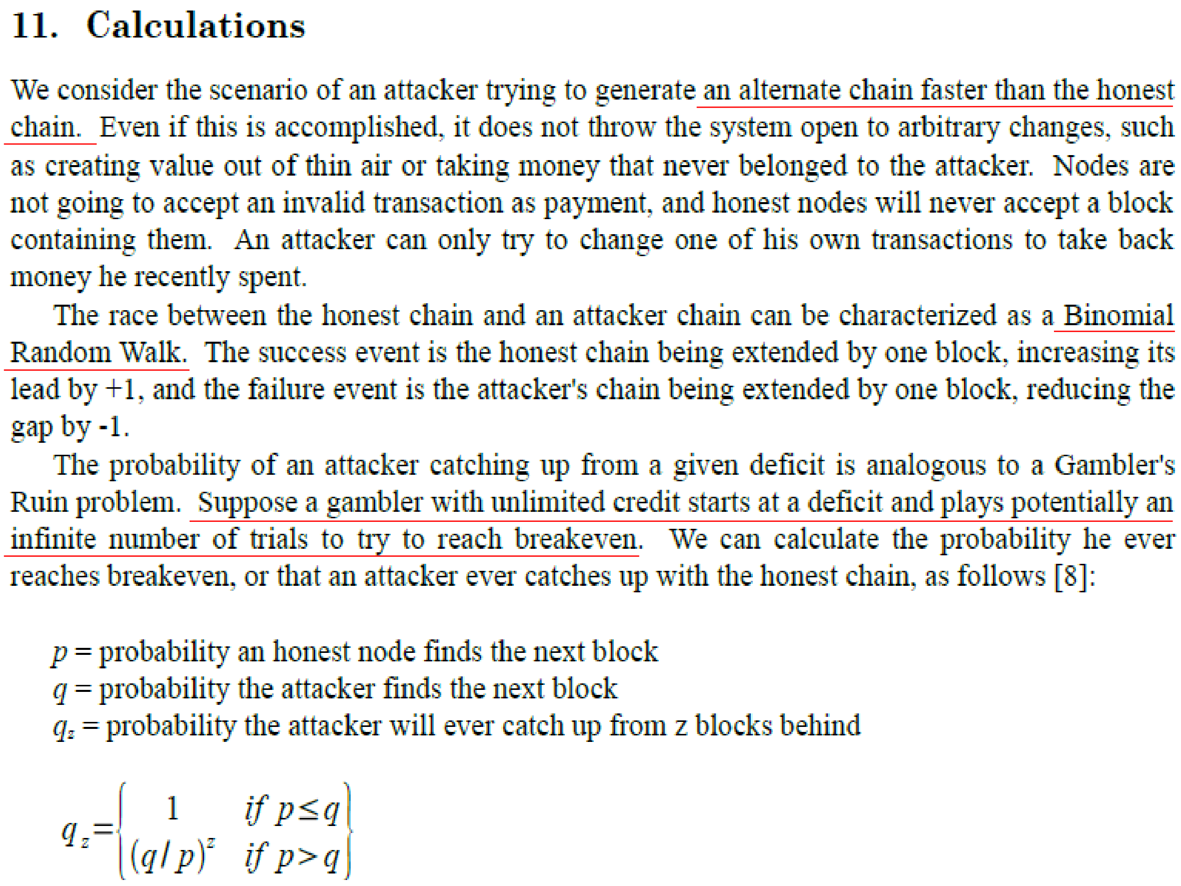
The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

How Difficulty to Attack?

- What happens when the attacker's chain dominates the honest chain?
- The best attack that can be made is to alter its own transaction.
- Namely, reclaim what he has paid.





11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

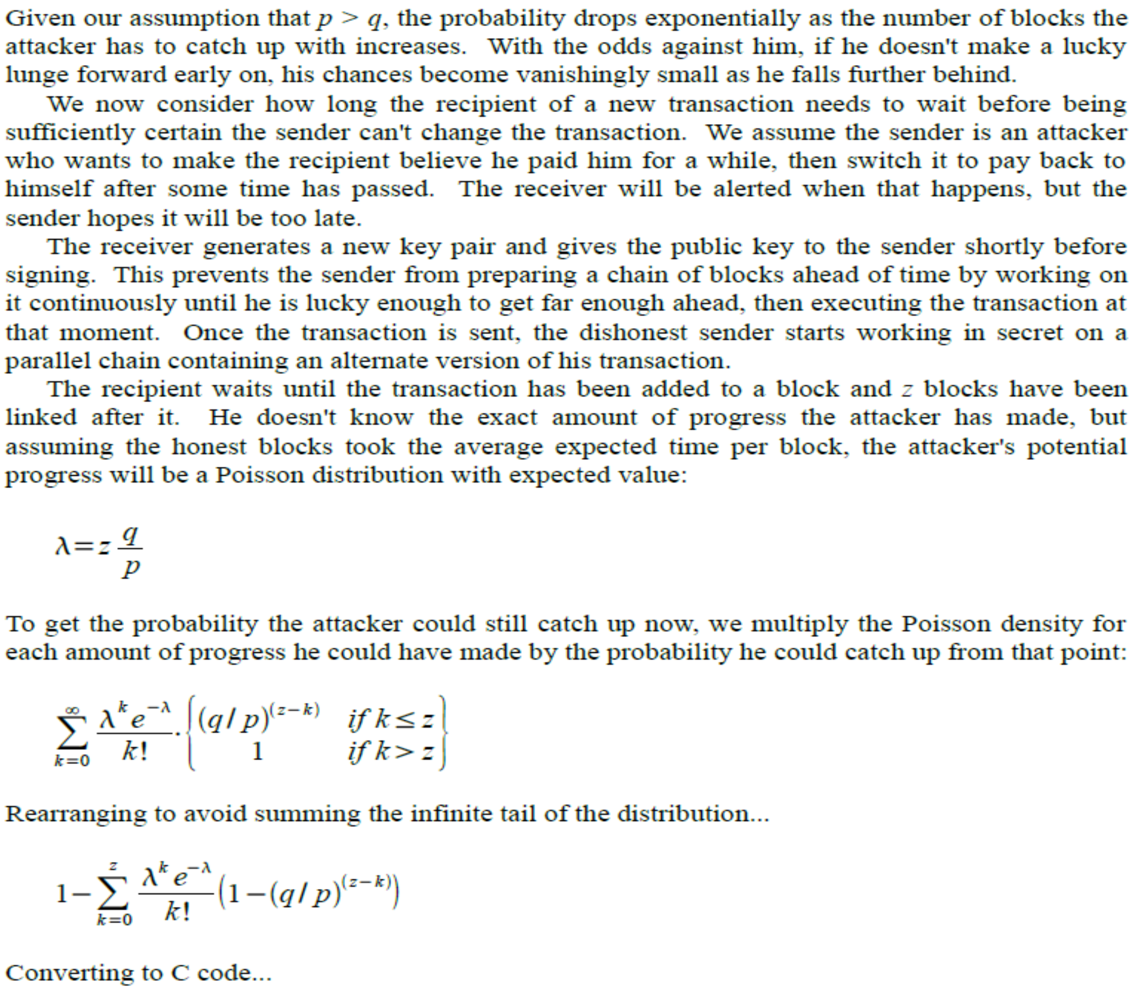
p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \left\{ \begin{array}{cc} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{array} \right\}$$

Attacker is the payer, fooling the payee!

- Given z blocks added. Assumed average time took by the honest nodes.

What is the probability that the attack is successful?



Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{Bmatrix} (q/p)^{(z-k)} & \mathit{if}\ k \le z \\ 1 & \mathit{if}\ k > z \end{Bmatrix}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

Double Spend Race Attack

A announces a TX showing A sends B 1 BTC at the end of time t0.

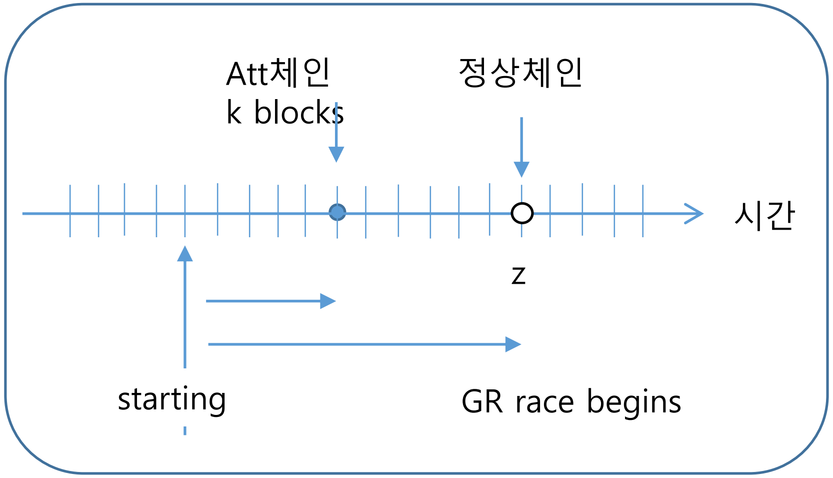
This TX gets into a block (1 confirmation) at t1.

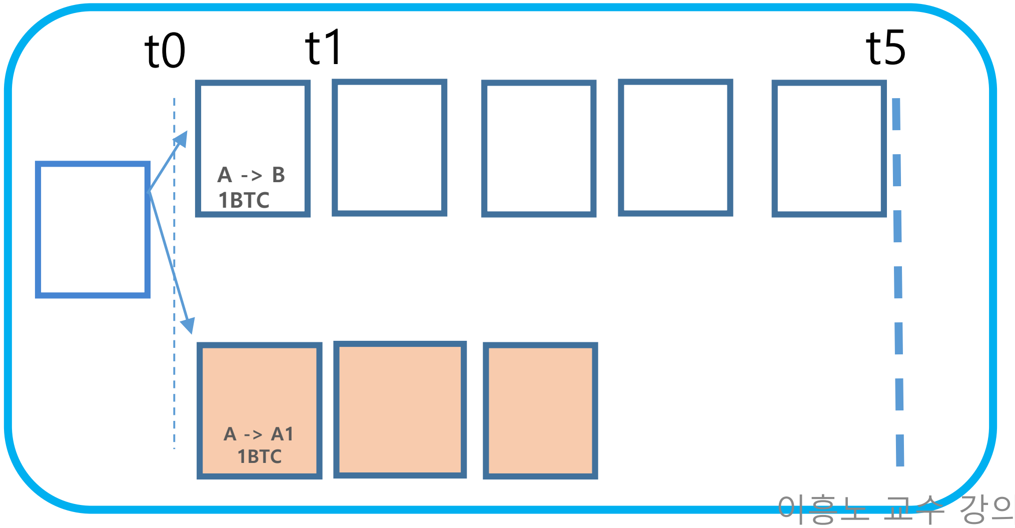
B waits until he gets the 5th confirmation at t5.

A is the attacker.

A starts preparing a double spend attack at t0. Namely, A grow its own chain. His chain has replaced the TX A->B 1BTC with a TX, A -> A1 1BTC. A1 is another public key of A.

At t5, A has mined 3 blocks and needs to decide if he continues to grow his own chain or not.





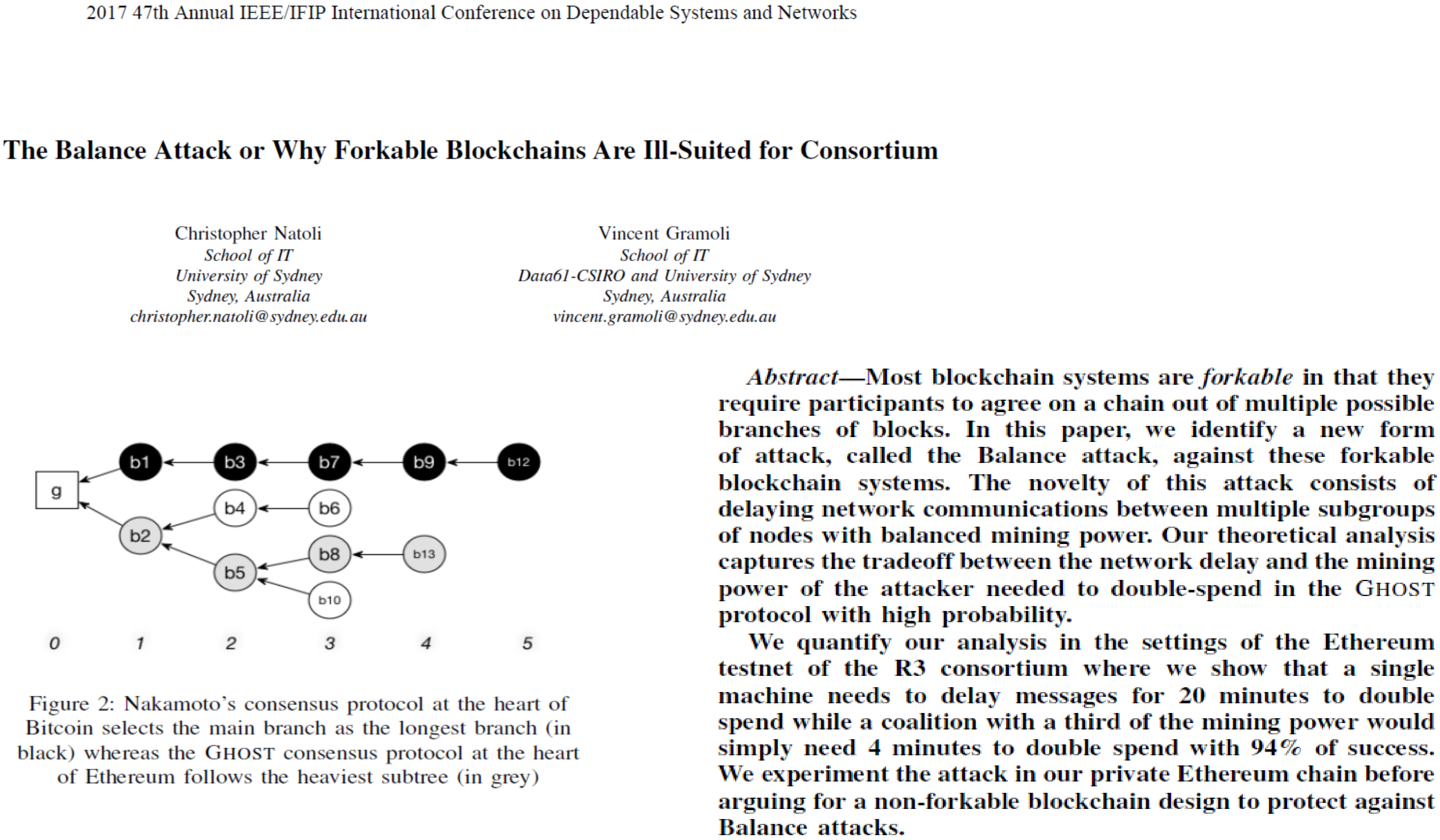
Attack Success Probability(q,z)

$$\sim \sum_{k=0}^{\infty} \begin{Bmatrix} (q/p)^{z-k} & k<z \\ 1 & k\geq z \end{Bmatrix} \text{Poisson}(\lambda = zq/p)$$

λ is the average number of blocks that the attacker mines in z unit of time

$$= \sum_{k=0}^{\infty} \begin{Bmatrix} (q/p)^{z-k} & k<z \\ 1 & k\geq z \end{Bmatrix} \frac{(zq/p)^{k}\, e^{-zq/p}}{k!}$$

Fork occurs, why and how to resolve



2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks

The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium

Christopher Natoli
School of IT
University of Sydney
Sydney, Australia
christopher.natoli@sydney.edu.au

Vincent Gramoli
School of IT
Data61-CSIRO and University of Sydney
Sydney, Australia
vincent.gramoli@sydney.edu.au

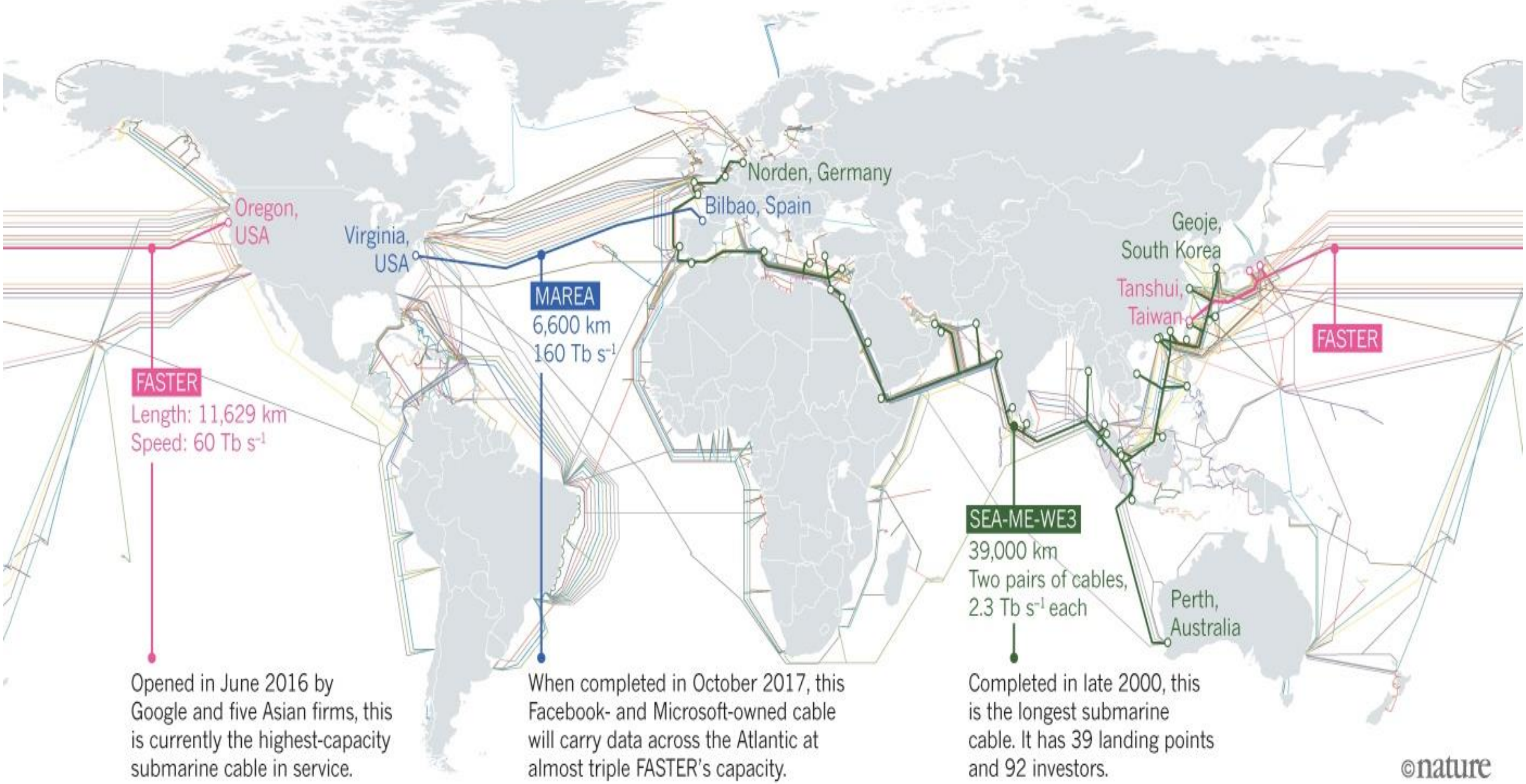
Figure 2: Nakamoto's consensus protocol at the heart of Bitcoin selects the main branch as the longest branch (in black) whereas the GHOST consensus protocol at the heart of Ethereum follows the heaviest subtree (in grey)

***Abstract*—Most blockchain systems are *forkable* in that they require participants to agree on a chain out of multiple possible branches of blocks. In this paper, we identify a new form of attack, called the Balance attack, against these forkable blockchain systems. The novelty of this attack consists of delaying network communications between multiple subgroups of nodes with balanced mining power. Our theoretical analysis captures the tradeoff between the network delay and the mining power of the attacker needed to double-spend in the GHOST protocol with high probability.**

We quantify our analysis in the settings of the Ethereum testnet of the R3 consortium where we show that a single machine needs to delay messages for 20 minutes to double spend while a coalition with a third of the mining power would simply need 4 minutes to double spend with 94% of success. We experiment the attack in our private Ethereum chain before arguing for a non-forkable blockchain design to protect against Balance attacks.

Internet Today

THE SUBMARINE WEB | Much of the world's Internet traffic passes under the oceans, through fibre-optic cables that can run along the sea bed for thousands of kilometres. Companies are constantly laying more and better cables.



FASTER
Length: 11,629 km
Speed: 60 Tb s⁻¹

Opened in June 2016 by Google and five Asian firms, this is currently the highest-capacity submarine cable in service.

MAREA
6,600 km
160 Tb s⁻¹

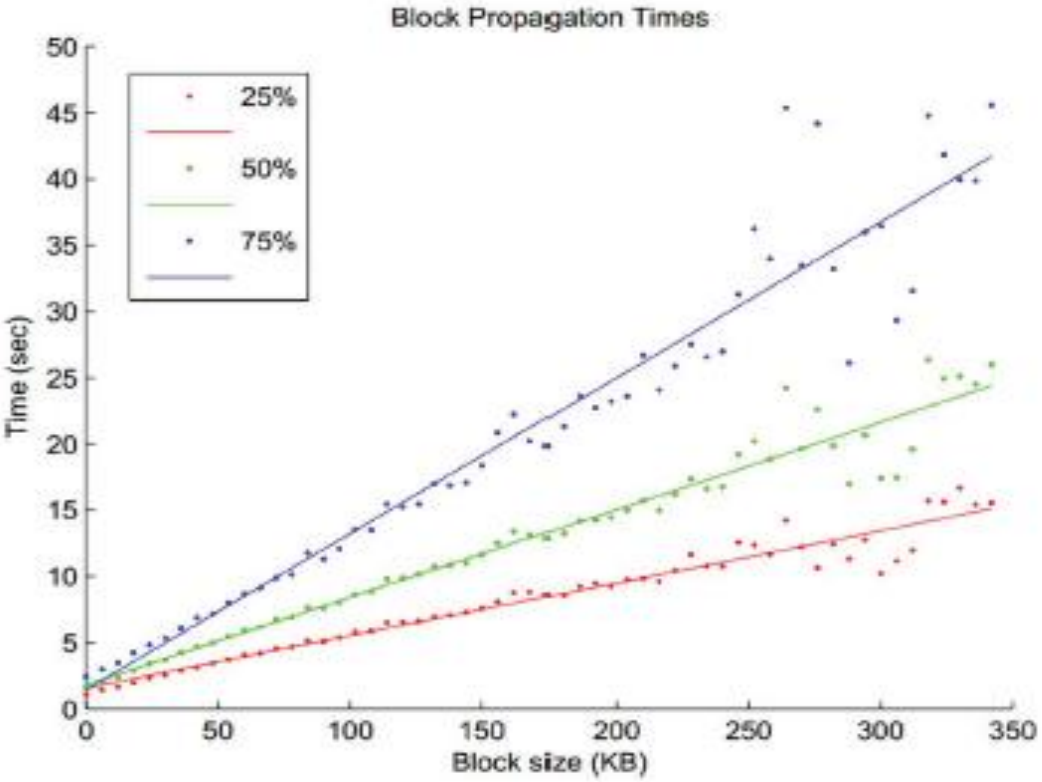
When completed in October 2017, this Facebook- and Microsoft-owned cable will carry data across the Atlantic at almost triple FASTER's capacity.

SEA-ME-WE3
39,000 km
Two pairs of cables, 2.3 Tb s⁻¹ each

Completed in late 2000, this is the longest submarine cable. It has 39 landing points and 92 investors.

Taken from Nature

Block Propagation Time

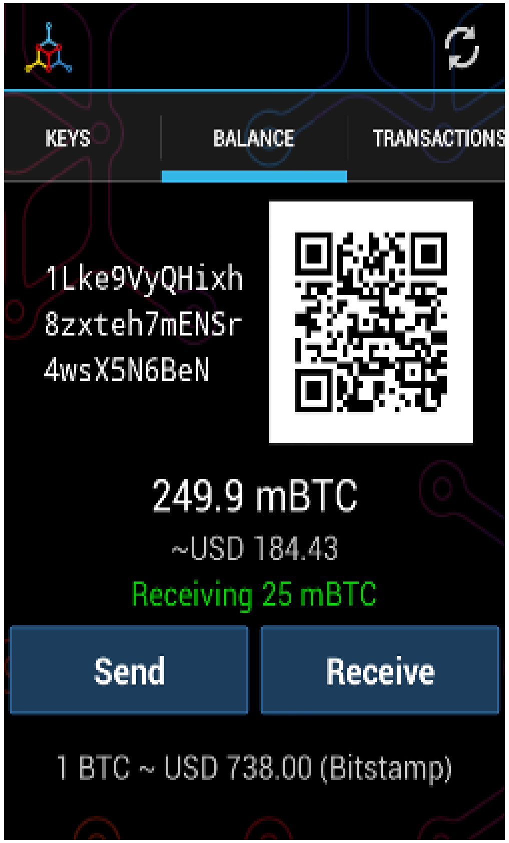


Source: Yonatan Sompolinsky and Aviv Zohar: "Accelerating Bitcoin's Transaction Processing" 2014

Figure 3.10 **Block propagation time.** This graph shows the average time that it takes a block to reach various percentages of the nodes in the network.

Wallet

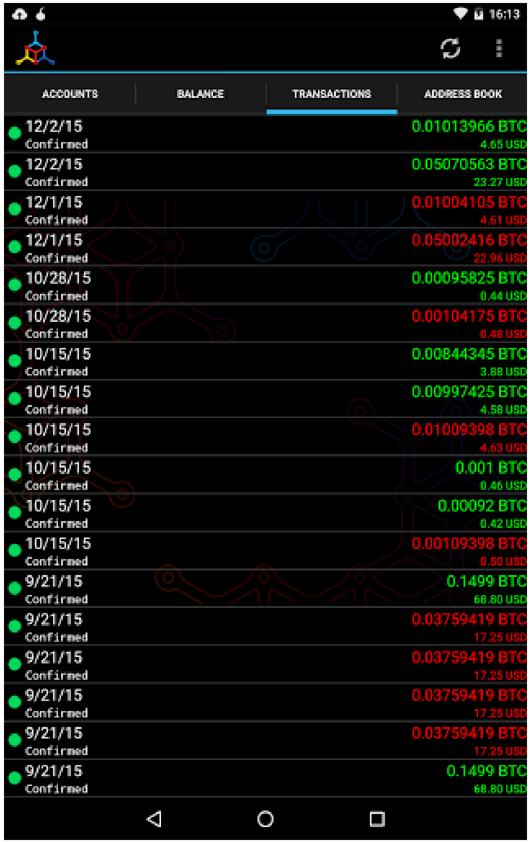
- Stores one's private and public key pairs
- Bitcoin addresses are derived from hashing a public key using SHA256 and RIPEMD-160, prepending a version number and appending a checksum for error detection.
- Addresses are base58-encoded to eliminate ambiguous characters.
- The purpose is to make it short and hide the public key.
- There was comparison based attack on signatures.



1Lke9VyQHixh
8zxteh7mENSr
4wsX5N6BeN

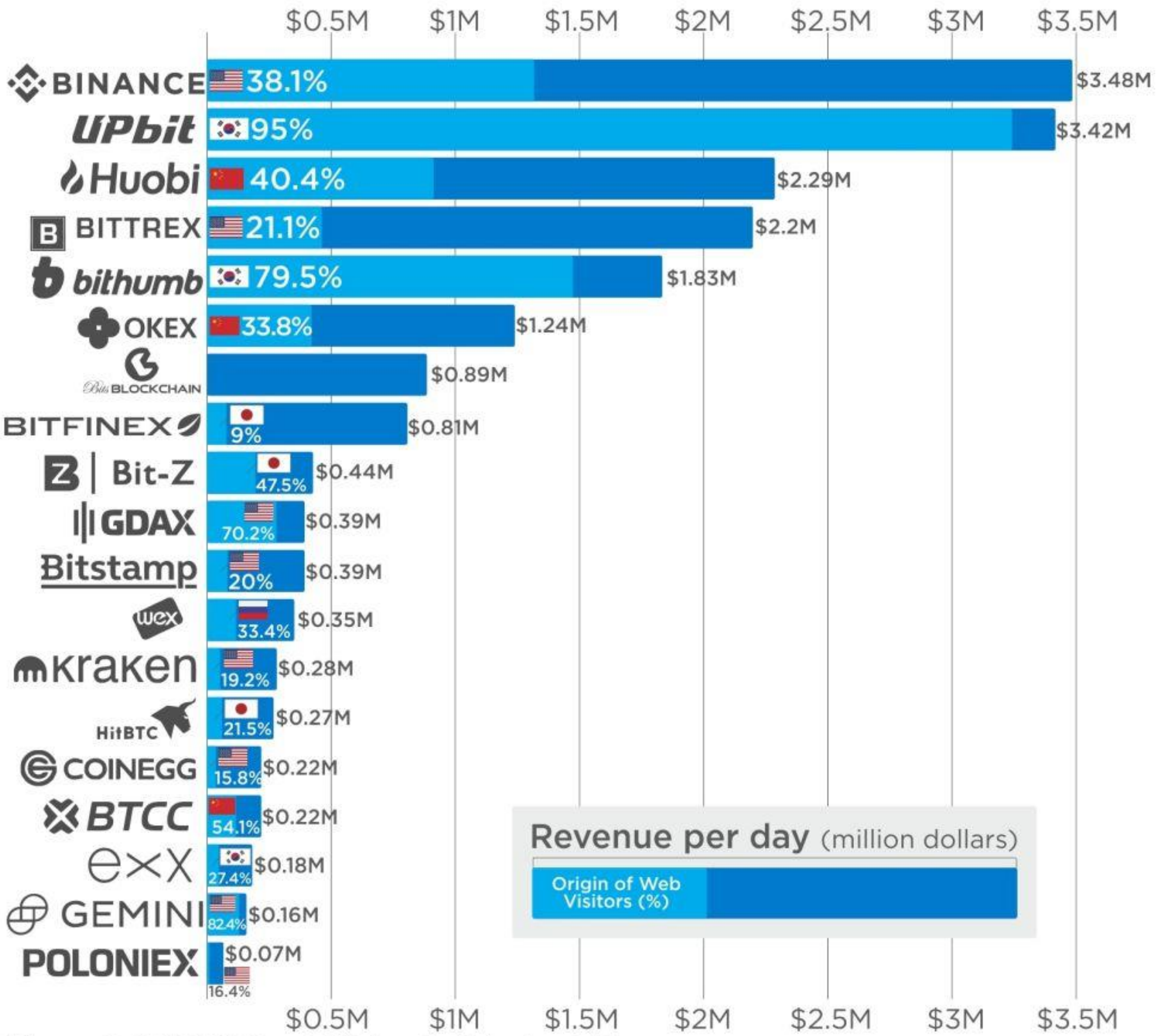
249.9 mBTC
~USD 184.43
Receiving 25 mBTC

1 BTC ~ USD 738.00 (Bitstamp)



12/2/15	Confirmed	0.01013966 BTC	4.65 USD
12/2/15	Confirmed	0.05070563 BTC	23.27 USD
12/1/15	Confirmed	0.01004105 BTC	4.61 USD
12/1/15	Confirmed	0.05002416 BTC	22.96 USD
10/28/15	Confirmed	0.00095825 BTC	0.44 USD
10/28/15	Confirmed	0.00104175 BTC	0.48 USD
10/15/15	Confirmed	0.00844345 BTC	3.88 USD
10/15/15	Confirmed	0.00997425 BTC	4.58 USD
10/15/15	Confirmed	0.01009398 BTC	4.63 USD
10/15/15	Confirmed	0.001 BTC	0.46 USD
10/15/15	Confirmed	0.00092 BTC	0.42 USD
10/15/15	Confirmed	0.00109398 BTC	0.50 USD
9/21/15	Confirmed	0.1499 BTC	68.80 USD
9/21/15	Confirmed	0.03759419 BTC	17.25 USD
9/21/15	Confirmed	0.03759419 BTC	17.25 USD
9/21/15	Confirmed	0.03759419 BTC	17.25 USD
9/21/15	Confirmed	0.1499 BTC	68.80 USD

Crypto Exchanges' Trading Revenue Per Day



* Daily revenue estimated with CoinMarketCap reported 24Hr volume and fees listed on exchanges' websites.

** Percent of visitors estimated by Alexa.com. It does not necessarily represents the % of revenue but only the % of web visitors.

Article & Sources:
https://howmuch.net/articles/crypto-exchanges-revenue
https://www.bloomberg.com
https://www.alexa.com

howmuch net

Coin Exchange

- What is a coin exchange.
- It provides service for good exchanges just like humanity did in ancient times.
- The assets for exchanges were rice, shells, and fish in ancient times.
- For cryptographic coins exchanges, the assets are the cryptocurrencies.
- Exchanges let users buy and sell coins for fiat money or altcoins.
- Exchanges many hold a significant amount of coins.
- They act as wallet providers.
- Users put a deposit who wish to trade.
- An exchange works because there are sellers and buyers.

Example TX at CryptoXchange

- Reference for further reading: page 112 ~ 114, Princeton_bitcoin_book.pdf.

- Suppose Alice holds 5000 dollars and three bitcoins in her account at CXchange .
- Bob holds 2000 dollars and four bitcoins in his account at CXchange .
- Alice put an order to buy 2 bitcoins at 500 dollars each. Fee is 10 dollars, 1% of TX money.
- Bob put an order to sell 2 bitcoins at a price above or equal to 500 dollars each. Fee is 10 dollars, 1% of TX money.
- CXchange matches up Alice and Bob and completes the transaction.
- After the match up transaction is completed, their account balances are changed to
- Alice has five bitcoins and 3990 dollars in her account.
- Bob has two bitcoins and 2990 dollars in his account

- Note here that no transactions have actually happened on the Bitcoin blockchain.
- All CXchange has done is changing the numbers in each account.
- It did not have to go through the blockchain to complete these exchange transactions. All it had done is to find the matchups.
- This practive of business is probably o.k. as long as the account holders at CXchange are satisfied. The exchange can have them satisfied as long as it retains the ability to give the money back in the account when it was asked to.

Kimchi premium, why?

- It is defined as the gap in bitcoin price in Korean exchanges compared to foreign exchanges.
- In December 2017, the demand for buying bitcoin in South Korea was at the peak.
- South Koreans has to pay a higher price for bitcoins than traders in other countries.
- This phenomenon was called the "kimchi premium." Kimchi is a Korean traditional side dish, fermented cabbage.
- The price difference was more than 40%, Korean bitcoin price was higher than the price in the United States.
- Investors can take the advantage of arbitrage.
- South Korean traders would first have to exchange the Korean won for a the U.S. dollar, to purchase a bitcoin on a US cryptocurrency exchange.
- Foreign investors would simply have to purchase bitcoins abroad and sell them on a South Korean exchange. The draw of profit should have eliminated this gap arbitrage, but capital controls, financial regulations, and anti-money laundering laws make the process difficult.
- South Koreans and South Korean firms are limited to the amount of money they can move out of the country each year, and the transfer must be approved by regulators. Regulators are likely to block the transfer for fear that it is really being made to launder money.
- Even if regulators approved of the transfer, it may take so much time that the arbitrage opportunity is no longer available. Capital controls also limit the inflow of cryptocurrencies by foreign investors. This has created a scenario in which digital currencies can only be traded in South Koreans by South Koreans.
-

  Read more: Kimchi Premium Definition | Investopedia https://www.investopedia.com/terms/k/kimchi-premium.asp#ixzz5C5OJLbhF
  Follow us: Investopedia on Facebook

‘주식 공매도 금지’ 청와대 국민청원 20만 돌파

- 삼성증권 우리사주 배당 사고와 관련해 삼성증권을 규제하고 공매도(없는 주식을 빌려 파는 것)를 금지해 달라는 청와대 국민청원 참여자가 20만 명을 넘어섰다.
- 청원 게시자는 지난 6일 ‘삼성증권 시스템 규제와 공매도 금지’라는 제목의 청원에서 “삼성증권의 발행 한도는 1억2천만 주인데 우리사주 1주당 1천 주씩 총 28억 주가 배당됐고 500만 주가 유통됐다”며 “이는 없는 주식을 배당하고, 그 없는 주식이 유통될 수 있다는 이야기로 주식을 빌리지 않고도 공매도 할 수 있다는 이야기가 된다. 서민만 당하는 공매도를 꼭 폐지하고 이를 계기로 증권사의 대대적인 조사를 바란다”고 적었다. 이 청원은 10일 오후 2시께까지 20만5천여명이 참여했다. 삼성증권은 지난 6일 직원들이 보유한 우리사주 283만1620만 주를 대상으로 1주당 1천 원씩 배당금을 주기로 했으나, 직원의 입력실수로 1주당 1천 주를 배당하는 사고를 냈다. 삼성증권 직원들은 이때 28억3천만 주 가량을 배당받았고, 이들 가운데 16명은 500만 주 이상 매도해 6일 삼성증권 주가가 장중 11.68% 포인트 급락한 바 있다.

- 성연철 기자 sychee@hani.co.kr
- 원문보기: http://www.hani.co.kr/arti/politics/bluehouse/839923.html#csidxb130b1b996922a7839eb7fd442fa0f0

공매도란

- Short Selling (공매도): 없는 것은 판다는 의미. 개인 혹은 단체가 주식, 채권 등을 보유하지 않은 상태에서 매도하는 행위를 말한다. 하락장에서 쓰는 투자 수단. https://ko.wikipedia.org/wiki/%EA%B3%B5%EB%A7%A4%EB%8F%84

- 영어로 된 definitio이 조금 순화 된 느낌을 준다.

- **What is a 'Short (or Short Position)'**
- A short, or short position, is a directional trading or investment strategy where the investor sells shares of borrowed stock in the open market. The expectation of the investor is that the price of the stock will decrease over time, at which point the he will purchase the shares in the open market and return the shares to the broker which he borrowed them from.
- **What is a 'Long (or Long Position)'**
- A long (or long position) is the buying of a security such as a stock, commodity or currency with the expectation that the asset will rise in value. In the context of options, long is the buying of an options contract. An investor that expects an asset's price to fall will go long on a put option, and an investor that hopes to benefit from an upward price movement will be long a call option.

Why is Short Selling Legal? A Brief History

By Adam Hayes, CFA | Updated August 9, 2016 — 11:19 AM EDT

Short Selling Becomes Legitimate

- The SEC adopted Rule 10a-1in 1937, the uptick rule, which stated market participants could legally sell short shares of stock only if it occurred on a price uptick from the previous sale.
- Despite its new legal status and the apparent benefits of short selling, many policymakers, regulators – and the public – remained suspicious of the practice. Being able to profit from the losses of others in a bear market just seemed unfair and unethical to many people.
- The SEC eventually eliminated the uptick rule in 2007 following a years-long study which concluded that the regulation did little to curb abusive behavior and had the potential to limit market liquidity.

The "Naked" Short Sale is banned by SEC in 2009, as a means to driving price down.

- The seller must "locate" shares to sell to avoid "selling shares that have not been affirmatively determined to exist." In the U.S., broker-dealers are required to have reasonable grounds to believe that shares can be borrowed so they can be delivered on time before allowing such a short sale. Executing a naked short runs the risk that they will not be able to deliver those shares to whomever the receiving party in the short sale. Another prohibited activity is to sell short and then fail to deliver shares at the time of settlement with the intent of driving down an asset’s price. (For more, see: The Truth About Naked Short Selling.)

Read more: Why is Short Selling Legal? A Brief History |Investopedia https://www.investopedia.com/articles/investing/110614/why-short-selling-legal-brief-history.asp#ixzz5CcvmxZv1

ISSUES
Reforming Wall Street

Wall Street cannot continue to be an island unto itself, gambling trillions in risky financial decisions while expecting the public to bail it out.

It is time to break up the largest financial institutions in the country.

The six largest financial institutions in this country today hold assets equal to about 60% of the nation's gross domestic product. These six banks issue more than two thirds of all credit cards and over 35% of all mortgages. They control 95% of all derivatives and hold more than 40% of all bank deposits in the United States. We must break up too-big-to-fail financial institutions. Those institutions received a $700 billion bailout from the US taxpayer, and more than $16 trillion in virtually zero interest loans from the Federal Reserve. Despite that, financial institutions made over$152 billion in profit in 2014 – the most profitable year on record, and three of the four largest financial institutions are 80% bigger today than they were before we bailed them out. Our banking system must be part of the productive, job-creating economy. The Federal Reserve, a government entity which serves as the engine of the banking industry, must eliminate its internal conflicts of interest, provide stricter oversight, and insist that the banks serve the economy in a way that works for everyone, not just a few.

If a bank is too big to fail, it's too big to exist. Today I introduced legislation to break up the big banks.
– Sen. Bernie Sanders
SHARE IF YOU AGREE | SANDERS.SENATE.GOV

The Evolution of Trust

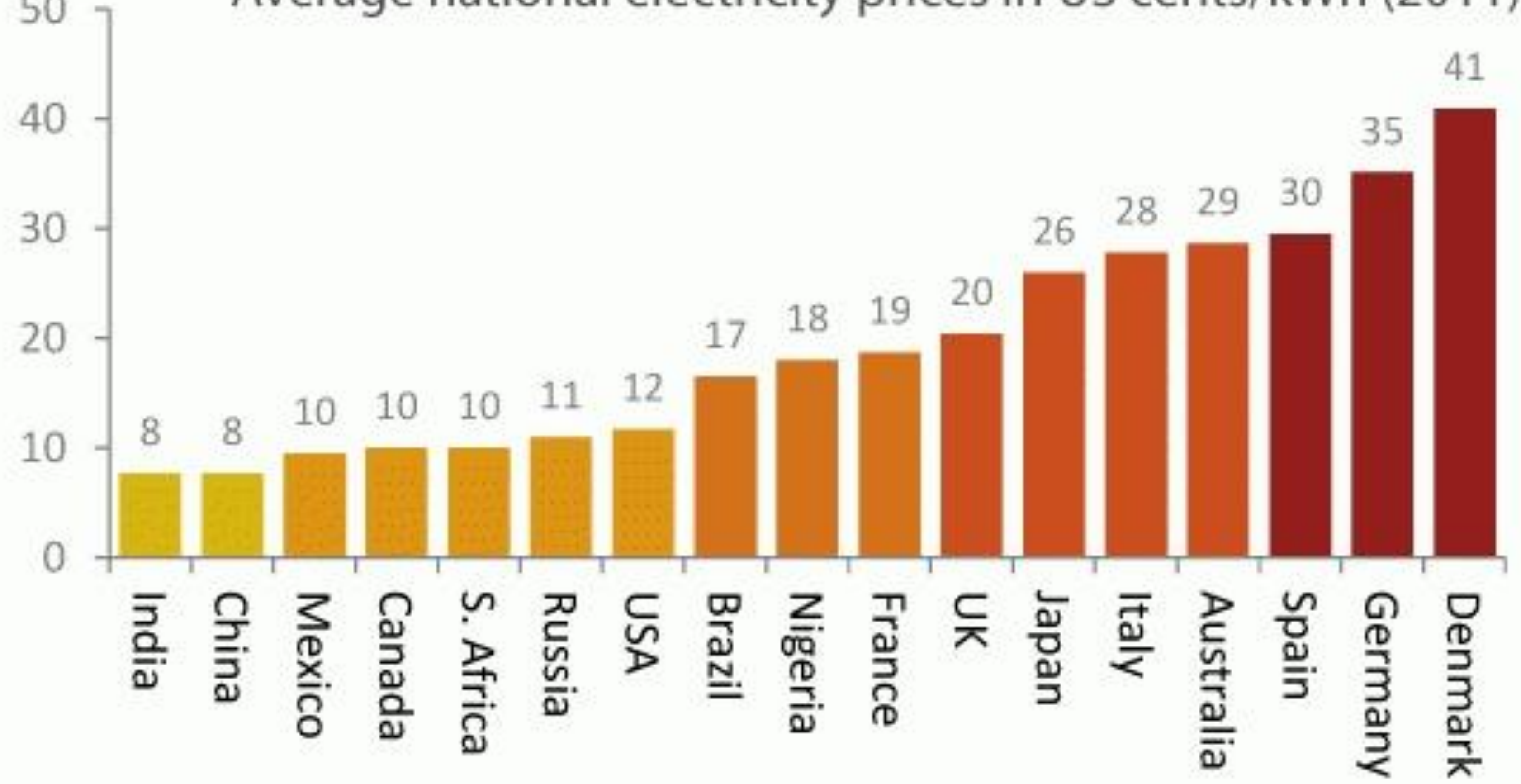
***Scientific American* 318, 38 - 41 (2018)**
Published online: 19 December 2017
| doi:10.1038/scientificamerican0118-38

Natalie Smolenski

- Banks and governments have in many ways failed to broker trust for the global economy, especially in the past few decades. Ordinary people have grown wary of centralized power and are seeking alternatives.
- Bitcoin—and blockchain technology in general—allows the brokering of trust to be shifted toward machines and away from human intermediaries such as bankers. This technology could design exploitation out of the system instead of punishing it later.
- Blockchains lend themselves both to human emancipation and to an unprecedented degree of surveillance and control. How they end up being used depends on how the software handles digital identity.

How much does electricity cost?

Average national electricity prices in US cents/kWh (2011)

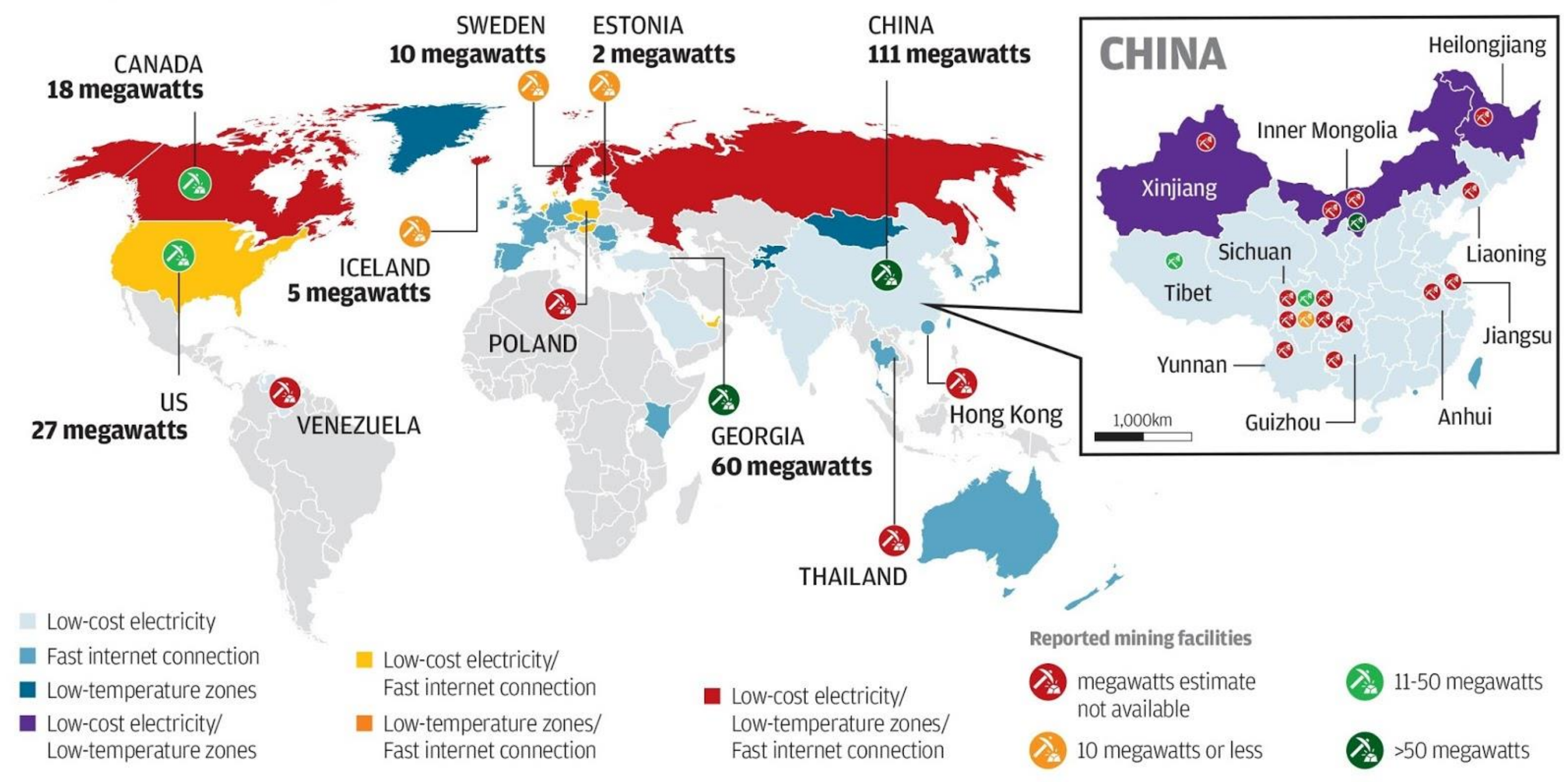


Data: average prices from 2011 converted at mean exchange rate for that year

Sources: IEA, EIA, national electricity boards, OANDA shrinkthatfootprint.com

PoW, Monopolized?

Global cryptocurrency mining sites

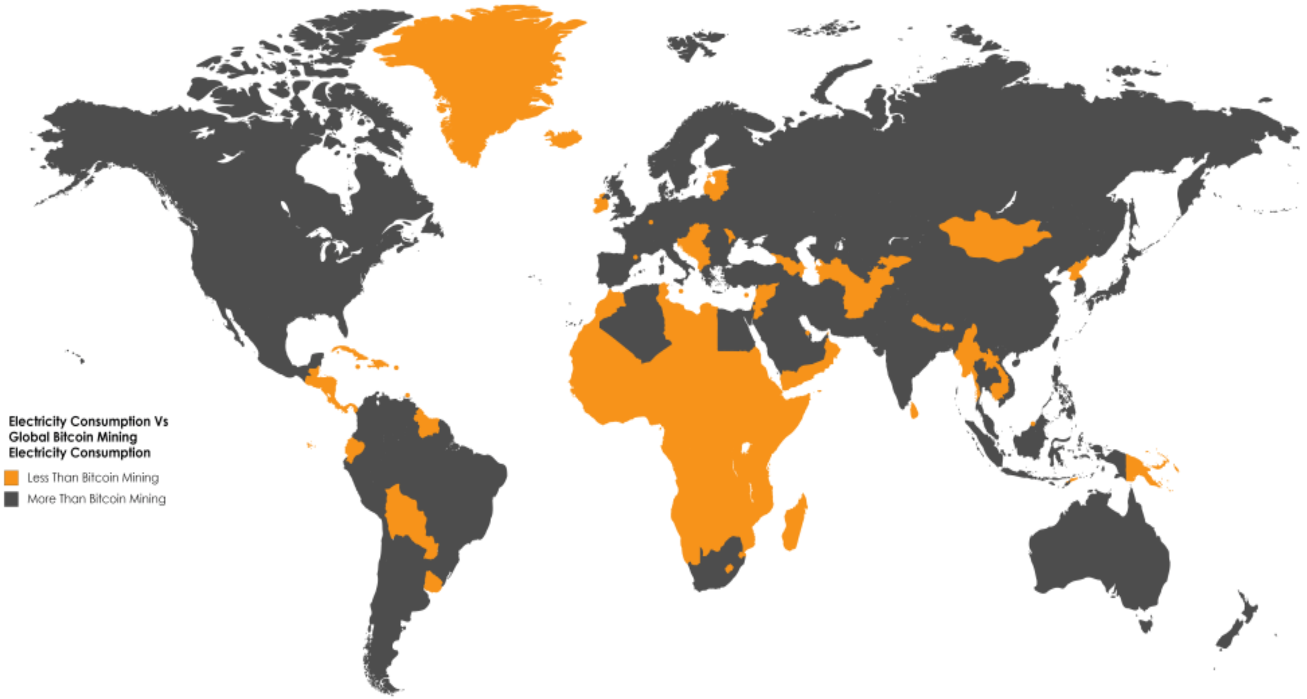


Source: University of Cambridge

SCMP

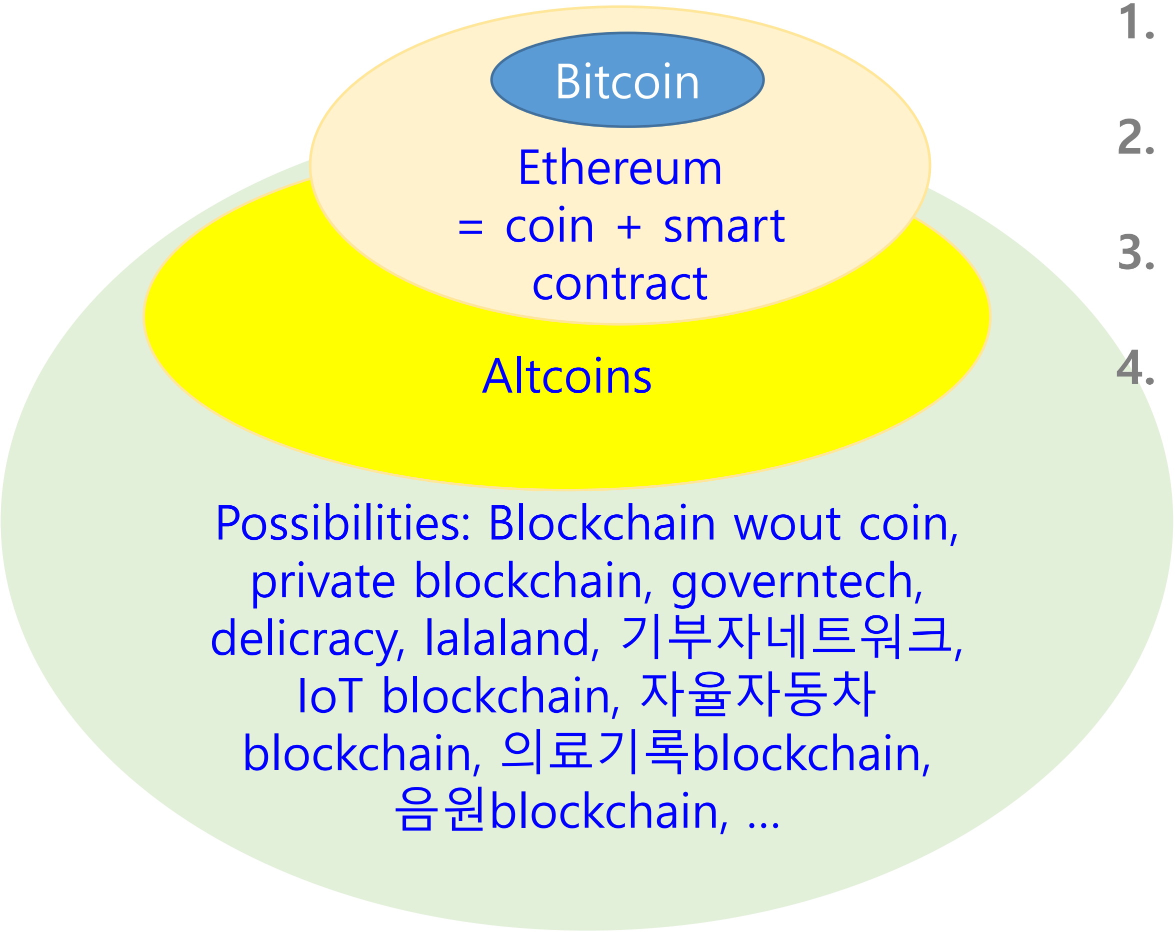
Energy spending for bitcoin mining exceeds energy consumption of a country

According to Bitcoin analysis blog Digiconomist, **energy consumed by Bitcoin mining now exceeds what is used by countries like Ireland, Hungary, Oman, and Lebanon**. Bitcoin uses about as much power as the entire country of Morocco and slightly less than Bulgaria. If Bitcoin were a country, it would have the 61st highest energy consumption. However, this only covers miners. It does not include any power consumed by Bitcoin-enabled devices like vending machines and ATMs.


Electricity Consumption Vs
Global Bitcoin Mining
Electricity Consumption
🟧 Less Than Bitcoin Mining
⬛ More Than Bitcoin Mining

Source: https://powercompare.co.uk/bitcoin/

Hypes vs Revolutionary ideas

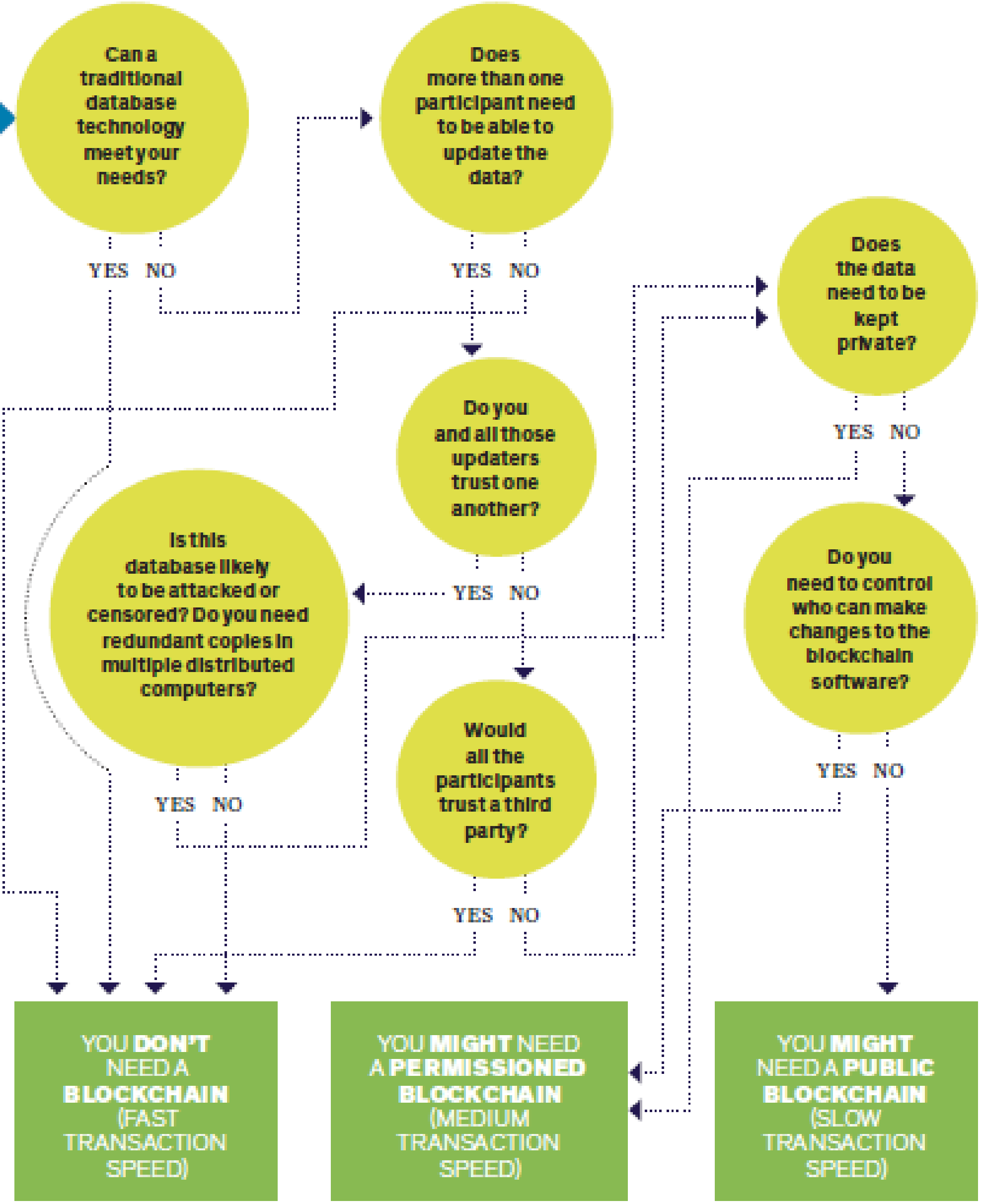

Bitcoin
Ethereum
= coin + smart
contract
Altcoins
Possibilities: Blockchain wout coin,
private blockchain, governtech,
delicracy, lalaland, 기부자네트워크,
IoT blockchain, 자율자동차
blockchain, 의료기록blockchain,
음원blockchain, …

Questions to ask

1. Who's developing the system?
2. How long should operate?
3. Who's doing the maintenance work?
4. Is blockchain the right solution for your objective?

I Want a Block-chain!

DO YOU REALLY NEED a blockchain? They can do some amazing things, but they are definitely not the solution to every problem. Asking yourself a handful of the questions on this chart can set you on the right path to an answer. You'll note that there are more reasons not to use a blockchain than there are reasons to do so. And if you do choose a blockchain, be ready for slower transaction speeds.



Can a traditional database technology meet your needs?

YES NO

Does more than one participant need to be able to update the data?

YES NO

Do you and all those updaters trust one another?

YES NO

Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?

YES NO

Would all the participants trust a third party?

YES NO

Does the data need to be kept private?

YES NO

Do you need to control who can make changes to the blockchain software?

YES NO

YOU **DON'T** NEED A **BLOCKCHAIN** (FAST TRANSACTION SPEED)

YOU **MIGHT** NEED A **PERMISSIONED BLOCKCHAIN** (MEDIUM TRANSACTION SPEED)

YOU **MIGHT** NEED A **PUBLIC BLOCKCHAIN** (SLOW TRANSACTION SPEED)

Bitcoin Summary

- Bitcoin is an electronic cash.
- This e-cash can be used to transfer the ownership a coin, via a chain of signatures.
- A fixed amount of bitcoins are created in each block.
- Created bitcoins for a block are given to the miner who has succeeded in finding the nonce value for the pertinent block.
- In fact, the miner has the right to produce a fixed amount of bitcoin and give it to one of his own bitcoin address.
- Each created bitcoin belongs to a bitcoin address.
- Ownership rights are transferred from payer bitcoin address to the payee bitcoin address.
- A transaction is valid only when it is attached with a digital sign.
- A valid digital sign shows the proof of ownership of the pertinent coin.
- Miners are the ones who verify the digital signs and make sure to see if the pertinent coin is not already spent.
- Miners put valid transactions to a block and find a good hash for the block.
- The miner who found a valid block summary is given the right to generate the bitcoin.
- Bitcoin is an electronic cash system which runs without the third party such as mint or bank.
- In Bitcoin, however, the third party is the network of miners who verify the validity of each transaction and scribing validated transactions into the blockchain.
- The miners are decentralized and autonomous. Anyone can join as a miner. They simply need to buy mining chips, connect to the open Bitcoin network, and become a miner (person). Anytime these miners can stop working as a miner any time.

Issues

- Minor monopoly, not truly decentralized
- Problems with electric energy spending
- What happens when there are no block mining reward?
- Regulations
  - Coin Exchanges
  - Developers

Conclusion

- Many Possibilities of Blockchain
- Verified by the market are Bitcoin
- To explore new territory, experiments are needed

  with budgets and man power invested.
- Needed are the research on regulation as regulations should be kept at the minimal level and more emphasis shall be on innovation.
- There are many research issues
  - Scalability
  - Speed of transaction
  - Privacy
  - Anonymity
  - Autonomous
  - Decentralization
  - Energy consumption
  -

References

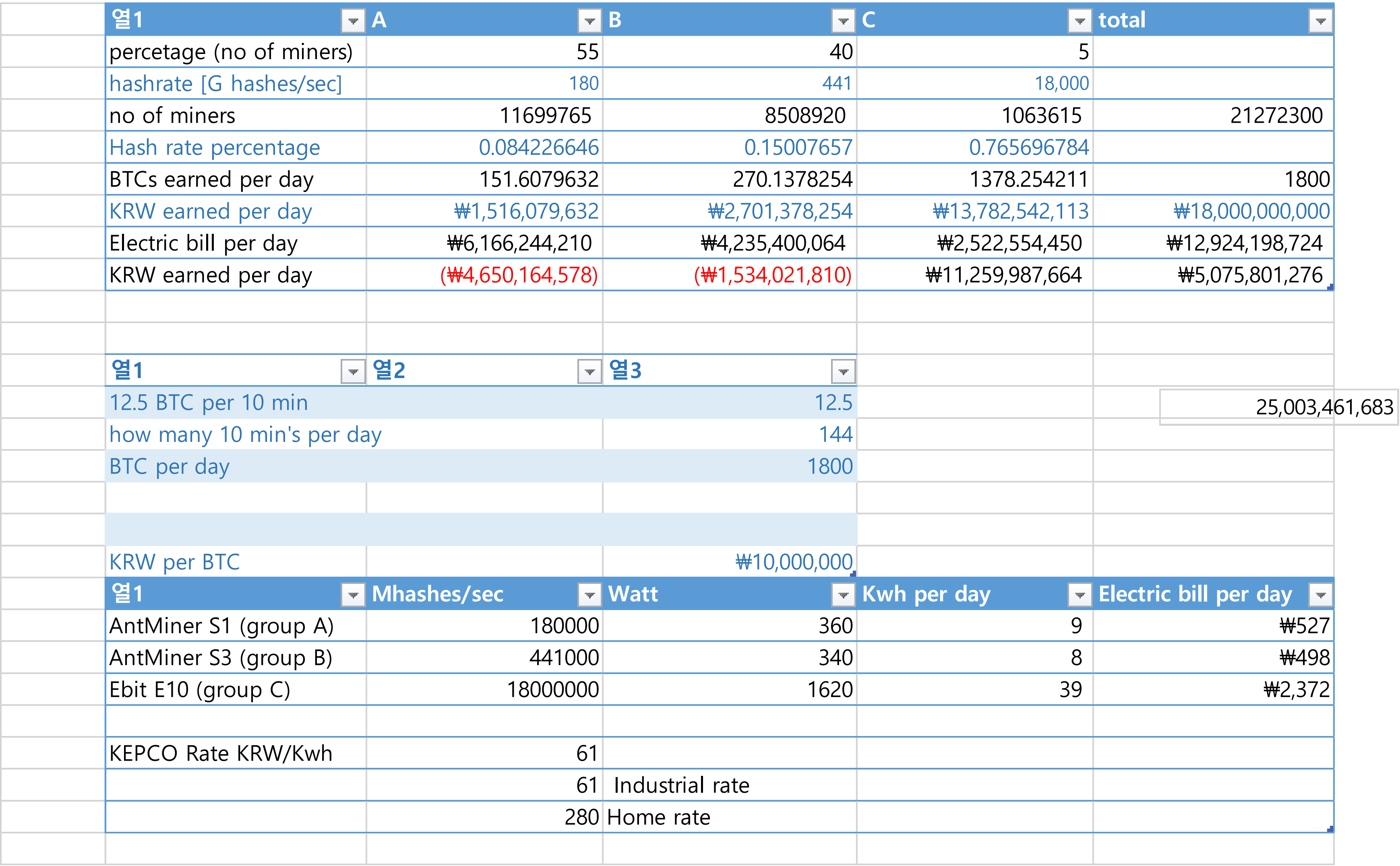
- 이흥노 교수 랩 블록체인페이지 https://infonet.gist.ac.kr/?page_id=6370.
- Blockchain.net
- Bitcoin.org
- Coursera course on Cryptocurrencies
- MIT Blockchain center
- Blockchain A beginner's guide, Blockchain Hub
- Satoshi Nakamoto's Bitcoin white paper.
- 그 외

HW#1

- Problem 1: Suppose that there are only three groups of bitcoin miners in the bitcoin network.
- The first group A uses AntMiner S1 miners, second group B uses AntMiner S3, third group C uses Ebit E10.
- The percentage of each group is 1st 55%, 2nd 40%, and the third 5% in terms of numbers of miners.
- Provide an estimation on the total number of miners working in the bitcoin network today March 14th 2018.
- Give the number of miners in each group.
  - Use the reference for ASIC miners at https://en.bitcoin.it/wiki/Mining_hardware_comparison.
  - Use the estimated hashrate published at (https://bitcoinwisdom.com/bitcoin/difficulty).

- Problem 2: Use the setting from Problem 1. Find the probability of mining success per block or the percentage of the mining success per block of group C.
- What is the estimate amount of money the group C pays for electricity bill per day?
- What is the amount of money the group expects to earn for a day?
- Find the average rate at the on-line information post at Kepco and provide your source.
- Use this and give an estimate of the energy spent per day the bitcoin network consumes.

Solutions to Prob 1 & Prob 2



열1	A	B	C	total
percetage (no of miners)	55	40	5	
hashrate [G hashes/sec]	180	441	18,000	
no of miners	11699765	8508920	1063615	21272300
Hash rate percentage	0.084226646	0.15007657	0.765696784	
BTCs earned per day	151.6079632	270.1378254	1378.254211	1800
KRW earned per day	₩1,516,079,632	₩2,701,378,254	₩13,782,542,113	₩18,000,000,000
Electric bill per day	₩6,166,244,210	₩4,235,400,064	₩2,522,554,450	₩12,924,198,724
KRW earned per day	(₩4,650,164,578)	(₩1,534,021,810)	₩11,259,987,664	₩5,075,801,276

열1	열2	열3
12.5 BTC per 10 min		12.5
how many 10 min's per day		144
BTC per day		1800
KRW per BTC		₩10,000,000

25,003,461,683

열1	Mhashes/sec	Watt	Kwh per day	Electric bill per day
AntMiner S1 (group A)	180000	360	9	₩527
AntMiner S3 (group B)	441000	340	8	₩498
Ebit E10 (group C)	18000000	1620	39	₩2,372
KEPCO Rate KRW/Kwh	61			
	61	Industrial rate		
	280	Home rate		

HW#1

- Problem 5. Use Satoshi's paper and my lecture note #1 for these answers. Two or three line answers for each shall be enough.

(a) What is the definition of bitcoin?

(b) What is the double spending problem? How is it resolved in bitcoin network?

(c) What is the timestamp server?

(d) Write down your reasoning why blockchain provides data immutability.

(e) Is the data stored in blockchain really immutable?

(f) What is the kind of attack the bitcoin paper says is possible?

(g) Write down the sequence of events to mine a block?

(h) List the field types that needs to be recorded inside the blockheader?

(i) What is the byte size of the private and that of the public key used in Bitcoin?

(j) What is the meaning of signature in Satoshi's paper?

(k) Bob wants to send Alice a bitcoin. What are the three basic things that must be done to complete this transaction?

(l) Why do we need proof-of-work in bitcoin network?

(m) What is the benefit of eliminating the third party according to Satoshi?

(n) Who is doing the proof-of-work in bitcoin network?

(o) What is a hash cycle?

HW#1

- Problem 6

a. Define what a money is. Provide your source.

b. Define what currency is. Provide your source.

c. What is the current market price of a bitcoin? Is it expensive or cheap? Justify your answer.

d. Bitcoin intends to get rid of the bank and uses P2P network instead. What are the possible benefits of using P2P network, instead of a bank? What are the possible drawbacks? Justify your answer.

e. Does the fiat money such as KRW and USD have any intrinsic value? Why do you think they have a market value? Who or what decides their values?

Quiz #1

- Problem 1 (5pts) What is nonce in bitcoin? How is it used? Why do you need it?

- Problem 2 (5pts) In the bitcoin system, what do we mean by data immutability? Is it really immutable? If yes, how is it done? Justify your answer.

Cryptocurrency Economy

전자공학회

@숭실대학교

April 19, 2018

박창기

(사) 블록체인산업진흥협회 회장

ckfrpark@gmail.com

1st Generation

Cryptocurrency

Bitcoin

bitcoin

decentralized

Global Single Bank

Blockchain 1.0

Cryptocurrenies

disrupts

Fiat Money & Banks

BN·AMRO
People's United Bank
Standard Chartered
BB&T
First National
KeyBank
TD Bank
JPMorganCh
eWest Bank
QNB
Your Community Bank
bank
Bank of America
BBVA Compass
Comerica Bank
BNP
COMMERZBANK
Santander
BridgeBank
RBS
The Royal Bank of Scotland
NATIONAL BANK
EMBASSY BANK
Associated Bank
SBERBANK
bank
Westpac
ROCKLAND TRUST
HSBC
Bank
First Interstate
Cambridge Trust Company
Capital One
bank
SVB
ANZ
LLOYDS BANK
PNC
BROWN BROTHERS HARRIMAN
Alfa-Ba
ZIONS BANK
Sierra Vista BANK
M&T Bank
citibank

2nd Generation

Cryptocurrency

Ethereum

ETHEREUM

decentralized

Global Single Computer

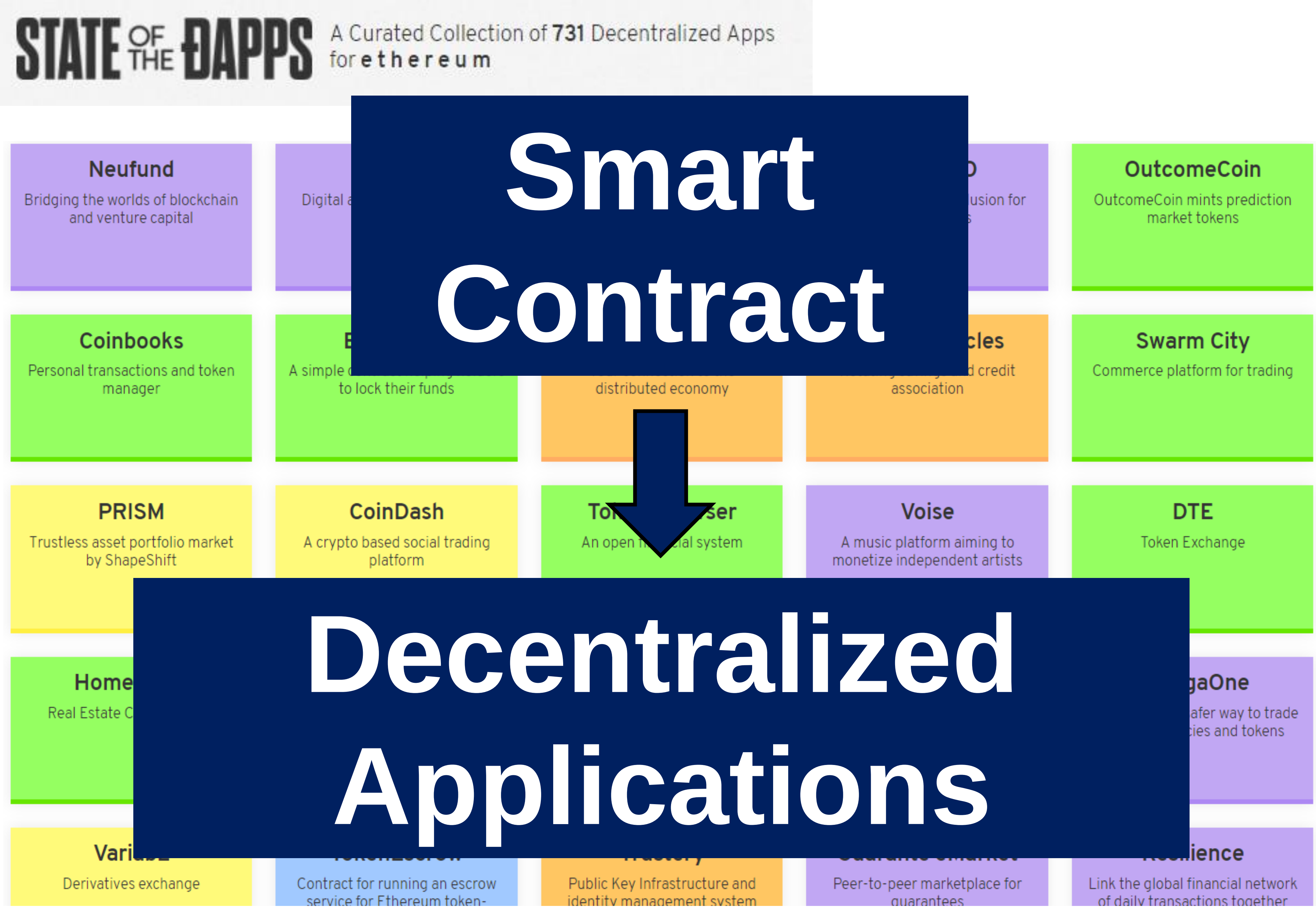
Blockchain 2.0

Smart Contract

1
<CONTRACT>
2
3
4
5
6
7
*
*
*
19
20
</CONTRACT>

dApps

Decentralized Applications



Smart Contract

Decentralized Applications

STATE OF THE ÐAPPS A Curated Collection of 731 Decentralized Apps for ethereum

Neufund
Bridging the worlds of blockchain and venture capital

Digital a

D
usion for
s

OutcomeCoin
OutcomeCoin mints prediction market tokens

Coinbooks
Personal transactions and token manager

E
A simple
to lock their funds

distributed economy

cles
d credit association

Swarm City
Commerce platform for trading

PRISM
Trustless asset portfolio market by ShapeShift

CoinDash
A crypto based social trading platform

To ser
An open fi cial system

Voise
A music platform aiming to monetize independent artists

DTE
Token Exchange

Home
Real Estate C

gaOne
afer way to trade
cies and tokens

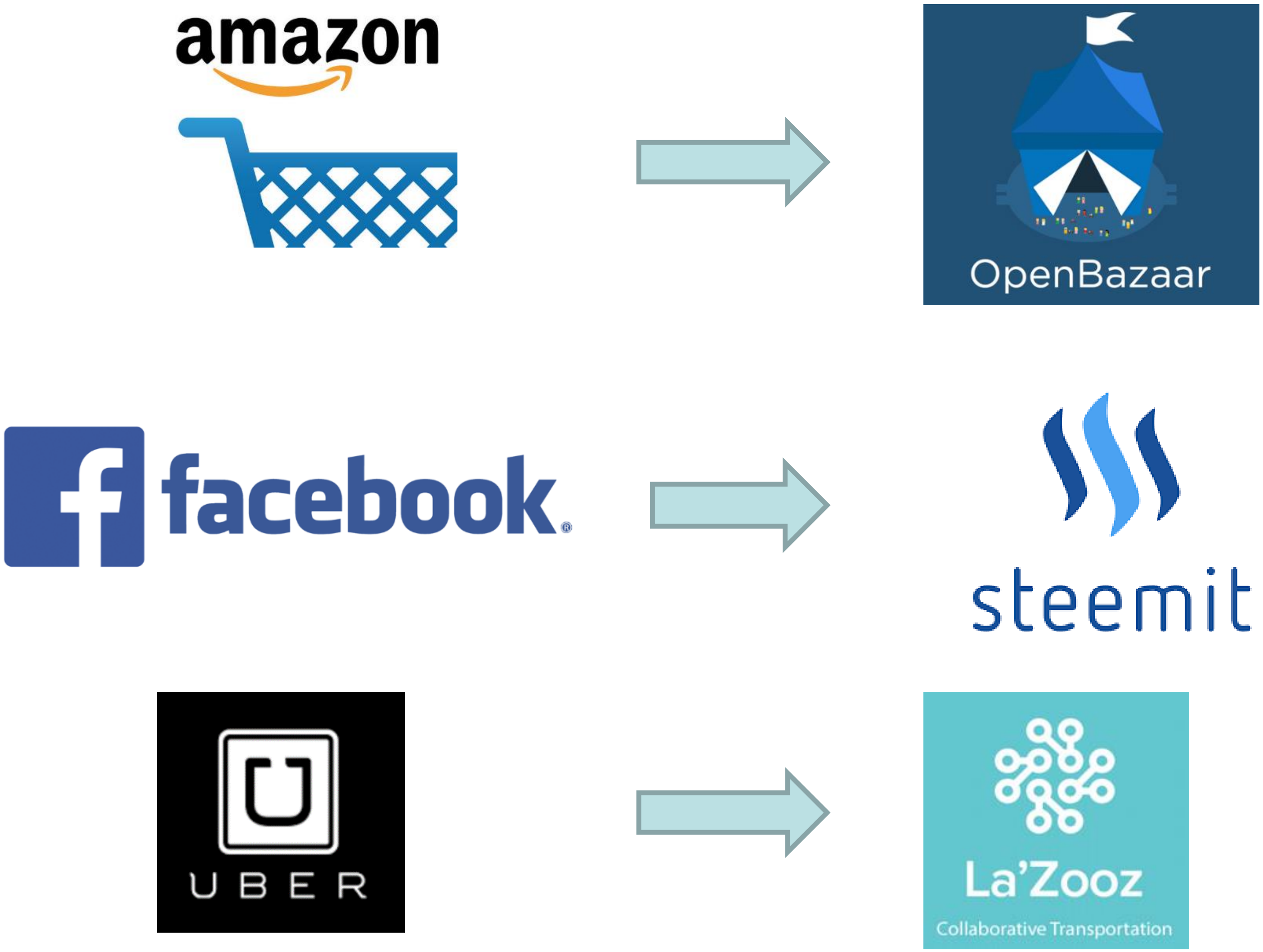
Vari
Derivatives exchange

Contract for running an escrow service for Ethereum token-

Public Key Infrastructure and identity management system

Peer-to-peer marketplace for guarantees

ilience
Link the global financial network of daily transactions together


amazon
OpenBazaar
facebook
steemit
UBER
La'Zooz
Collaborative Transportation

Global Single Computer

Smart contracts

disrupts

Nation State & Government

ORDEM E PROGRESSO

Nation State

Fiat Money
+ Legal codes
+ Land + People

Cyber Nation

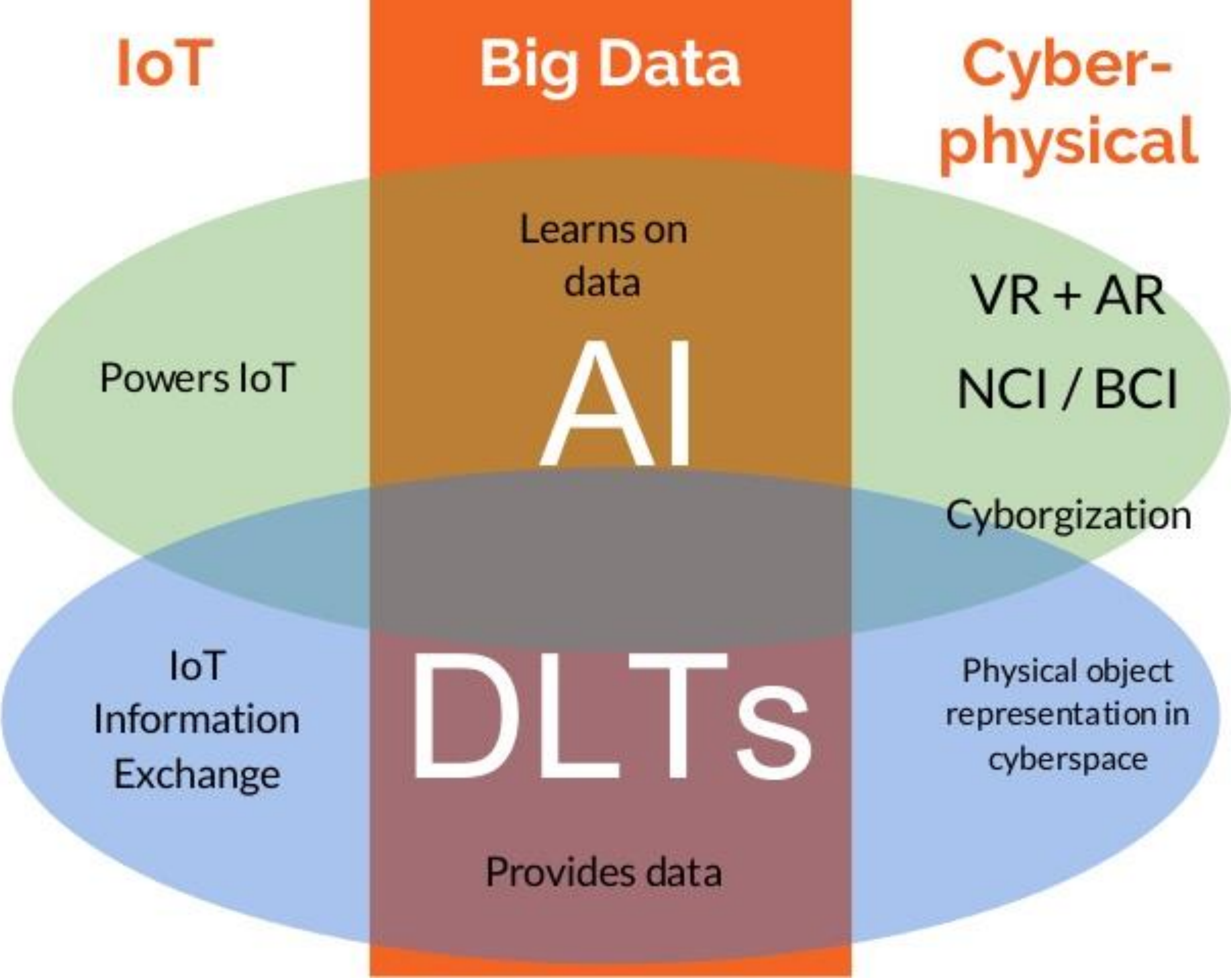
Cryptocurrency
+ Smart Contract codes
+ Cyber Space

City of Industry 4.0

- IoT
- Hyper connected, automated
- M2M Comm’n

→ Smart contract

→ Cryptocurrency



IoT

Big Data

Cyber-physical

Learns on data

AI

Powers IoT

VR + AR

NCI / BCI

Cyborgization

DLTs

IoT

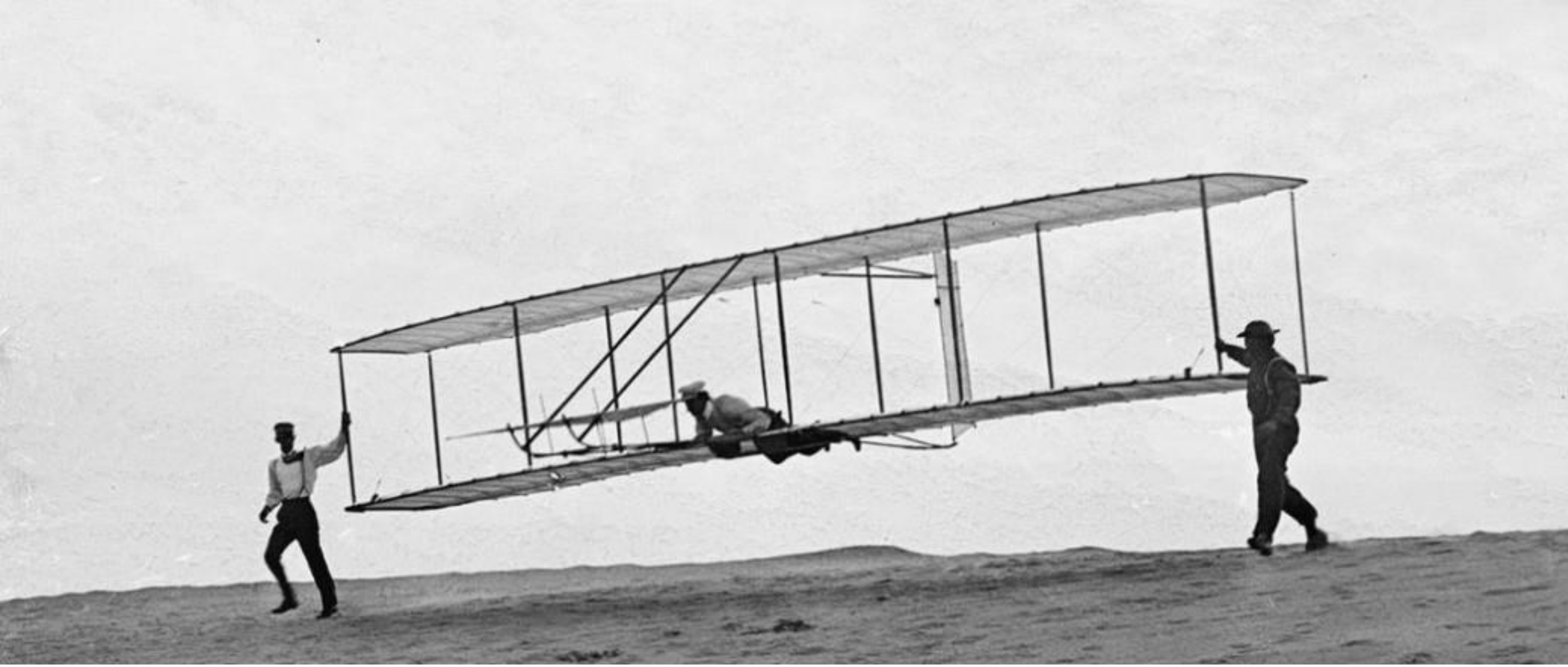
IoT Information Exchange

Physical object representation in cyberspace

Provides data

Blockchain City, Why?

1. Anti Cyber-terror & Hacking
2. Trust from Distributed Ledger
3. Decentralized Governance
4. Small Govern’t → Low Tax



bitcoin

Blériot XI

ETHEREUM

Bitcoin & Ethereum

Slow & expensive

Scalability problems

Not easy to upgrade

No good governance

Not easy to use

Lost & theft

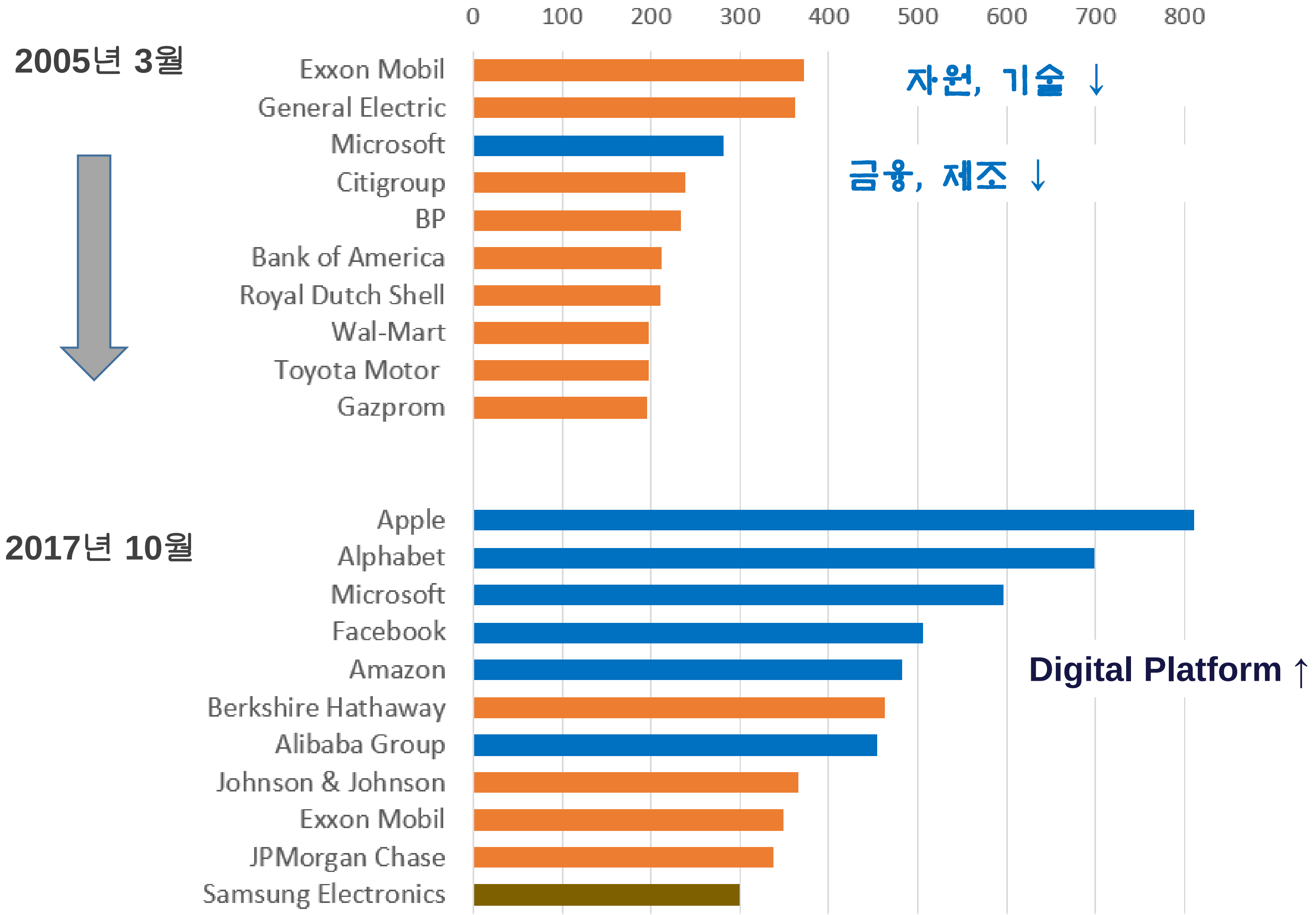
Re-centralized

3rd Generation Cryptocurrency

Blockchain 3.0

Platform Economics

시가총액 상위 종목의 변화



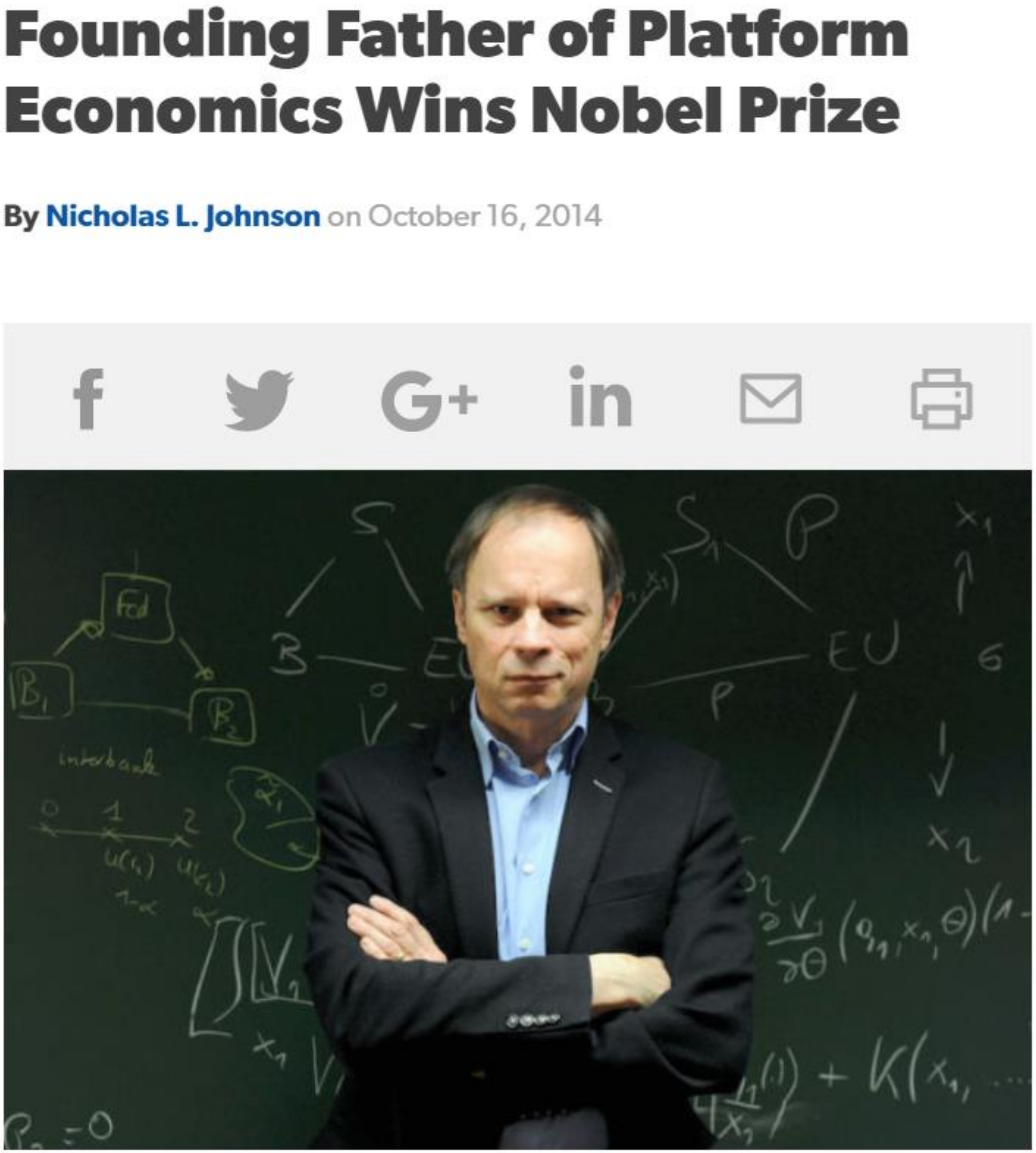
2005년 3월

2017년 10월

자원, 기술 ↓

금융, 제조 ↓

Digital Platform ↑



Founding Father of Platform Economics Wins Nobel Prize

By Nicholas L. Johnson on October 16, 2014

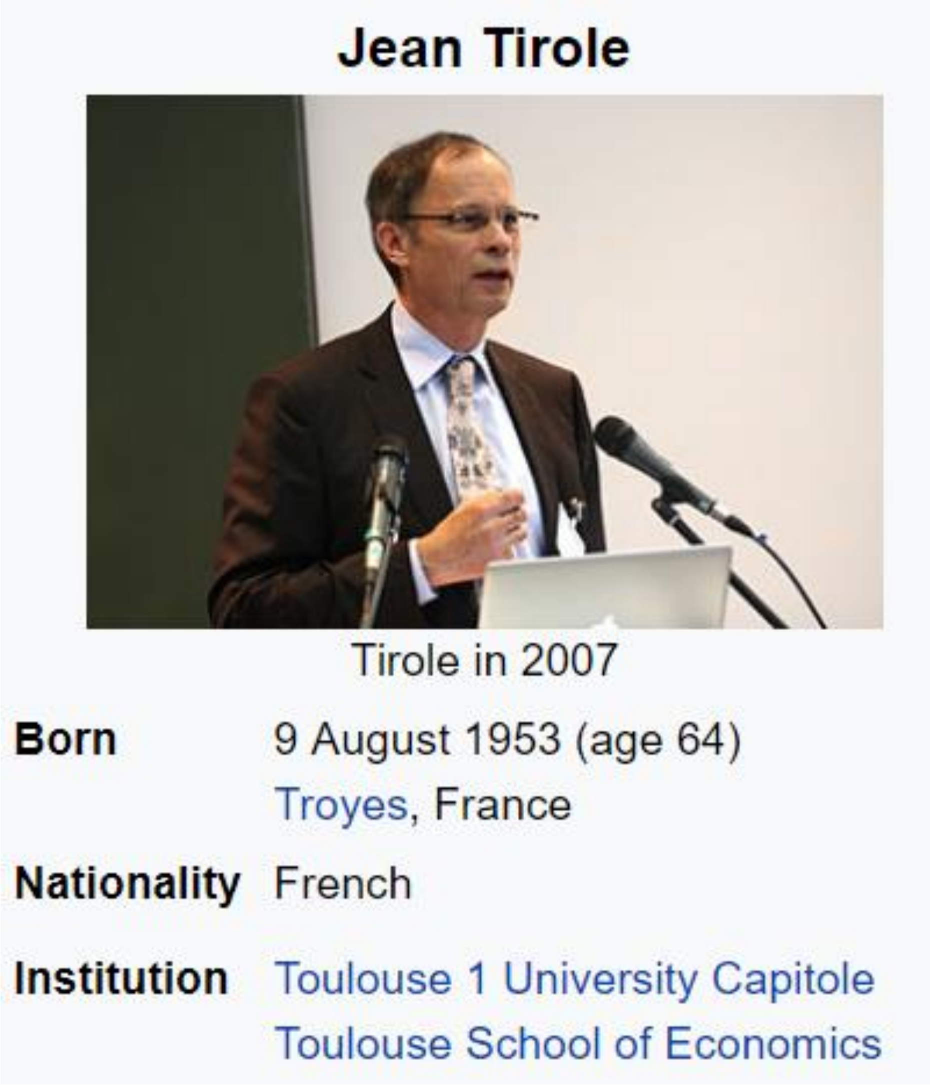
2014 Novel Prize

Economics

Game Theory

Analysis of

market power and regulation

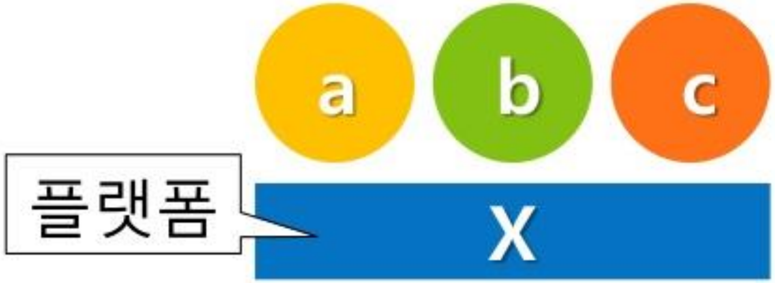


Jean Tirole

Tirole in 2007

Born	9 August 1953 (age 64) Troyes, France
Nationality	French
Institution	Toulouse 1 University Capitole Toulouse School of Economics

Platforms



a

b

c

플랫폼

X

$$aX + bX + cX = (a+b+c)\ X$$

X | 기차역, win OS, **공통역량**

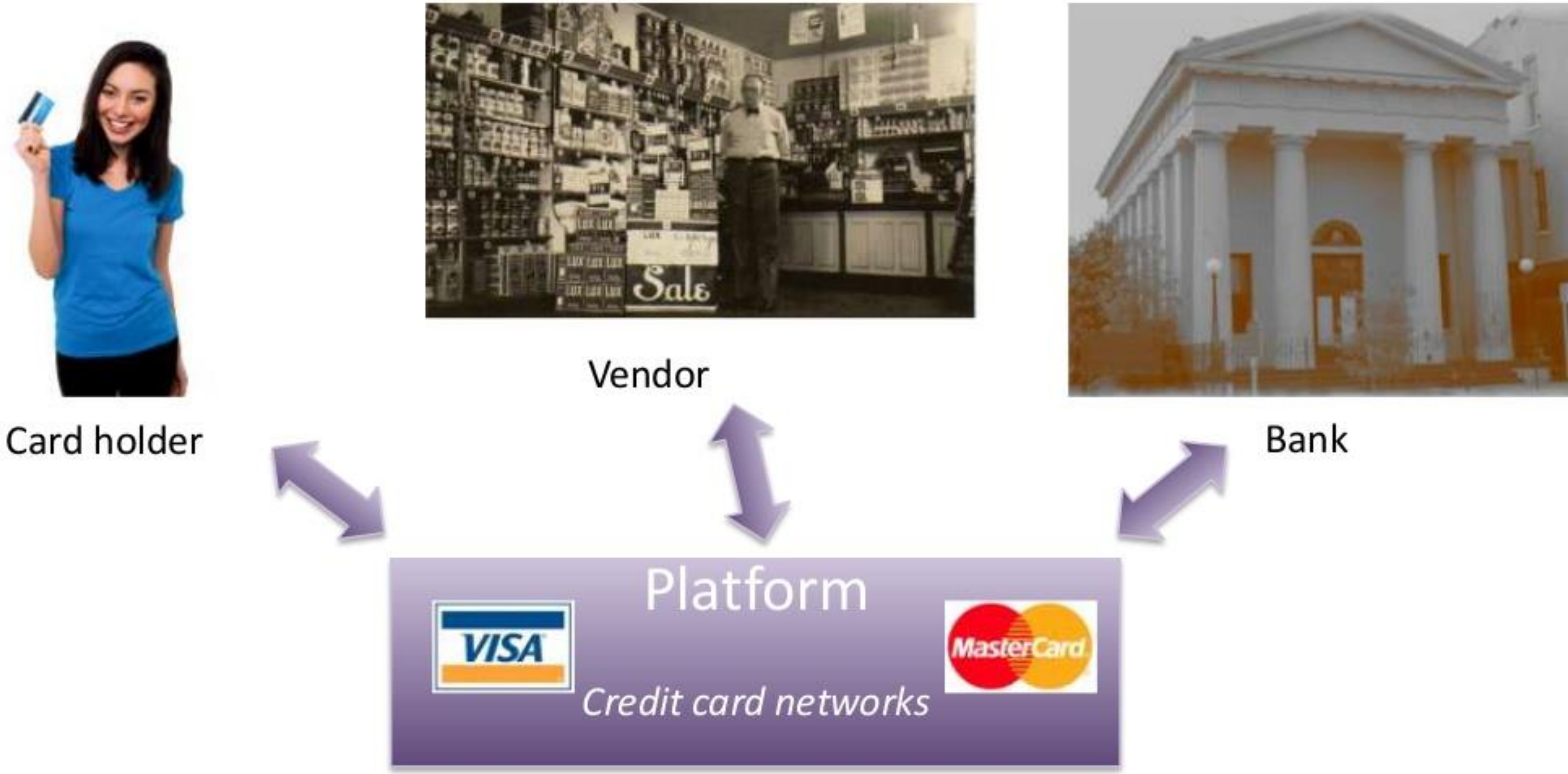
a,b,c | 노선, 응용프로그램, **핵심역량**

온라인 플랫폼

오프라인 플랫폼

자료: 창조경제연구회, 이민화

Platforms credit cards



Card holder

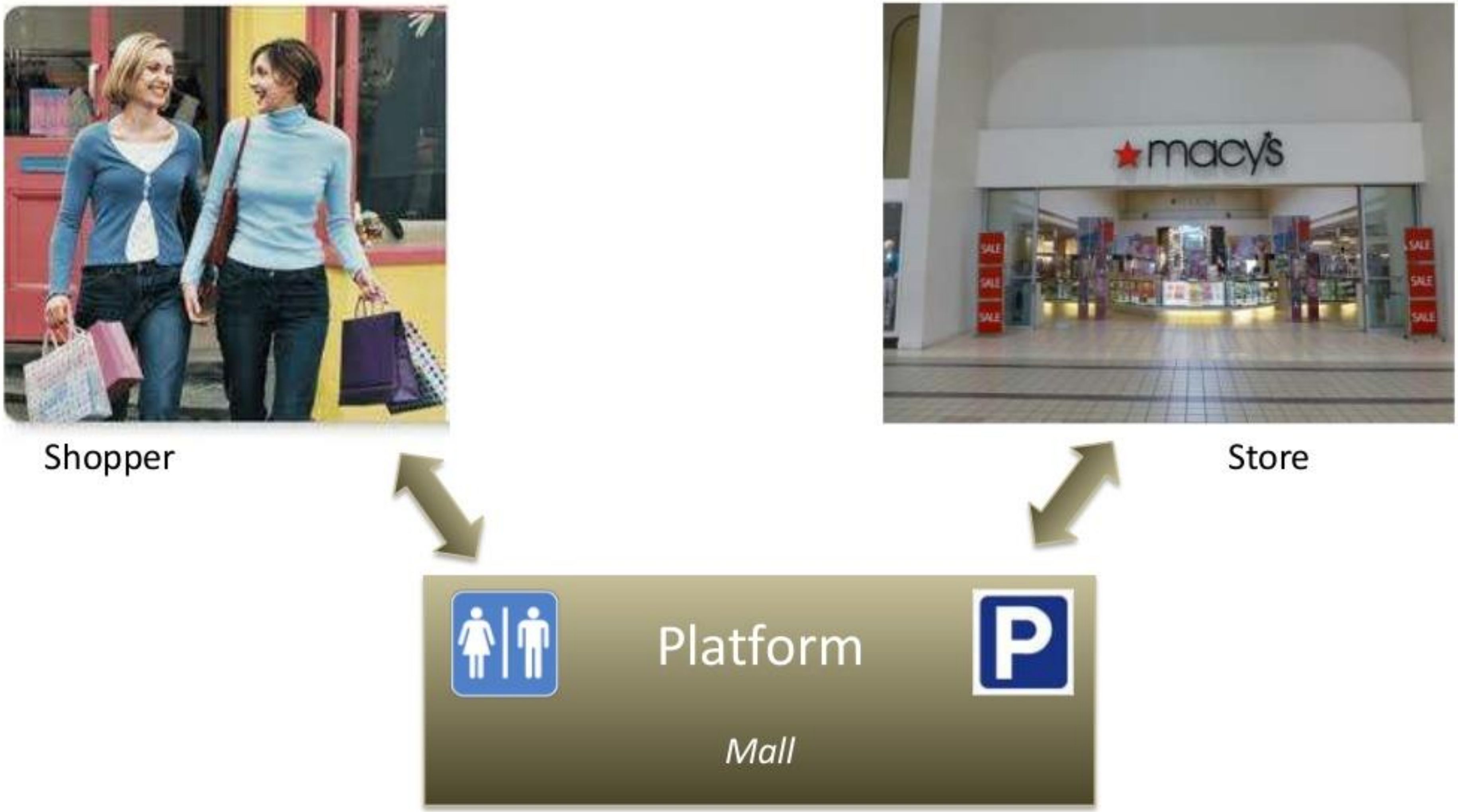
Vendor

Bank

Platform

Credit card networks

Platforms: Shopping Mall



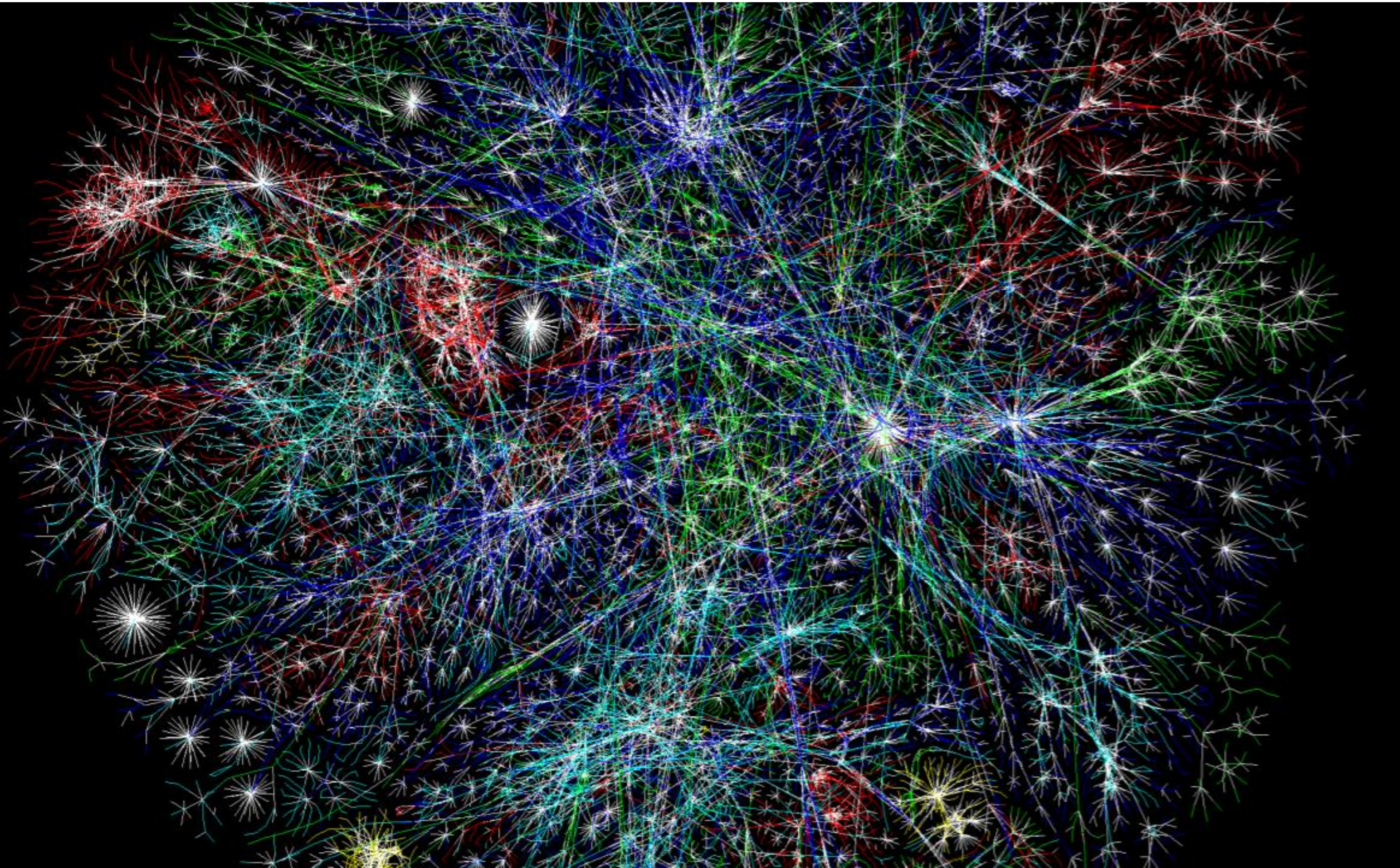
Shopper

Store

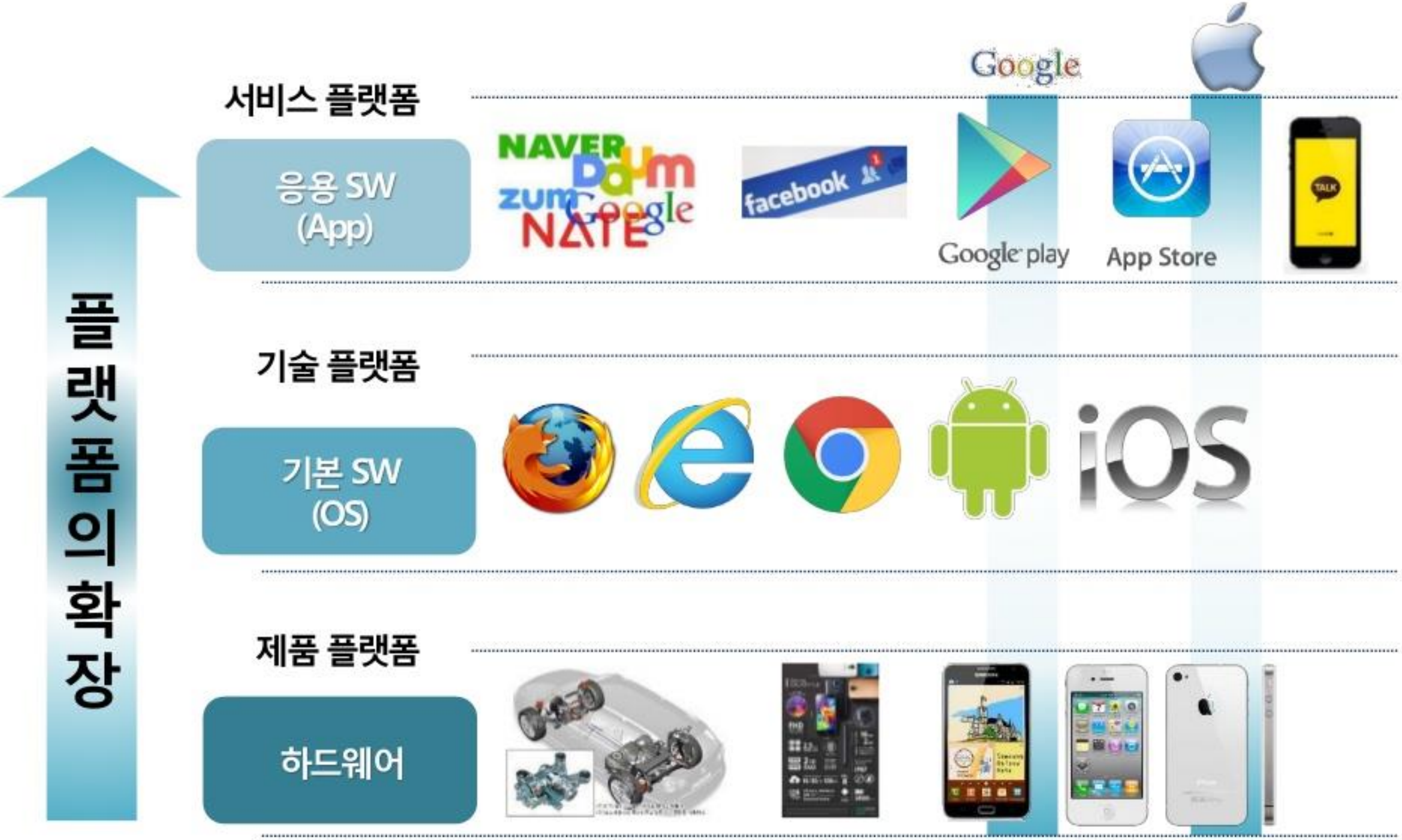
Platform

Mall

Internet Platform



플랫폼개념의 확장



플랫폼의 확장

서비스 플랫폼

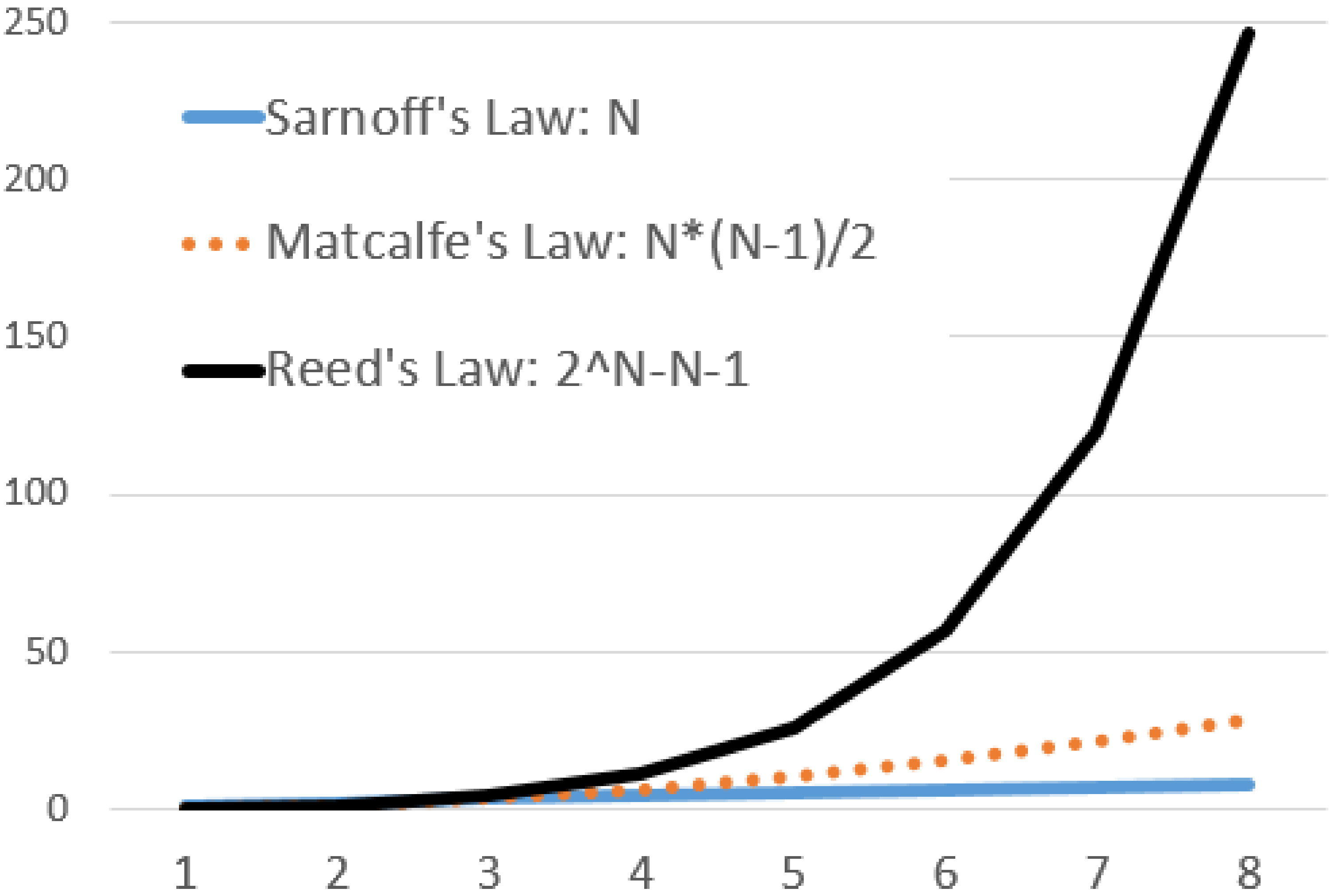
응용 SW (App)

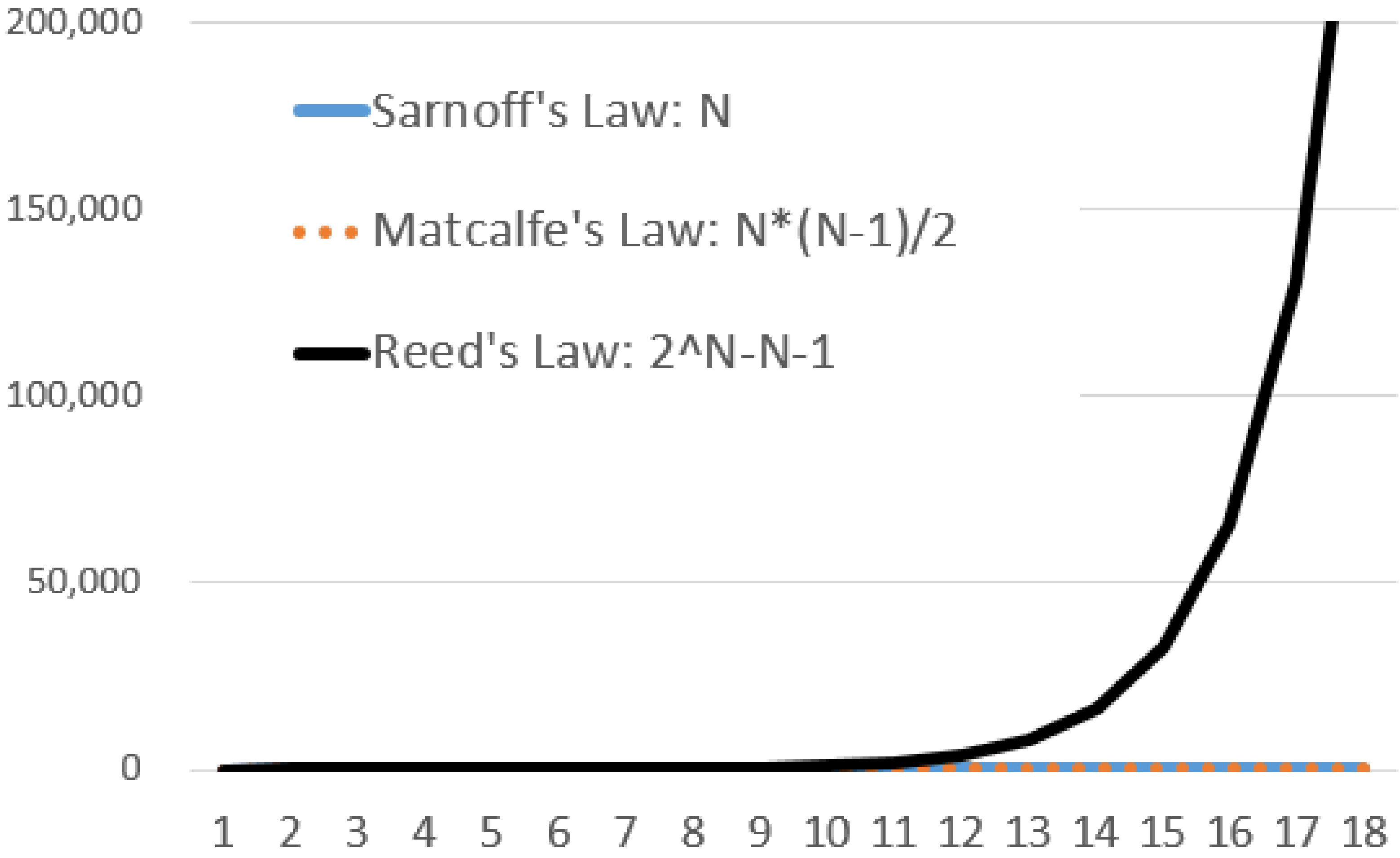
기술 플랫폼

기본 SW (OS)

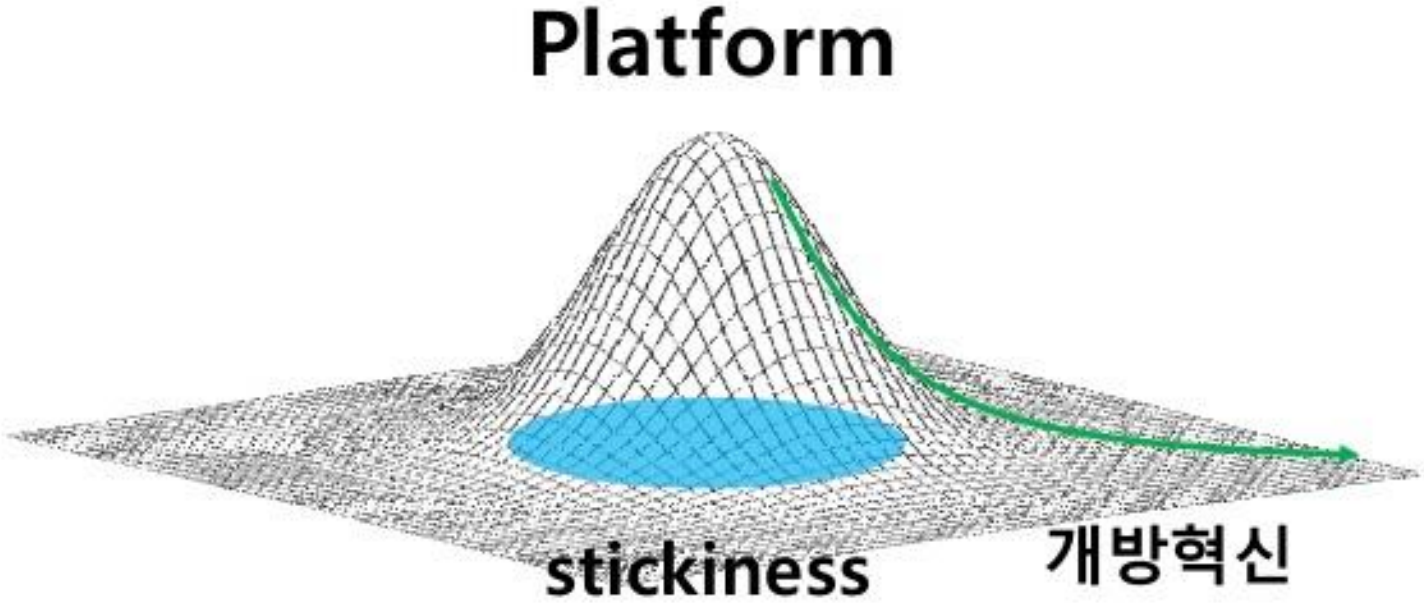
제품 플랫폼

하드웨어


250
200
150
100
50
0
Sarnoff's Law: N
Matcalfe's Law: N*(N-1)/2
Reed's Law: 2^N-N-1
1
2
3
4
5
6
7
8


200,000
150,000
100,000
50,000
0
Sarnoff's Law: N
Matcalfe's Law: N*(N-1)/2
Reed's Law: 2^N-N-1
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

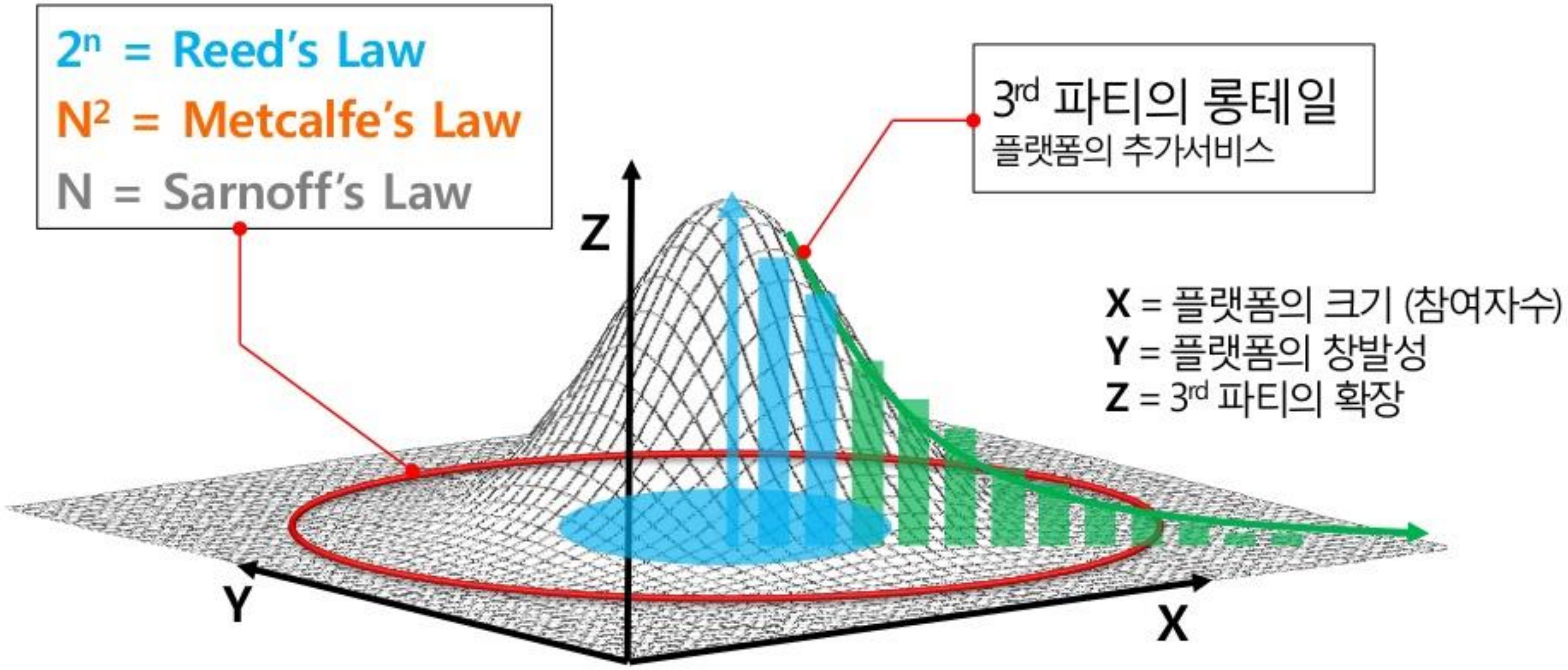
플랫폼의 가치



크고(Node) 끈끈하게(Link)

플랫폼의 가치

플랫폼의 가치 = 플랫폼의 크기 × 끈끈함 × ***3rd*** 파티

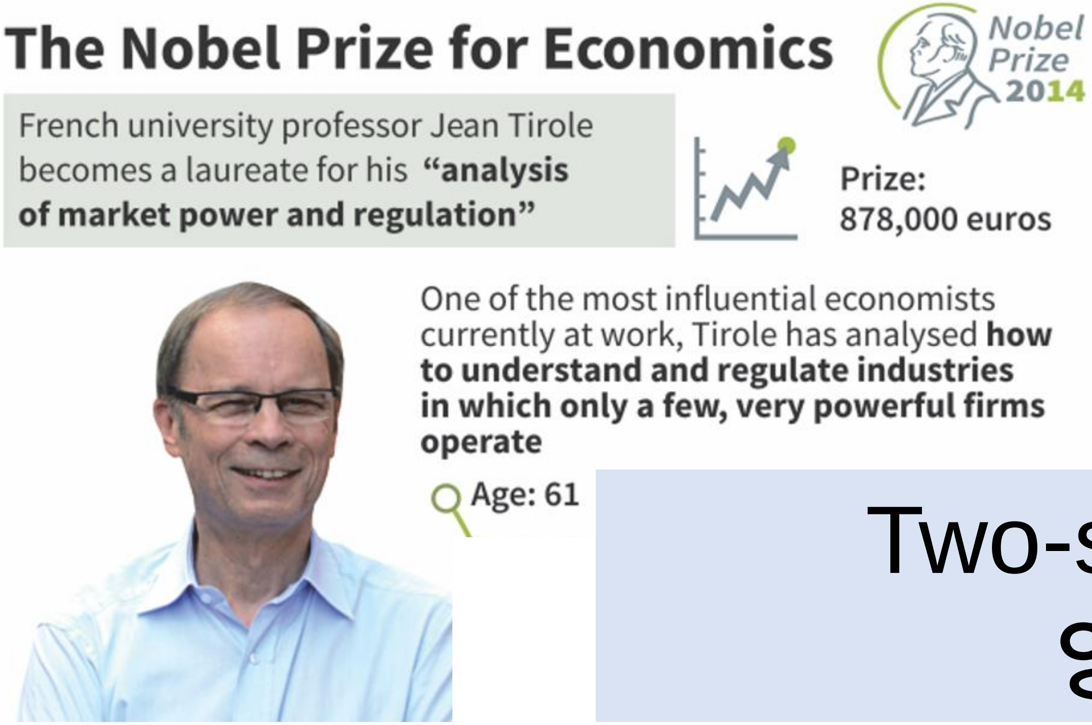


X = 플랫폼의 크기 (참여자수)
Y = 플랫폼의 창발성
Z = 3rd 파티의 확장

Major 사업

개방혁신 롱테일

2-sided Market



The Nobel Prize for Economics

Nobel Prize 2014

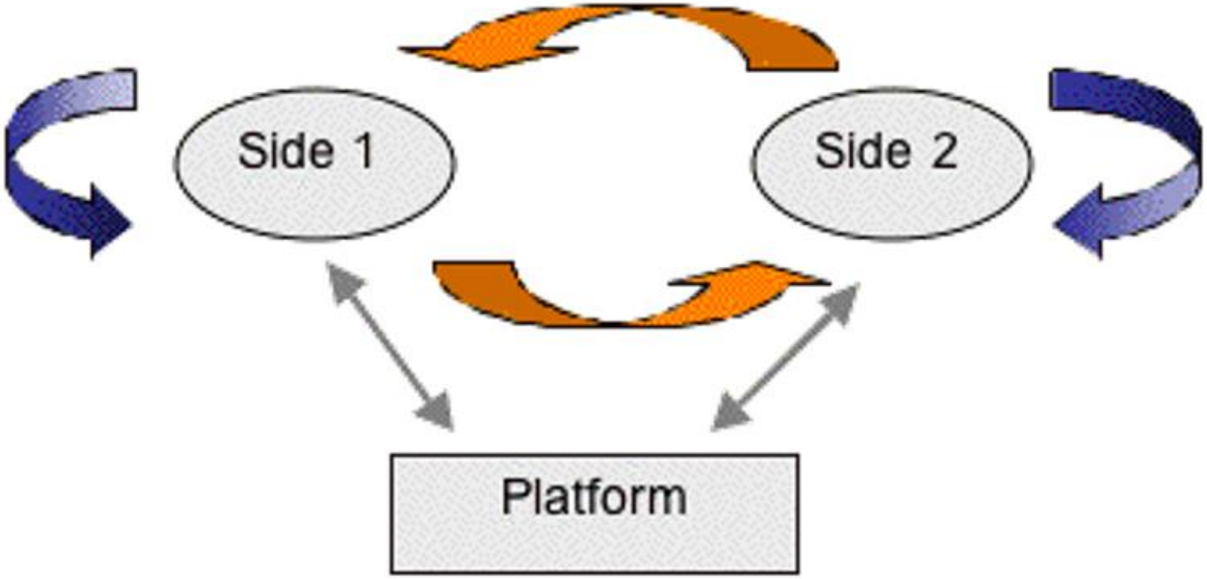
French university professor Jean Tirole becomes a laureate for his **“analysis of market power and regulation”**

Prize:
878,000 euros

One of the most influential economists currently at work, Tirole has analysed **how to understand and regulate industries in which only a few, very powerful firms operate**

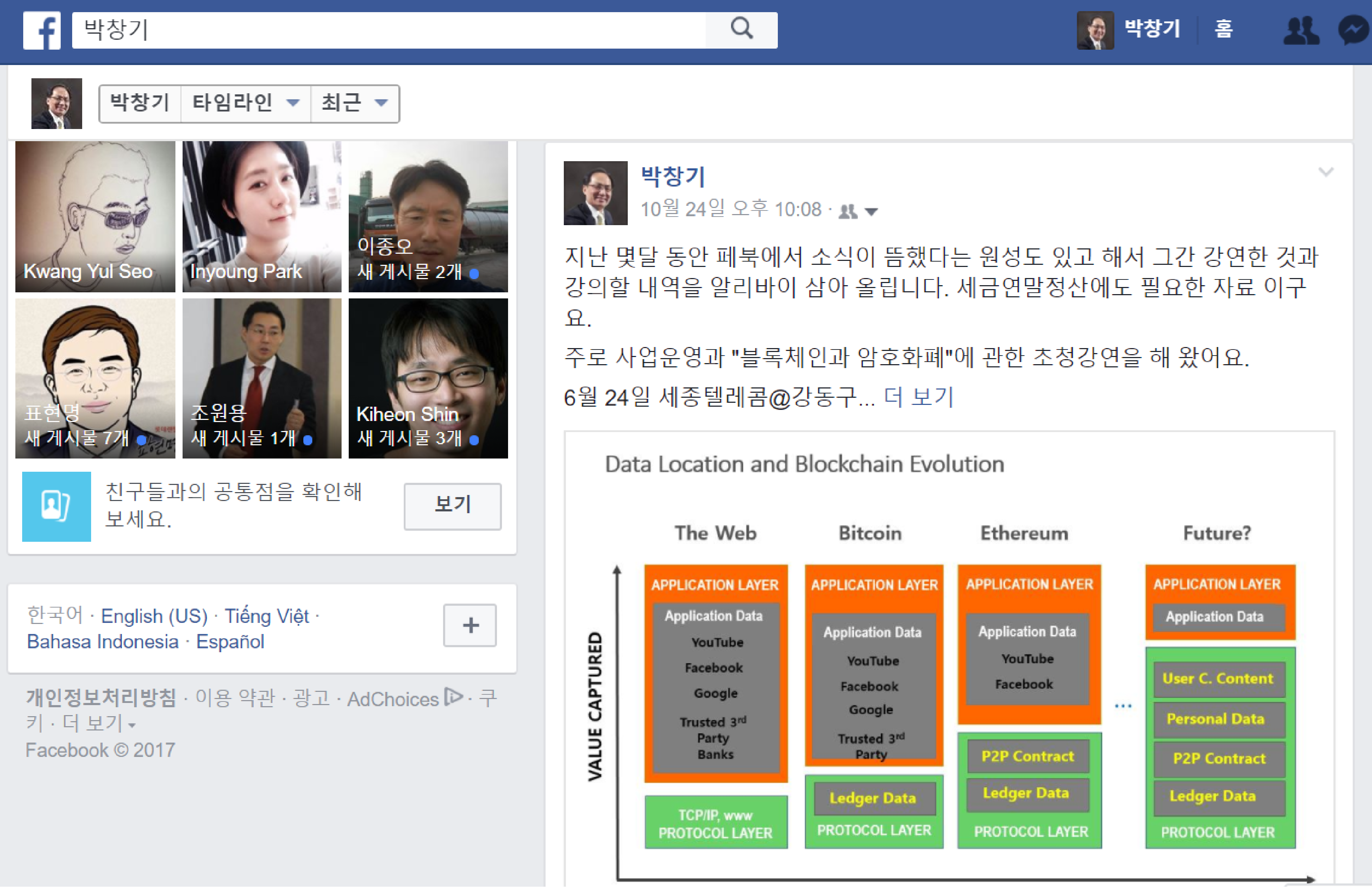
Age: 61

Two-sided Market
양면시장



Two-sided Market

Two-sided Market


박창기
박창기
홈
박창기
타임라인
최근
Kwang Yul Seo
Inyoung Park
이종오
새 게시물 2개
표현명
새 게시물 7개
조원용
새 게시물 1개
Kiheon Shin
새 게시물 3개
친구들과의 공통점을 확인해 보세요.
보기
한국어 · English (US) · Tiếng Việt · Bahasa Indonesia · Español
+
개인정보처리방침 · 이용 약관 · 광고 · AdChoices · 쿠키 · 더 보기
Facebook © 2017

박창기
10월 24일 오후 10:08 ·

지난 몇달 동안 페북에서 소식이 뜸했다는 원성도 있고 해서 그간 강연한 것과 강의할 내역을 알리바이 삼아 올립니다. 세금연말정산에도 필요한 자료 이구요.

주로 사업운영과 "블록체인과 암호화폐"에 관한 초청강연을 해 왔어요.

6월 24일 세종텔레콤@강동구... 더 보기

Data Location and Blockchain Evolution

The Web	Bitcoin	Ethereum	Future?
APPLICATION LAYER Application Data YouTube Facebook Google Trusted 3rd Party Banks	APPLICATION LAYER Application Data YouTube Facebook Google Trusted 3rd Party	APPLICATION LAYER Application Data YouTube Facebook	APPLICATION LAYER Application Data
TCP/IP, www PROTOCOL LAYER	Ledger Data PROTOCOL LAYER	P2P Contract Ledger Data PROTOCOL LAYER	User C. Content Personal Data P2P Contract Ledger Data PROTOCOL LAYER

®
Alibaba Group
阿里巴巴集团

Facebook, Google :

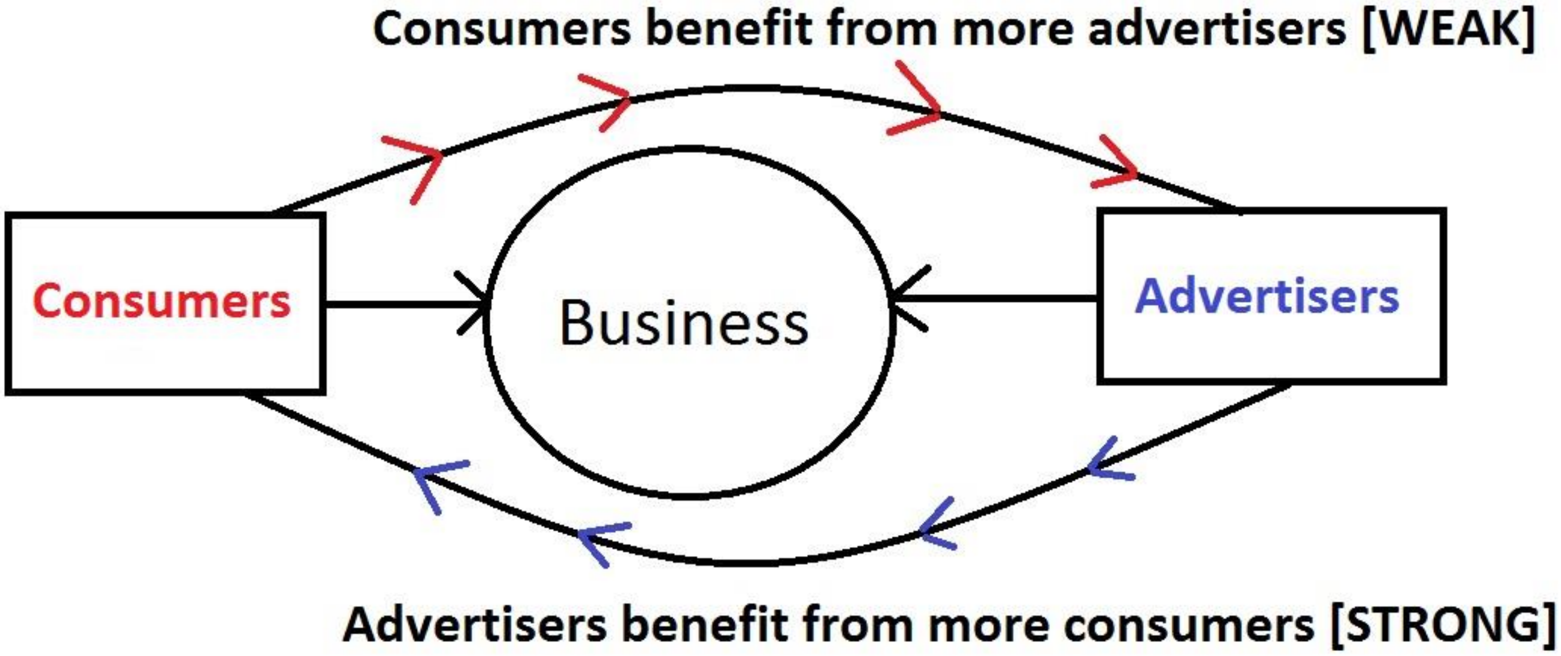
컨텐트 제공자 vs 광고비 지출자

“사용자는 무료로 쓰지만 자신이 상품이 된다.”

Apple:
App Store 수입이 30%

App 공급자 vs 유로 App 사용자

Two-Sided Market


Consumers benefit from more advertisers [WEAK]

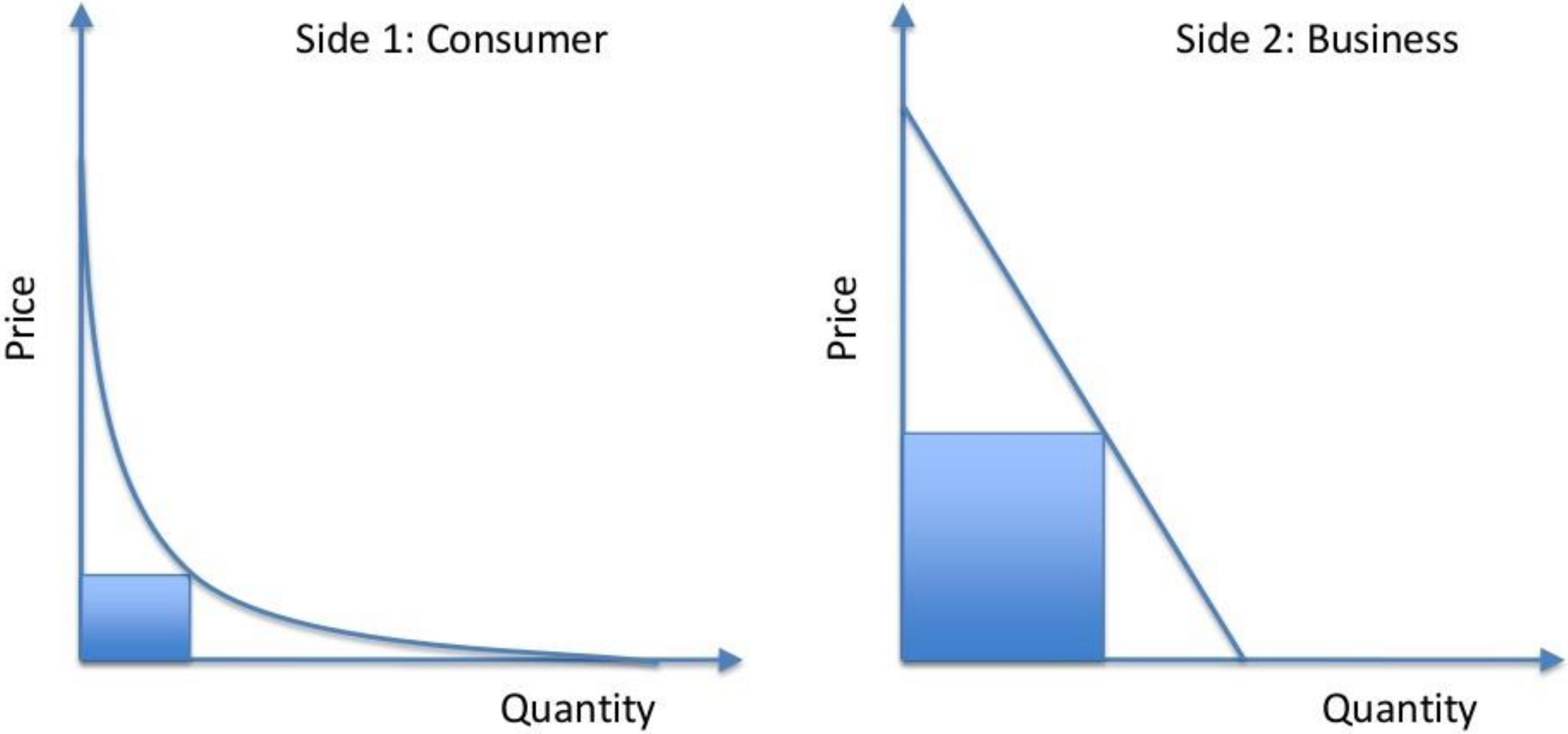
Consumers

Business

Advertisers

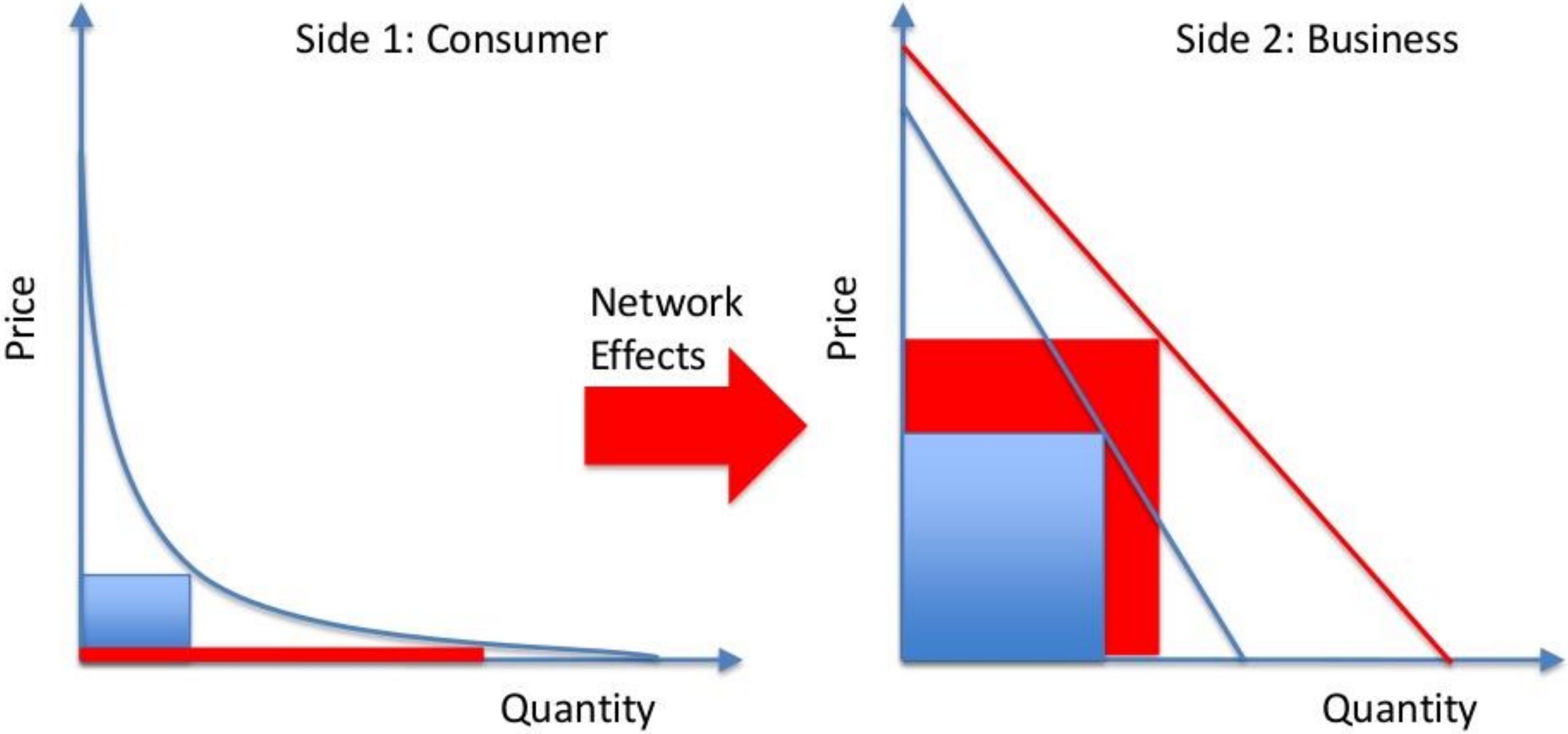
Advertisers benefit from more consumers [STRONG]

Independently maximize each market



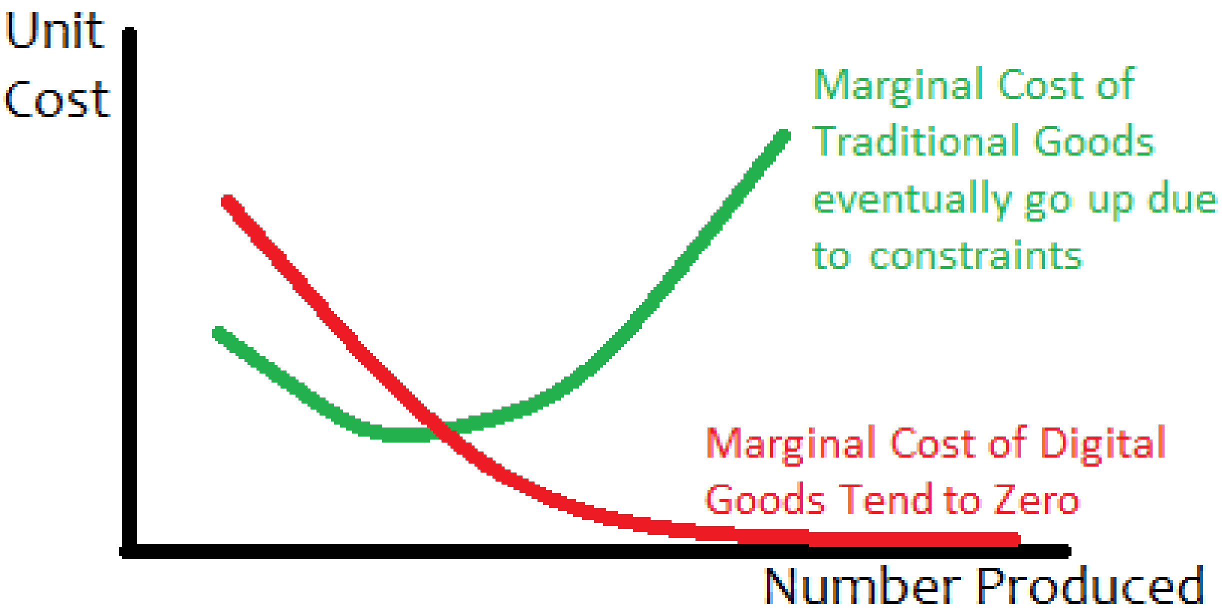
Neglects critical network effects

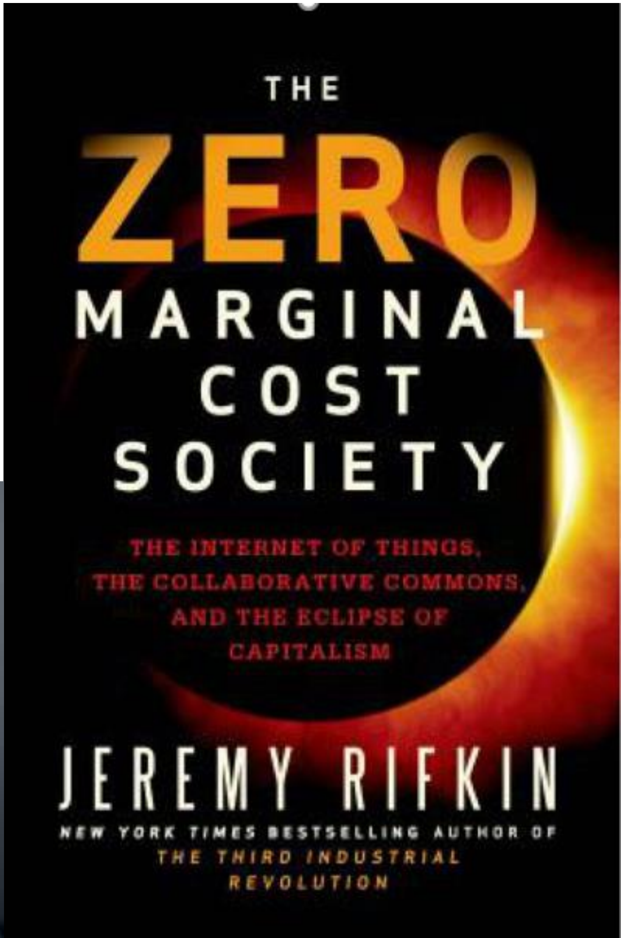
Collectively maximize both markets



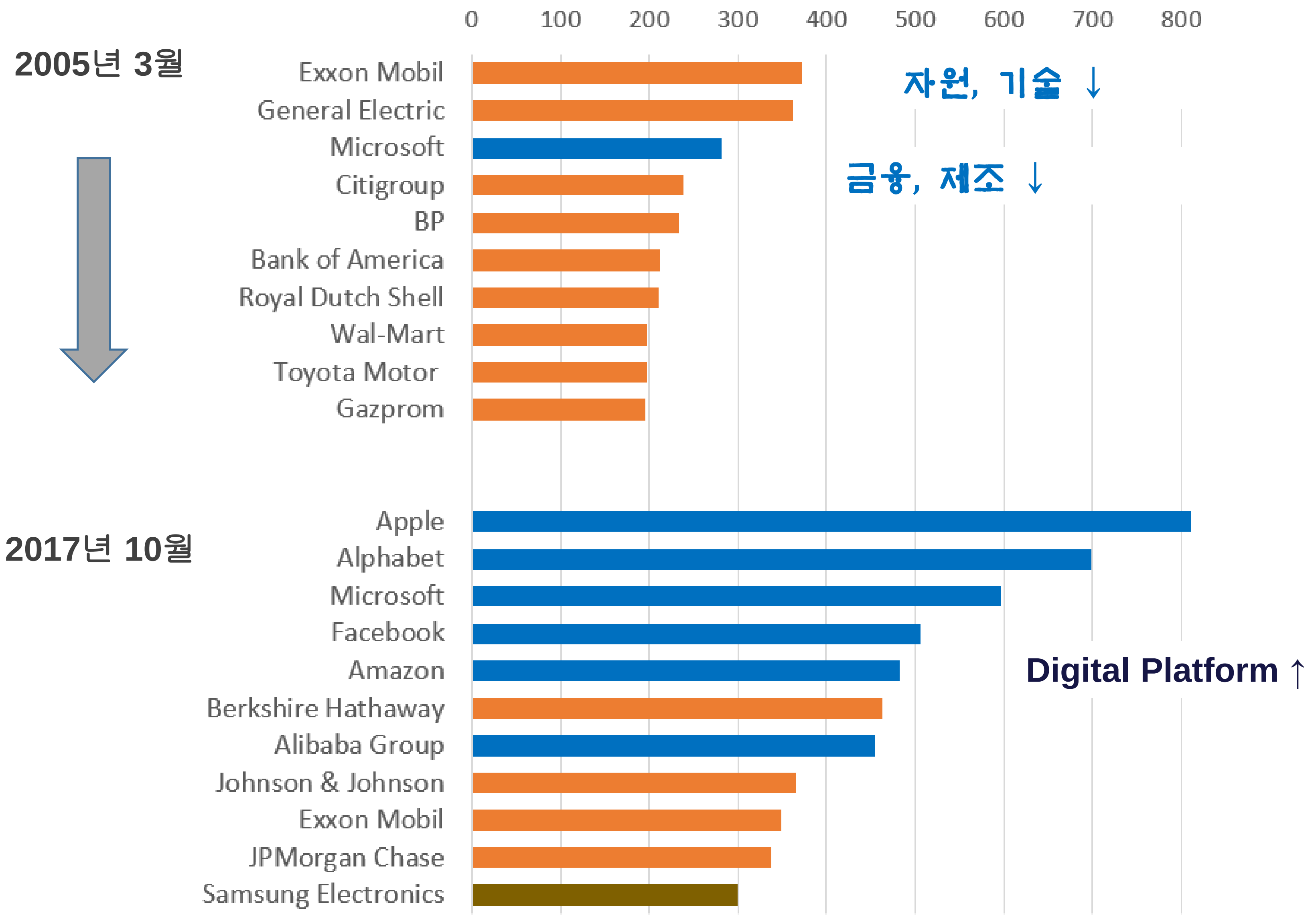
Total of red boxes must exceed blue

Leverage network effects


Unit Cost
Marginal Cost of Traditional Goods eventually go up due to constraints
Marginal Cost of Digital Goods Tend to Zero
Number Produced


THE
ZERO
MARGINAL
COST
SOCIETY
THE INTERNET OF THINGS, THE COLLABORATIVE COMMONS, AND THE ECLIPSE OF CAPITALISM
JEREMY RIFKIN
NEW YORK TIMES BESTSELLING AUTHOR OF
THE THIRD INDUSTRIAL REVOLUTION

시가총액 상위 종목의 변화



Network Effect를 보는 2개의 관점

Natural monopoly

Externality

Market Failure

Need regulation

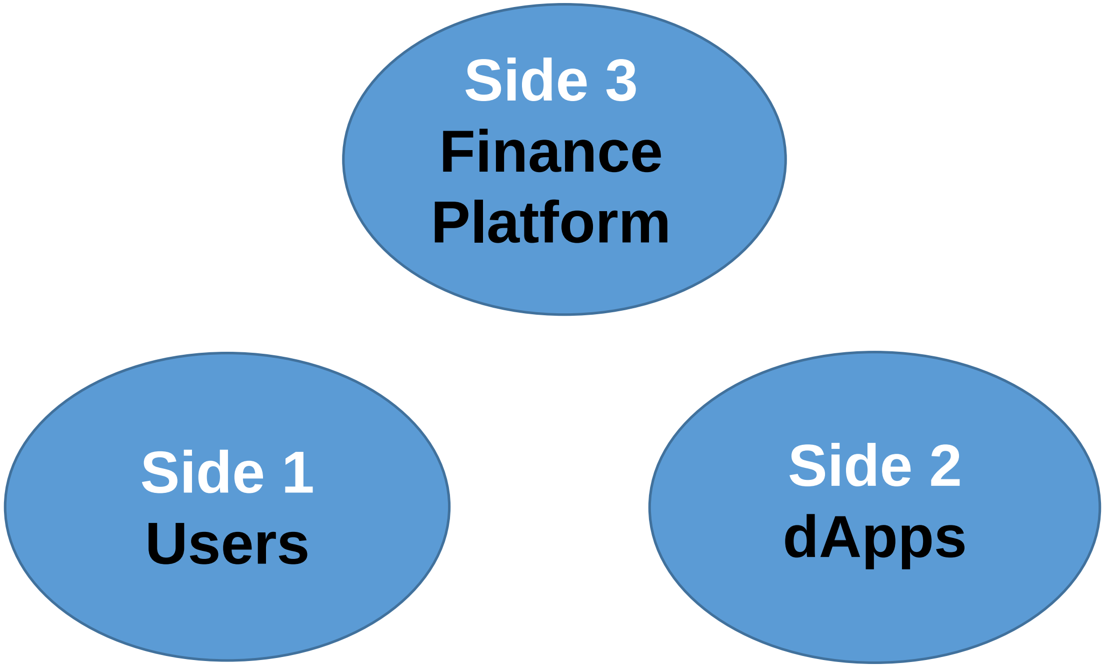
Productivity up

Consumer utility

Zero-marginal cost

Minimum regulation

2-sided Market → 3-sided Market



Side 3
Finance
Platform

Side 1
Users

Side 2
dApps

auto smart contract

거래비용과

인터넷 & 블록체인

Ronald Coase

1991 Novel Prize

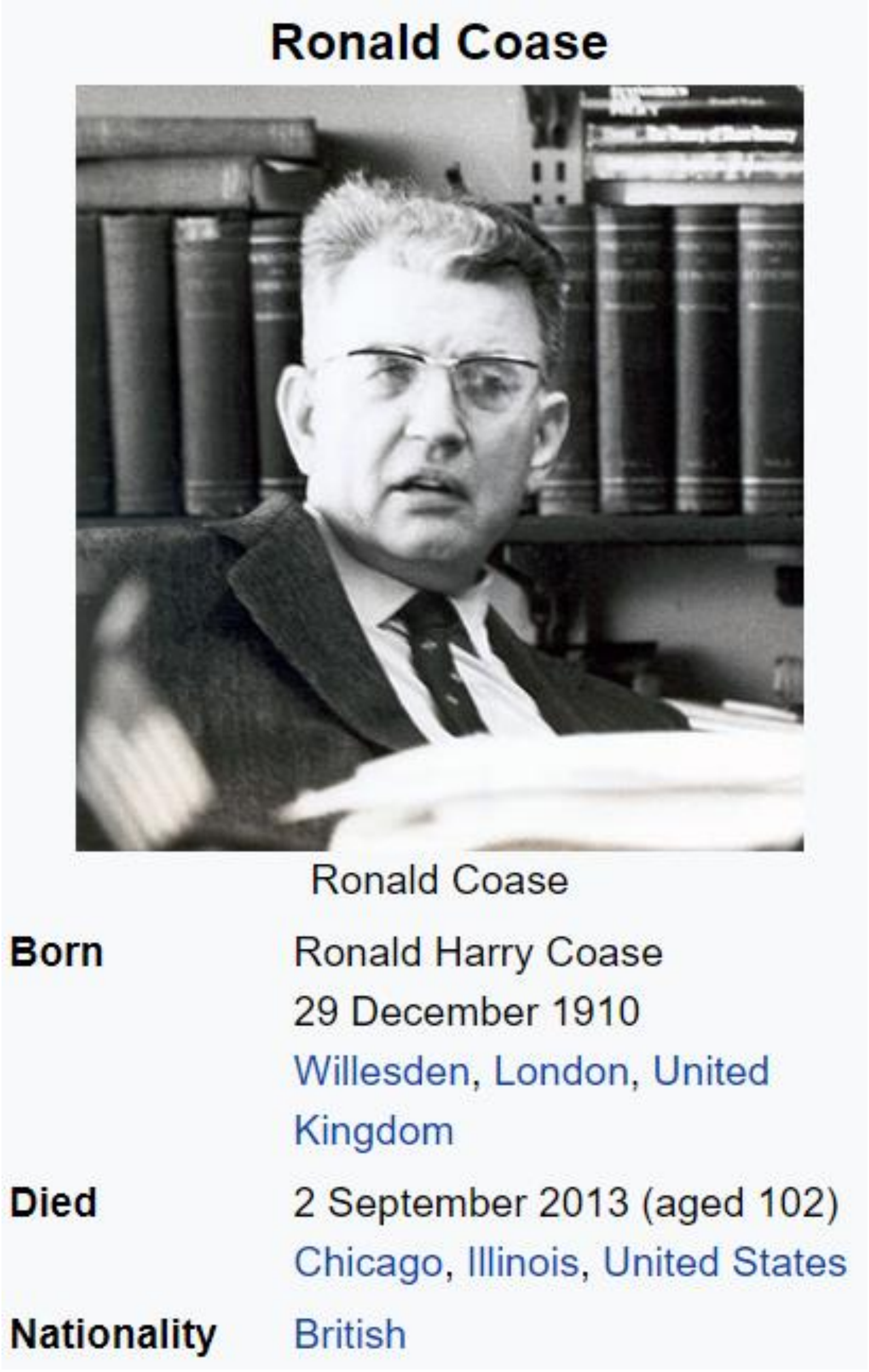
Economics

Chicago Law School

<The Nature of the Firm> 1937

<The Problem of Social Cost>

1960



Ronald Coase

Ronald Coase

Born	Ronald Harry Coase 29 December 1910 Willesden, London, United Kingdom
Died	2 September 2013 (aged 102) Chicago, Illinois, United States
Nationality	British

Efficient Market → individual Contract

(Free Economy)

Transaction cost: Search, Negotiation, Contract, Dispute

→ Big Companies by hiring people

(Planned Economy)

Lowering Transaction Cost

Law & Trusted 3rd Party

Internet & Blockchain

→ 4th Industrial Revolution

4차 산업혁명의 동력

SNS, Big data, AI, IoT로

무장한 벤처의

전통 대기업 모델 분해

Unbundling

탈 중앙화 Decentralization

Beyond BRICs: 7 Emerging Markets to Watch
FORTUNE
THE AGE OF UNICORNS
At Least 80 Tech Startups Are Worth $1 Billion or More. Is This Boom for Real?
Plus
The Most Powerful (and Hated) Force in Education
The Algorithmic CEO
The Quest for the Foolproof Flu Shot

GLOBAL UNICORN CLUB: 197 PRIVATE COMPANIES VALUED AT $1B+ MARKET MAP as of 5/26/2017

E-COMMERCE/ MARKETPLACE

Africa Internet Group
houzz
airbnb
酒仙网
爱屋吉屋
口袋购物 koudai.com
AUTO1 GROUP
mercari
贝贝网 beibei.com
蜜芽 mia.com
Blue Apron
NewDada 新达达
美团 + 大众点评
OfferUp
Coupang
ShopClues
Delivery Hero
JUSTFAB
FANATICS
返利 Fanli.com
FARFETCH
Thumbtack
tujia 途家
flipkart
GFG GLOBAL FASHION GROUP
VANCL 凡客诚品
瓜子 二手车直卖 Guazi.com
WARBY PARKER
微票儿
wish
lianjia 链家
小红书

INTERNET SOFTWARE & SERVICES

anaplan
C3 IoT
AppDirect
知乎
APTTUS
AUTOMATTIC
MEDALLIA
docker
zoom
DocuSign
Pivotal
FANDUEL
slack
SMS ASSIST
GitHub
Spotify
KATERRA
glassdoor
SYMPHONY
网易 NETEASE
Hootsuite
Tenx
rubrik
infor
Zeta
Quora

ON-DEMAND

BlaBlaCar
ele.me
ofo
Careem
GO-JEK
lyft
instacart
GRABTAXI
OLA
滴滴
UBER

BIG DATA

actifio
afiniti
Qualtrics
DOMO
INSIDESALES.COM
OVH.com
MarkLogic
Palantir
mongoDB
UPTAKE
Mu Sigma

FINTECH

51信用卡
陆金所 LU.com
adyen
Mozido
AVANT
one97
PROSPER
avaloq
融360
Credit Karma
SoFi
Funding Circle
TransferWise
GreenSky
GUSTO
Kabbage
ZENEFITS
robinhood
Klarna
众安保险
stripe

HARDWARE

carbon
datto
NIO
dji
MEIZU
PELOTON
INFINIDAT
UBTECH
JAWBONE
mi 小米
RAZER
magic leap
ROYOLE
SPACEX

MOBILE SOFTWARE & SERVICES

APUS
InMobi
Garena
SHAZAM
ironSource
yello mobile
快手

REAL ESTATE

COMPASS
GLOBAL SWITCH
UR WORK
OPENDOOR
Mofang
wework

SOCIAL

hike
sprinklr
kik
Tango
蘑菇街 mogujie.com
xiaoka 一下科技
Nextdoor
Pinterest
zomato

CYBERSECURITY

TANIUM
avast!
illumio
CROWDSTRIKE
Lookout
CYLANCE
CLOUDFLARE
zscaler

HEALTHCARE

23andMe
挂号网
Clover
Adaptive
moderna
HUMAN LONGEVITY, INC.
oscar
BenevolentAI
NANOPORE
iCarbonX
proteus
FLATIRON
Intarcia
Zocdoc

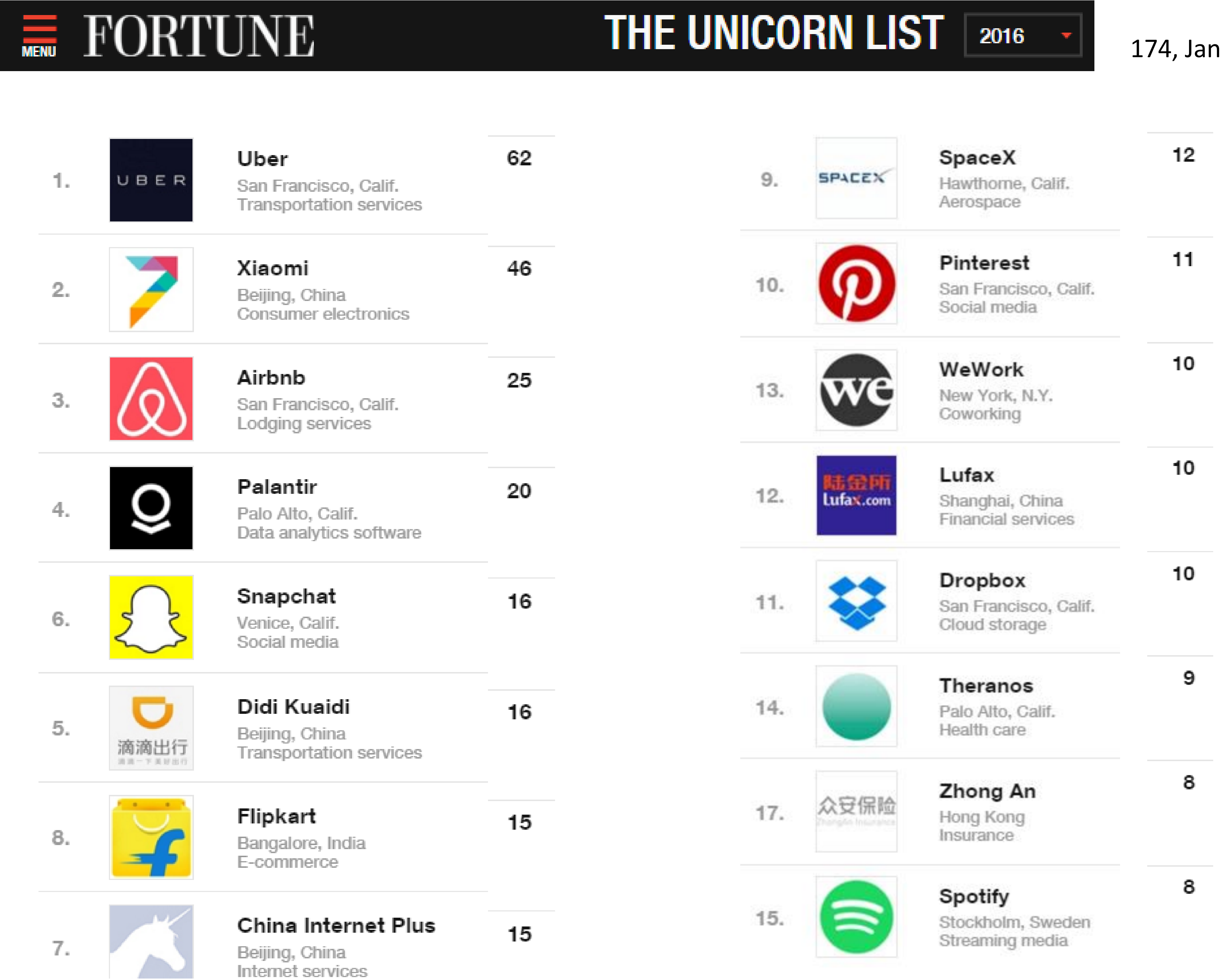
MEDIA

BuzzFeed
STX ENTERTAINMENT
今日头条
VICE
VOX MEDIA

OTHER

IMPROBABLE
PLURALSIGHT
沪江 HUJIANG.COM
appnexus
猎聘网 Liepin.com
ReNew POWER
PANSHI 盘石
网易云音乐
LifeMiles
BREWDOG
JETSMARTER
KENDRA SCOTT
PROCORE
unity
Age of Learning
decolar.com
CJ
iTutorGroup
QUANERGY
mindmaze
ZOOX
货车帮
PROMASIDOR
Bloomenergy

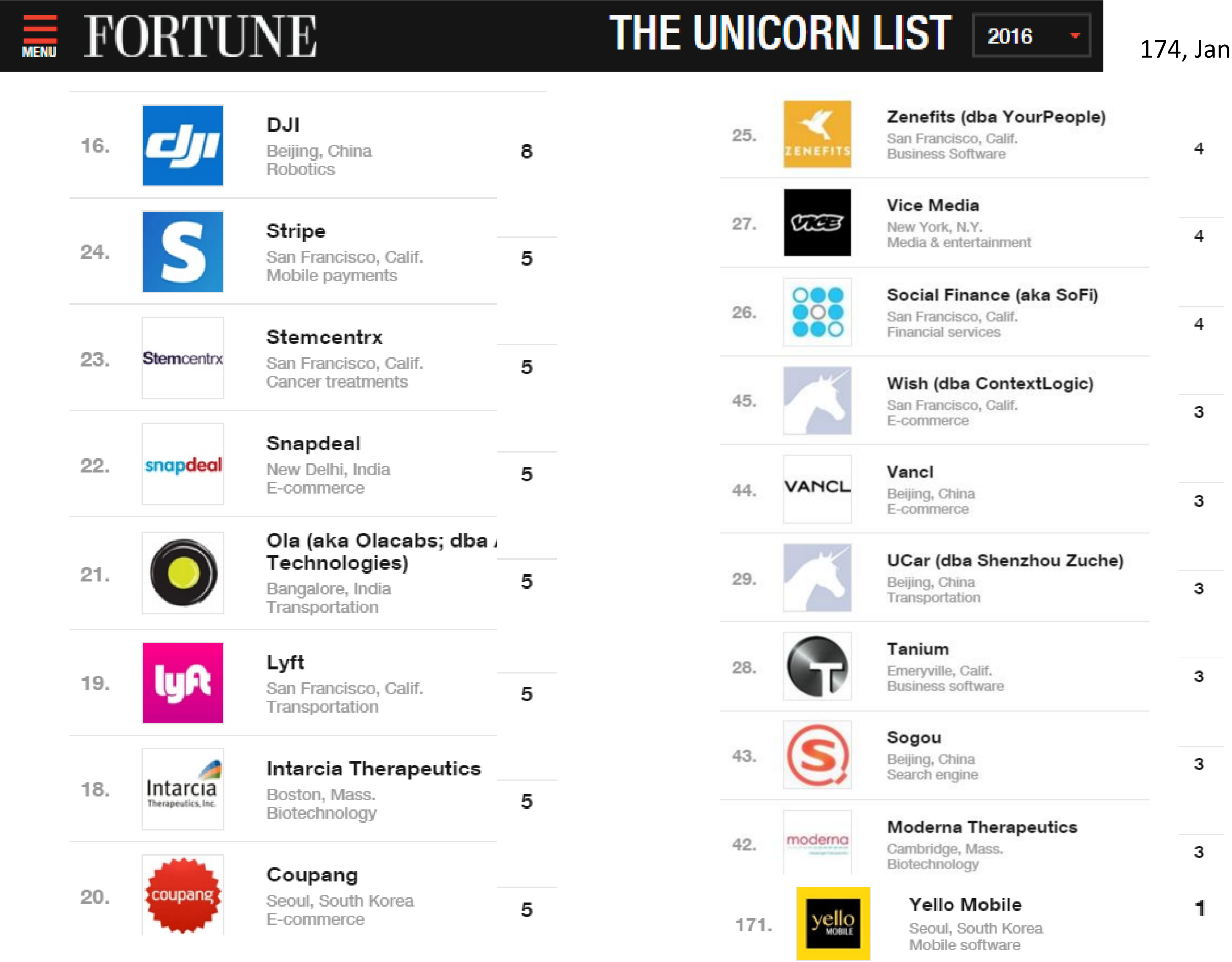
CBINSIGHTS



FORTUNE THE UNICORN LIST 2016

174, Jan. 2016

1.	Uber	San Francisco, Calif.	Transportation services	62
2.	Xiaomi	Beijing, China	Consumer electronics	46
3.	Airbnb	San Francisco, Calif.	Lodging services	25
4.	Palantir	Palo Alto, Calif.	Data analytics software	20
6.	Snapchat	Venice, Calif.	Social media	16
5.	Didi Kuaidi	Beijing, China	Transportation services	16
8.	Flipkart	Bangalore, India	E-commerce	15
7.	China Internet Plus	Beijing, China	Internet services	15
9.	SpaceX	Hawthorne, Calif.	Aerospace	12
10.	Pinterest	San Francisco, Calif.	Social media	11
13.	WeWork	New York, N.Y.	Coworking	10
12.	Lufax	Shanghai, China	Financial services	10
11.	Dropbox	San Francisco, Calif.	Cloud storage	10
14.	Theranos	Palo Alto, Calif.	Health care	9
17.	Zhong An	Hong Kong	Insurance	8
15.	Spotify	Stockholm, Sweden	Streaming media	8



FORTUNE

THE UNICORN LIST 2016

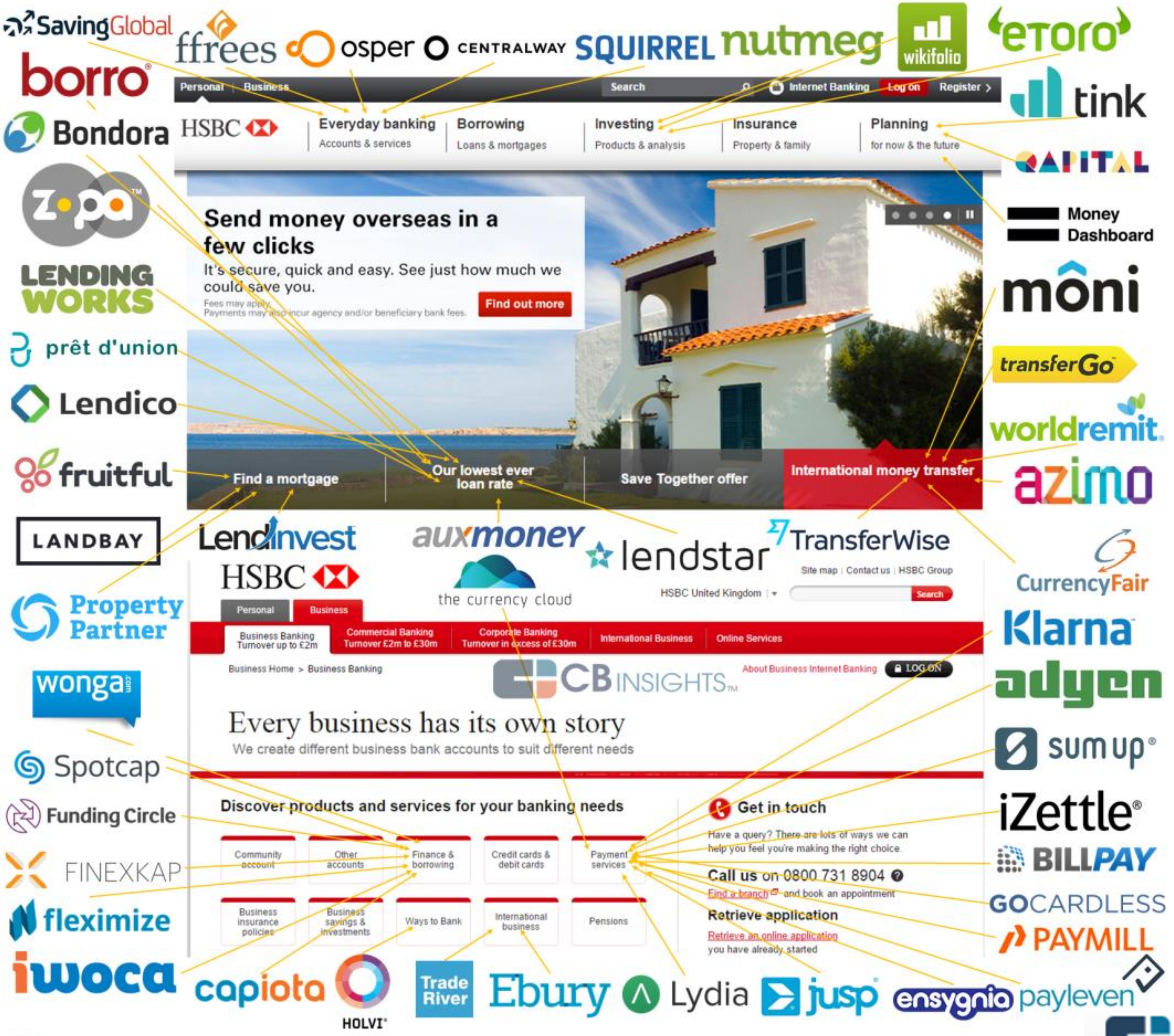
174, Jan. 2016

16.	DJI	Beijing, China	Robotics	8
24.	Stripe	San Francisco, Calif.	Mobile payments	5
23.	Stemcentrx	San Francisco, Calif.	Cancer treatments	5
22.	Snapdeal	New Delhi, India	E-commerce	5
21.	Ola (aka Olacabs; dba Technologies)	Bangalore, India	Transportation	5
19.	Lyft	San Francisco, Calif.	Transportation	5
18.	Intarcia Therapeutics	Boston, Mass.	Biotechnology	5
20.	Coupang	Seoul, South Korea	E-commerce	5

25.	Zenefits (dba YourPeople)	San Francisco, Calif.	Business Software	4
27.	Vice Media	New York, N.Y.	Media & entertainment	4
26.	Social Finance (aka SoFi)	San Francisco, Calif.	Financial services	4
45.	Wish (dba ContextLogic)	San Francisco, Calif.	E-commerce	3
44.	Vancl	Beijing, China	E-commerce	3
29.	UCar (dba Shenzhou Zuche)	Beijing, China	Transportation	3
28.	Tanium	Emeryville, Calif.	Business software	3
43.	Sogou	Beijing, China	Search engine	3
42.	Moderna Therapeutics	Cambridge, Mass.	Biotechnology	3
171.	Yello Mobile	Seoul, South Korea	Mobile software	1

174 업체 중 미국 101 중국 36 영국 7
인도 7 독일 5 싱가폴 3 한국 2개

Unbundling of a European Bank



Send money overseas in a few clicks

It's secure, quick and easy. See just how much we could save you.

Fees may apply. Payments may also incur agency and/or beneficiary bank fees.

Every business has its own story

We create different business bank accounts to suit different needs

Discover products and services for your banking needs

Get in touch

Have a query? There are lots of ways we can help you feel you're making the right choice.

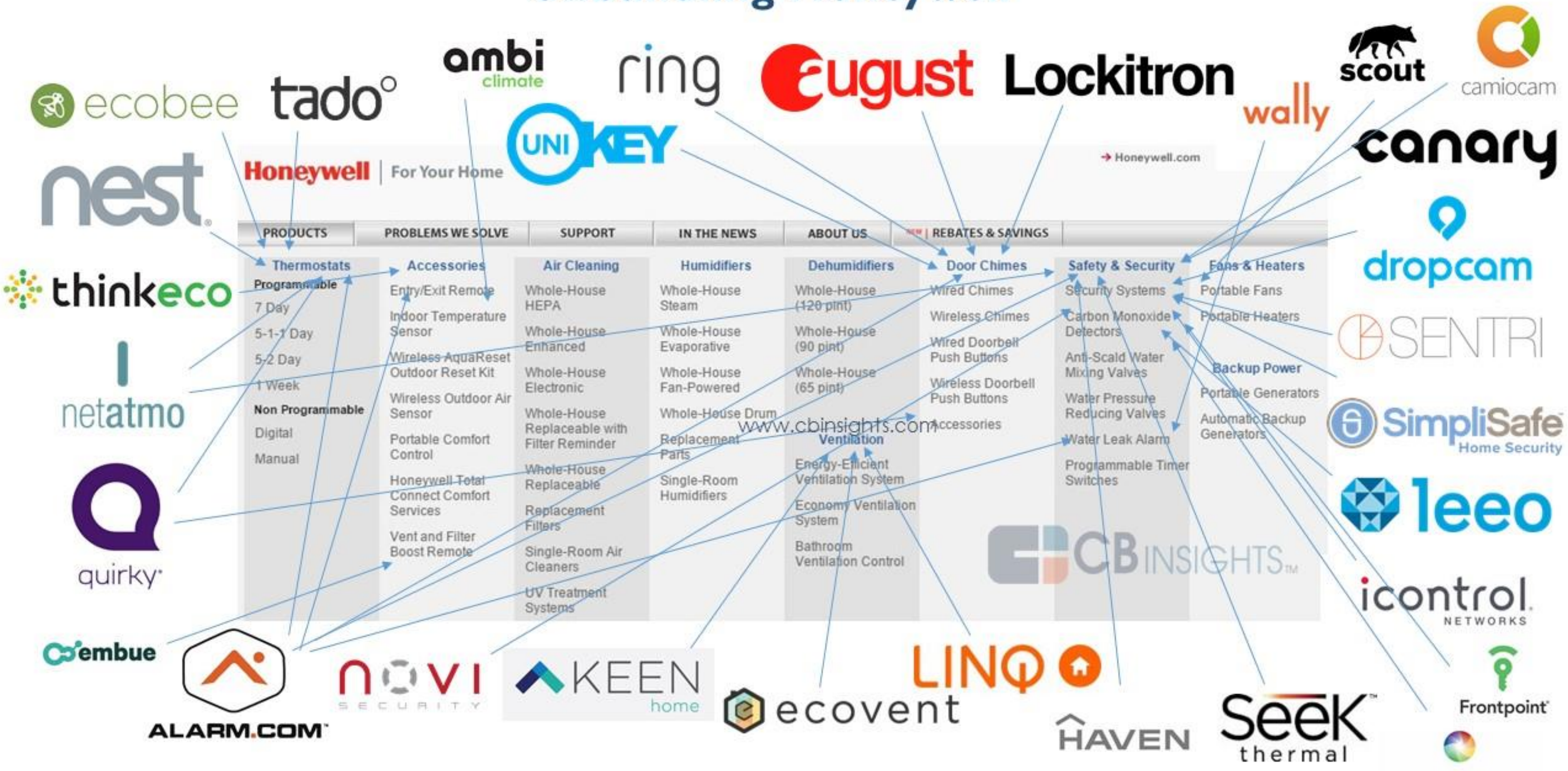
Call us on 0800 731 8904

Find a branch and book an appointment

Retrieve application

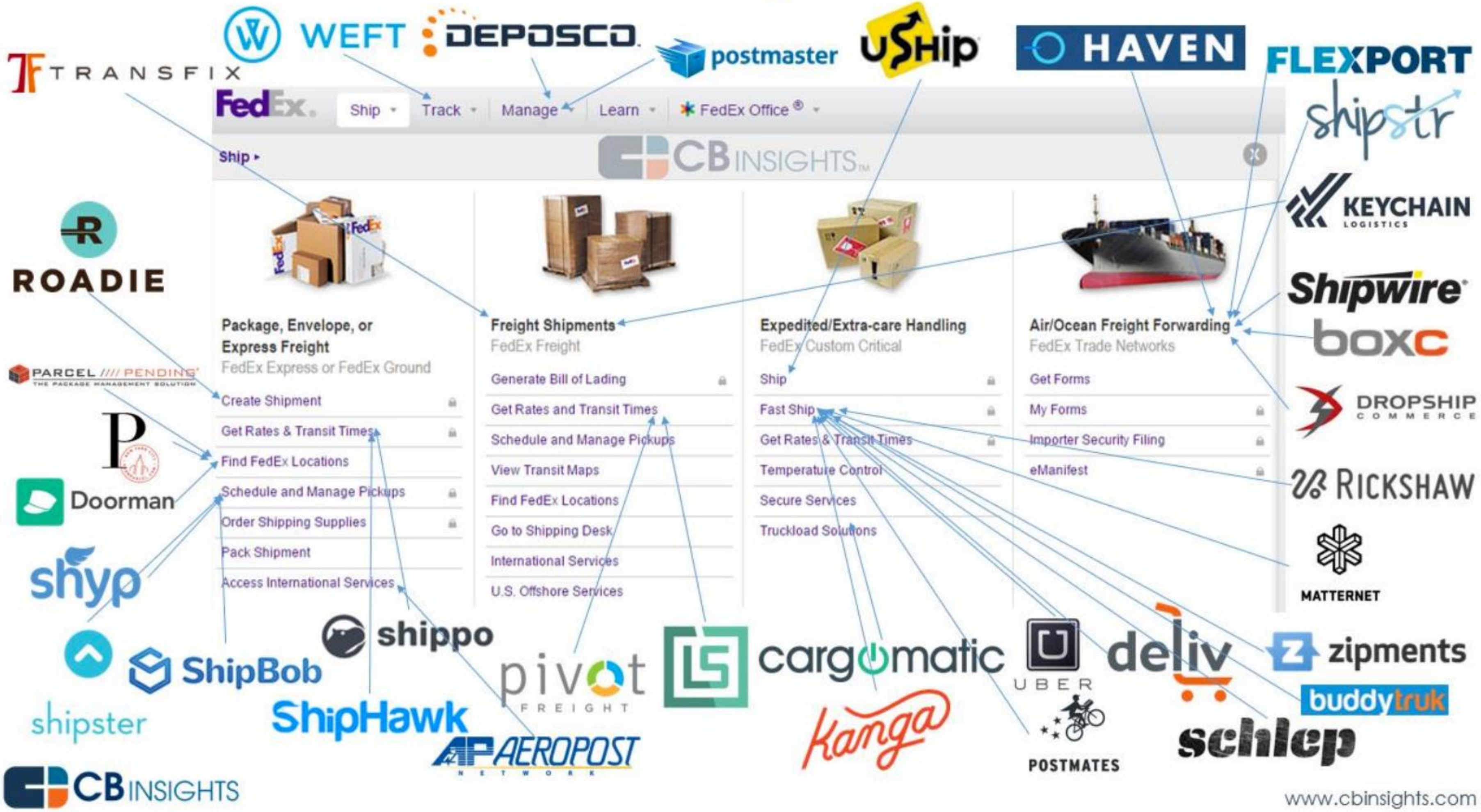
Retrieve an online application you have already started

Unbundling Honeywell



www.cbinsights.com

Unbundling FedEx



FedEx. Ship ▾ Track ▾ Manage ▾ Learn ▾ FedEx Office ® ▾

Ship ▸

Package, Envelope, or Express Freight
FedEx Express or FedEx Ground

- Create Shipment
- Get Rates & Transit Times
- Find FedEx Locations
- Schedule and Manage Pickups
- Order Shipping Supplies
- Pack Shipment
- Access International Services

Freight Shipments
FedEx Freight

- Generate Bill of Lading
- Get Rates and Transit Times
- Schedule and Manage Pickups
- View Transit Maps
- Find FedEx Locations
- Go to Shipping Desk
- International Services
- U.S. Offshore Services

Expedited/Extra-care Handling
FedEx Custom Critical

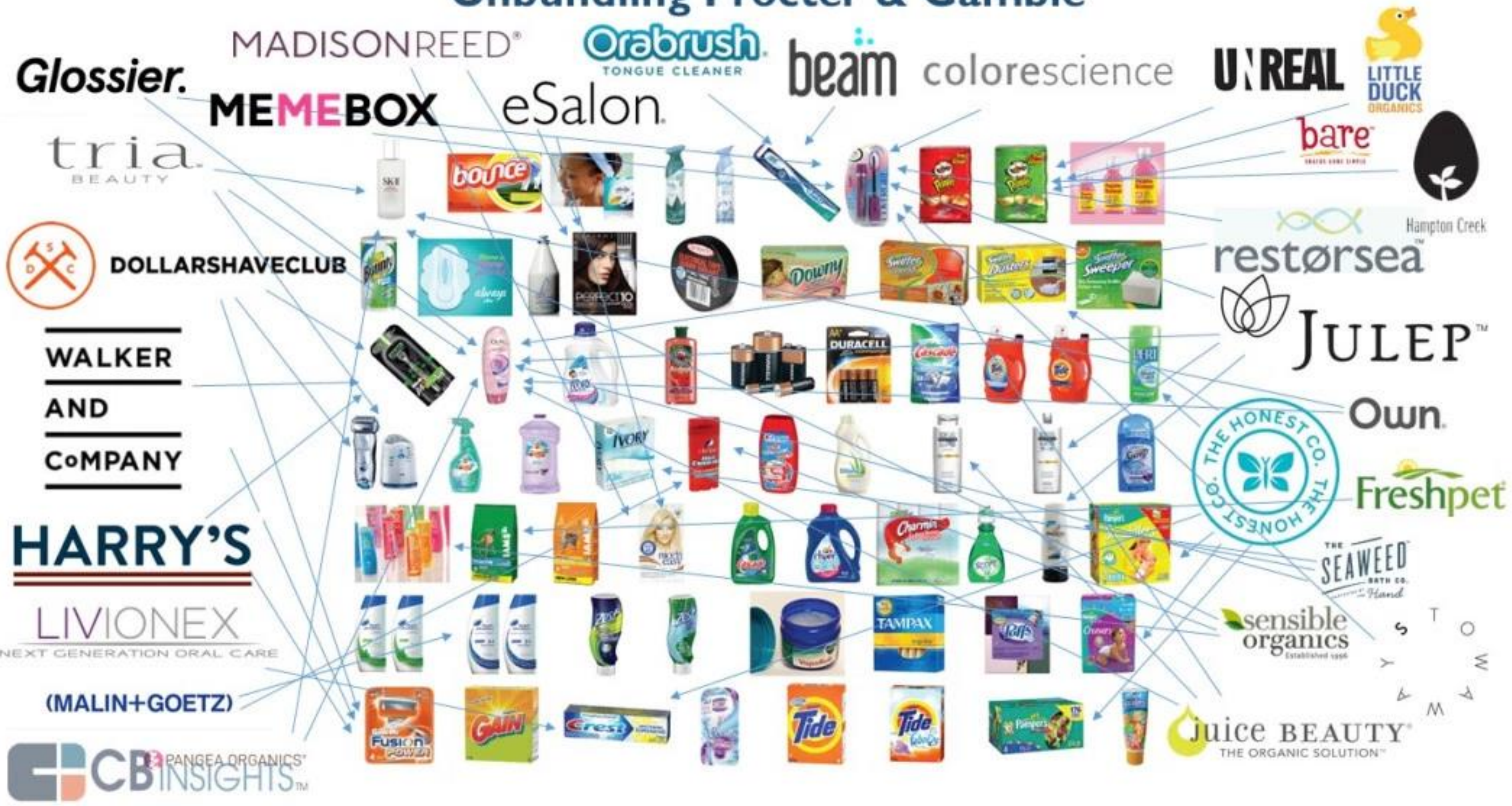
- Ship
- Fast Ship
- Get Rates & Transit Times
- Temperature Control
- Secure Services
- Truckload Solutions

Air/Ocean Freight Forwarding
FedEx Trade Networks

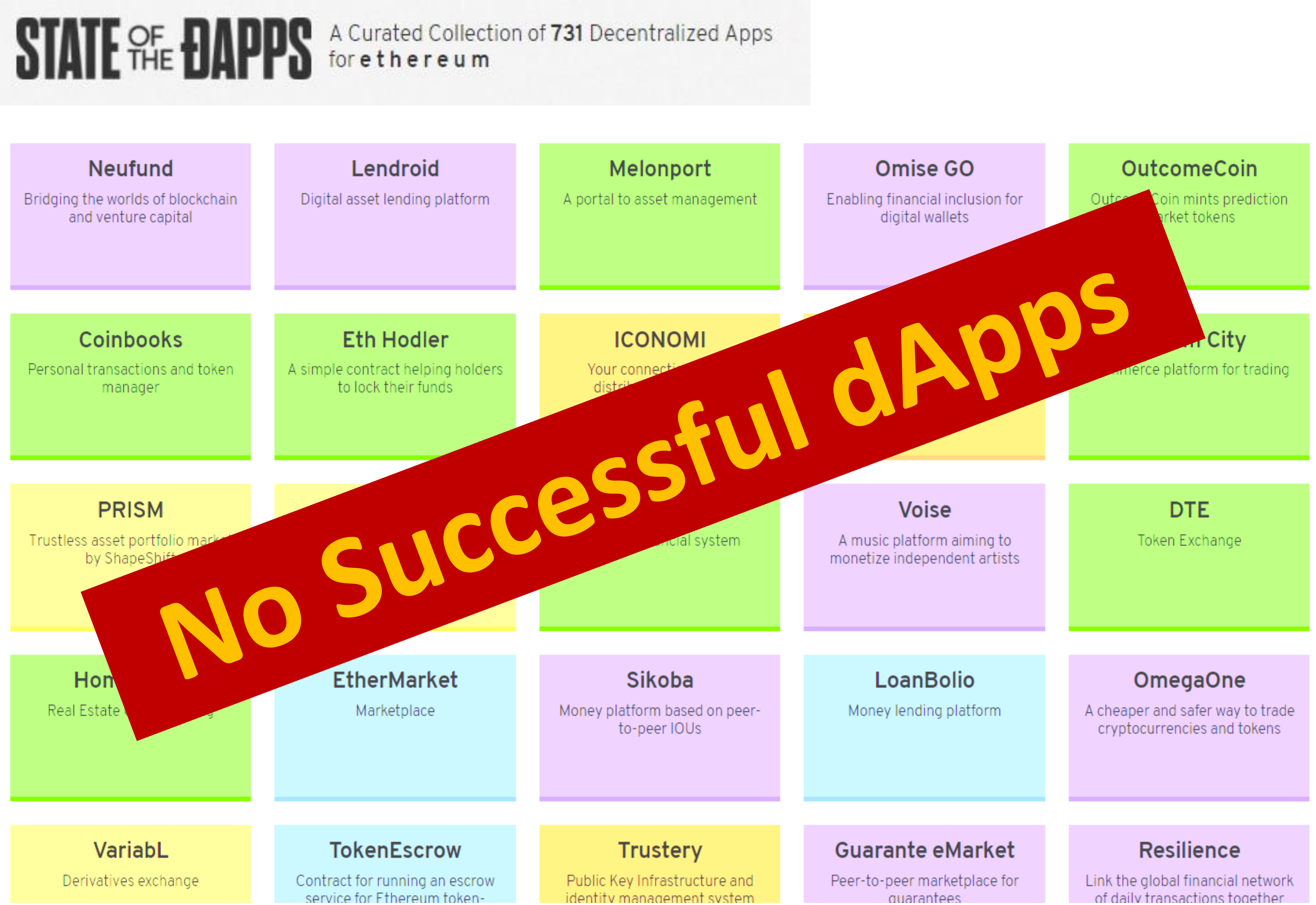
- Get Forms
- My Forms
- Importer Security Filing
- eManifest

www.cbinsights.com

Unbundling Procter & Gamble



Why dApps could not make a success



STATE OF THE ĐAPPS A Curated Collection of **731** Decentralized Apps for **ethereum**

Neufund
Bridging the worlds of blockchain and venture capital

Lendroid
Digital asset lending platform

Melonport
A portal to asset management

Omise GO
Enabling financial inclusion for digital wallets

OutcomeCoin
Outc Coin mints prediction rket tokens

Coinbooks
Personal transactions and token manager

Eth Hodler
A simple contract helping holders to lock their funds

ICONOMI
Your connecti distri

City
merce platform for trading

PRISM
Trustless asset portfolio mark by ShapeShift

cial system

Voise
A music platform aiming to monetize independent artists

DTE
Token Exchange

Hon
Real Estate

EtherMarket
Marketplace

Sikoba
Money platform based on peer-to-peer IOUs

LoanBolio
Money lending platform

OmegaOne
A cheaper and safer way to trade cryptocurrencies and tokens

VariabL
Derivatives exchange

TokenEscrow
Contract for running an escrow service for Ethereum token-

Trustery
Public Key Infrastructure and identity management system

Guarante eMarket
Peer-to-peer marketplace for guarantees

Resilience
Link the global financial network of daily transactions together

No Successful dApps

Problems of Decentralized Organization

Free riders

Rational ignorance

Tragedy of the Commons

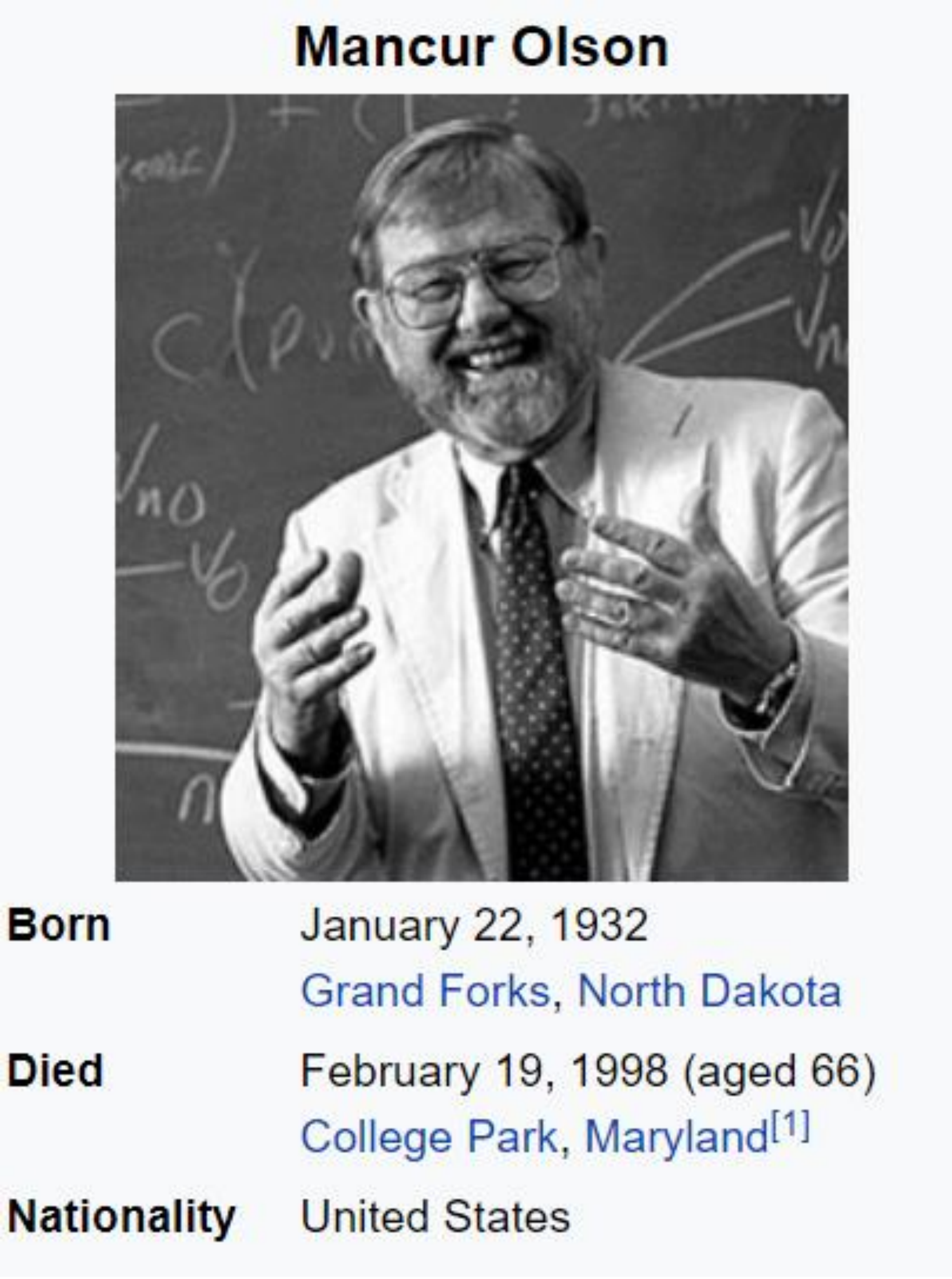
One of the Top 3 Economists during 2^{nd} half of the 20th Century

Institutional Economics

Public goods

Collective action

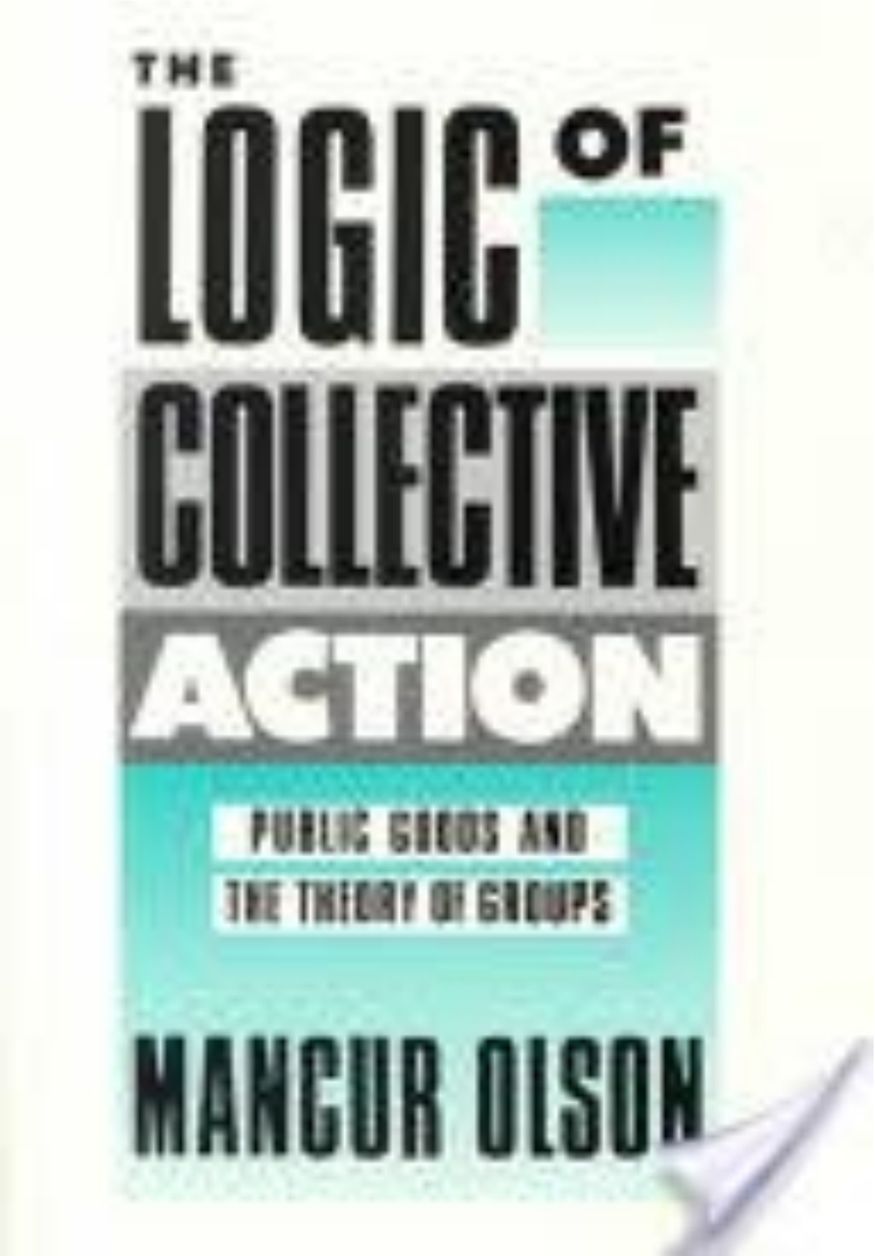
Economic development



Mancur Olson

Born	January 22, 1932 Grand Forks, North Dakota
Died	February 19, 1998 (aged 66) College Park, Maryland[1]
Nationality	United States

1965

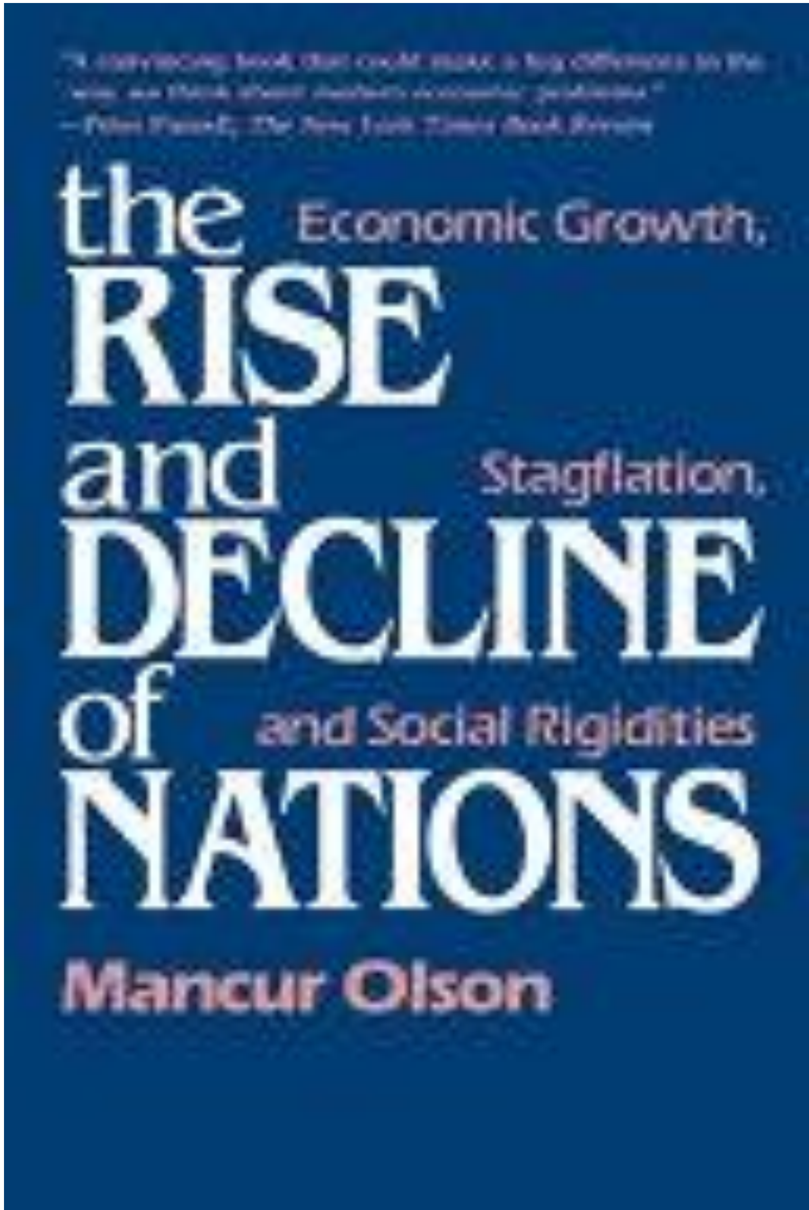


THE LOGIC OF COLLECTIVE ACTION

PUBLIC GOODS AND THE THEORY OF GROUPS

MANCUR OLSON

1982

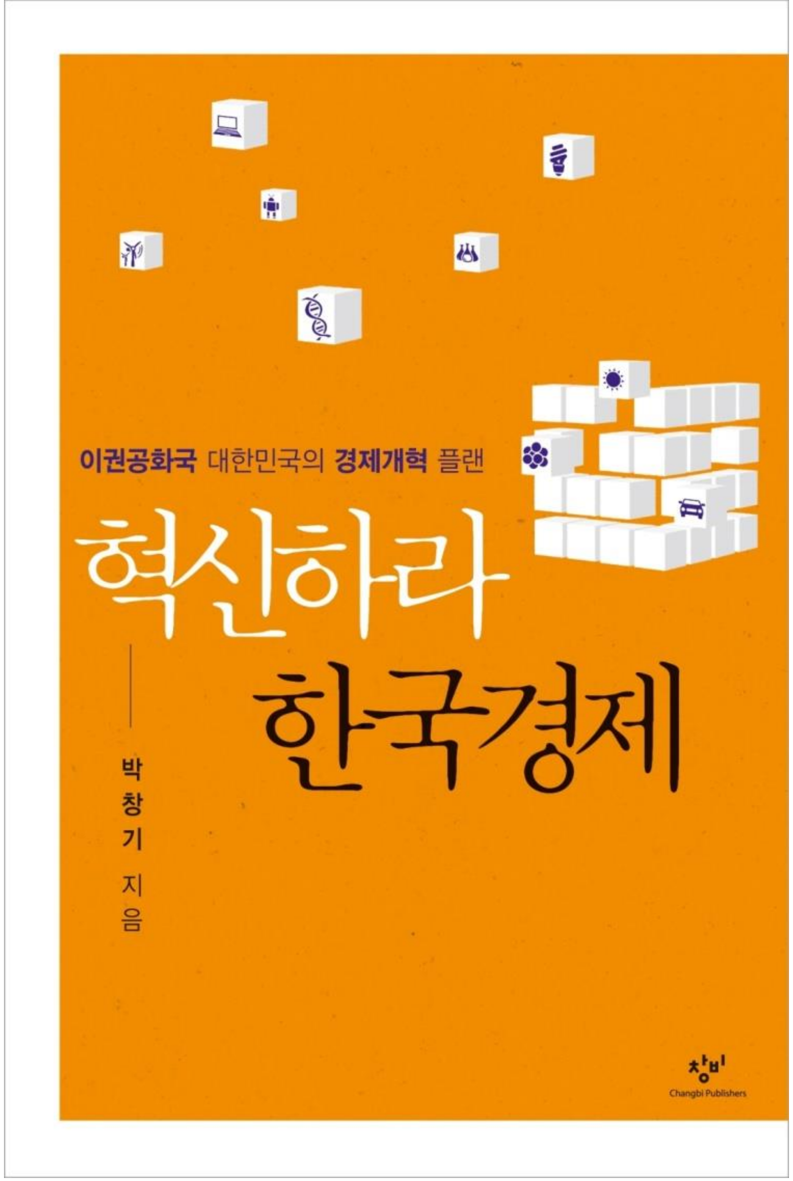


"A convincing book that could make a big difference in the way we think about nation's economic problems."
—Peter Passell, *The New York Times Book Review*

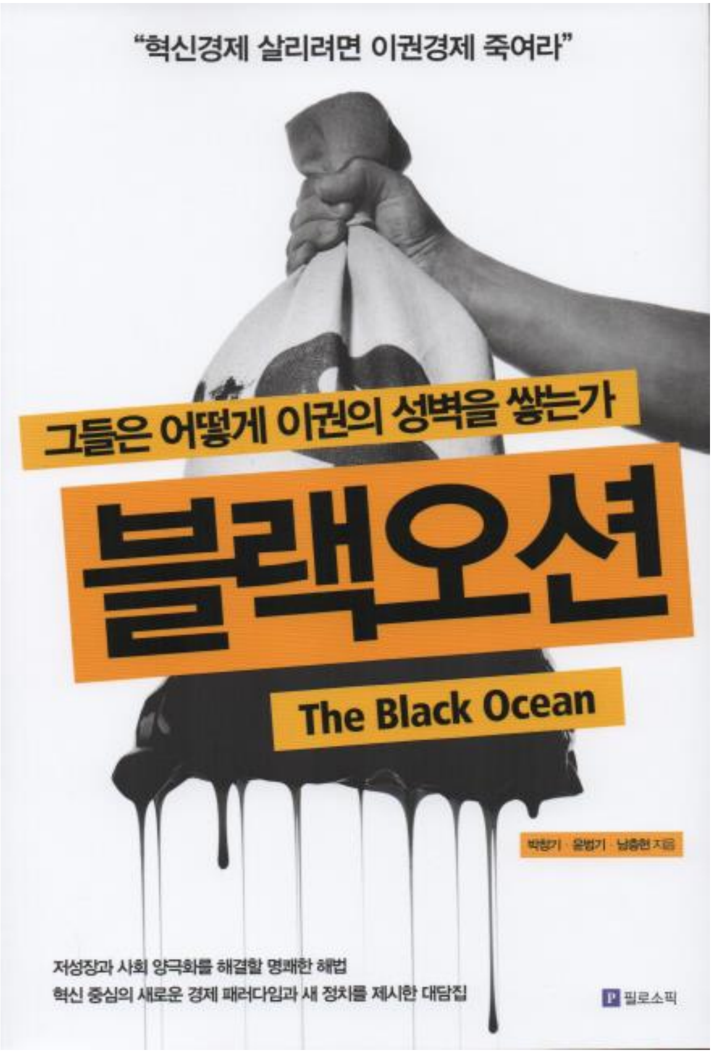
the RISE and DECLINE of NATIONS

Economic Growth,
Stagflation,
and Social Rigidities

Mancur Olson


이권공화국 대한민국의 경제개혁 플랜
혁신하라 한국경제
박창기 지음
창비
Changbi Publishers

2012년


"혁신경제 살리려면 이권경제 죽여라"
그들은 어떻게 이권의 성벽을 쌓는가
블랙오션
The Black Ocean
박창기 · 윤범기 · 남충현 지음
저성장과 사회 양극화를 해결할 명쾌한 해법
혁신 중심의 새로운 경제 패러다임과 새 정치를 제시한 대담집
필로소픽

2013년

큰 조직은

구성원 모두에게

이익이 있어도

잘 만들어지지 않는다.

모두에겐 이익이 되고

주도자에게는

큰 이익이 생겨야 한다.

인간은 이기적이고 합리적이라는 가정

각 개인은 집단활동을 위한 투자보다
그 결과로 얻는 이익이 크면 참여한다.

투자<이익 → 행동

가설 1.

한 집단이 속해 있는 구성원들이

공통의 이익을 갖게 되면

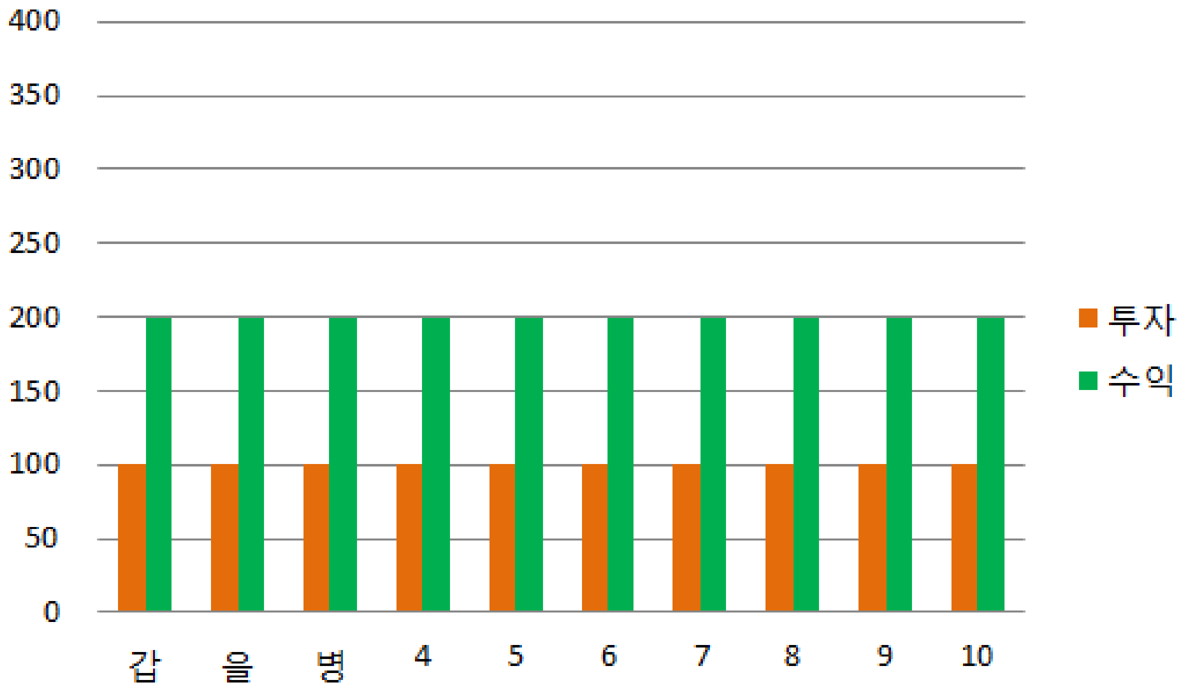
구성원들은 공동이익을 위한

공공재를 만들어 간다

가설 1.

Model A

	투자	수익
갑	100	200
을	100	200
병	100	200
4	100	200
5	100	200
6	100	200
7	100	200
8	100	200
9	100	200
10	100	200
합계	1,000	2,000



명제 1.

숫자가 많은 집단의 개개인은
집단의 공동이익을 위해 행동하지 않는
경향이 있다.

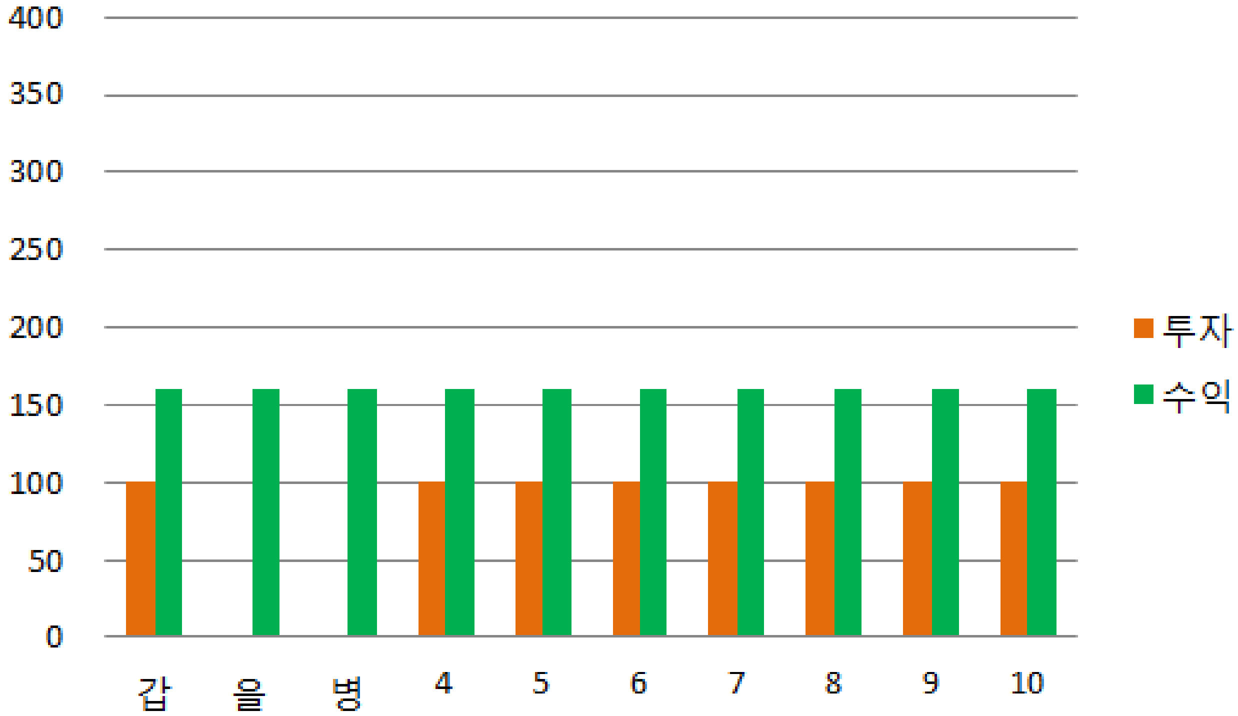
무임승차 경향 free-ride → 가설1 틀려

합리적 무시 rational ignorance

명제 1

Model B

	투자	수익
갑	100	160
을	0	160
병	0	160
4	100	160
5	100	160
6	100	160
7	100	160
8	100	160
9	100	160
10	100	160
합계	800	1,600



명제 2.

대규모 집단이 만들어지는 원리는

다수에게 주는 공공재의 편익은 필요조건이며

집단을 주도하는 소수에게 주는

‘차별적 부추김’ Selective incentive이

충분조건이다.

대의제 정당의 수혜자는?

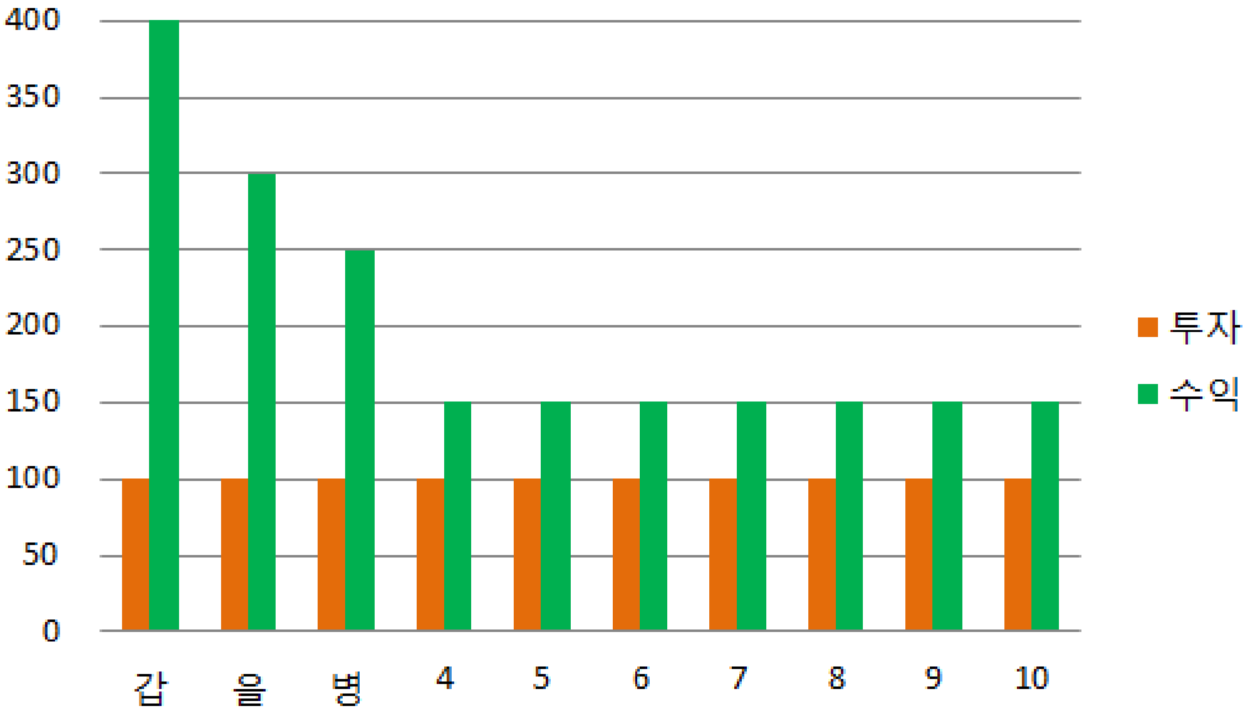
영국 노동조합 1890년경 산업혁명 후 100년

한국 노동조합 1987년경 산업화 후 20년

명제 2

Model C

	투자	수익
갑	100	400
을	100	300
병	100	250
4	100	150
5	100	150
6	100	150
7	100	150
8	100	150
9	100	150
10	100	150
합계	1,000	2,000



집단이 생기는 이유: 차별적 부추김

- 긍정적 Positive Selective incentive

  지도자에게 금전적 혜택과 존경, 명예 부여

  소속원에게 선전으로 정보와 소속감.

  단체구매, 사단법인화 혜택, 집단 이익 관철

- 음의 Negative Selective incentive

  노조 강제 가입, 회비강제 납부

  세금 안내면 벌금 부과

  병역 의무 기피하면 징역

공공재는 모든 구성원이 수용해야 한다.
국가는 하나의 법률체계 세금정책,
하나의 국방정책을 갖는다.

공공재는 집단은 주도하는 사람들을 위한
차별적인 부추김 때문에 생겨나므로
모든 구성원을 만족시키기는 어렵다. 따라서,

명제 3. 공공재의 성격, 비용, 만드는 방법에 대한
집단 내 합의는 어렵다.

집단이 클수록 협상과 설득에 **시간**과 비용이 많이 든다.

명제 4.

구성원 수가 작은 집단은 비용에 비해 편익이 크면 차별적 부추김이 없어도 빠르게 만들어진다.

마피아 조직

기업 카르텔, 담합

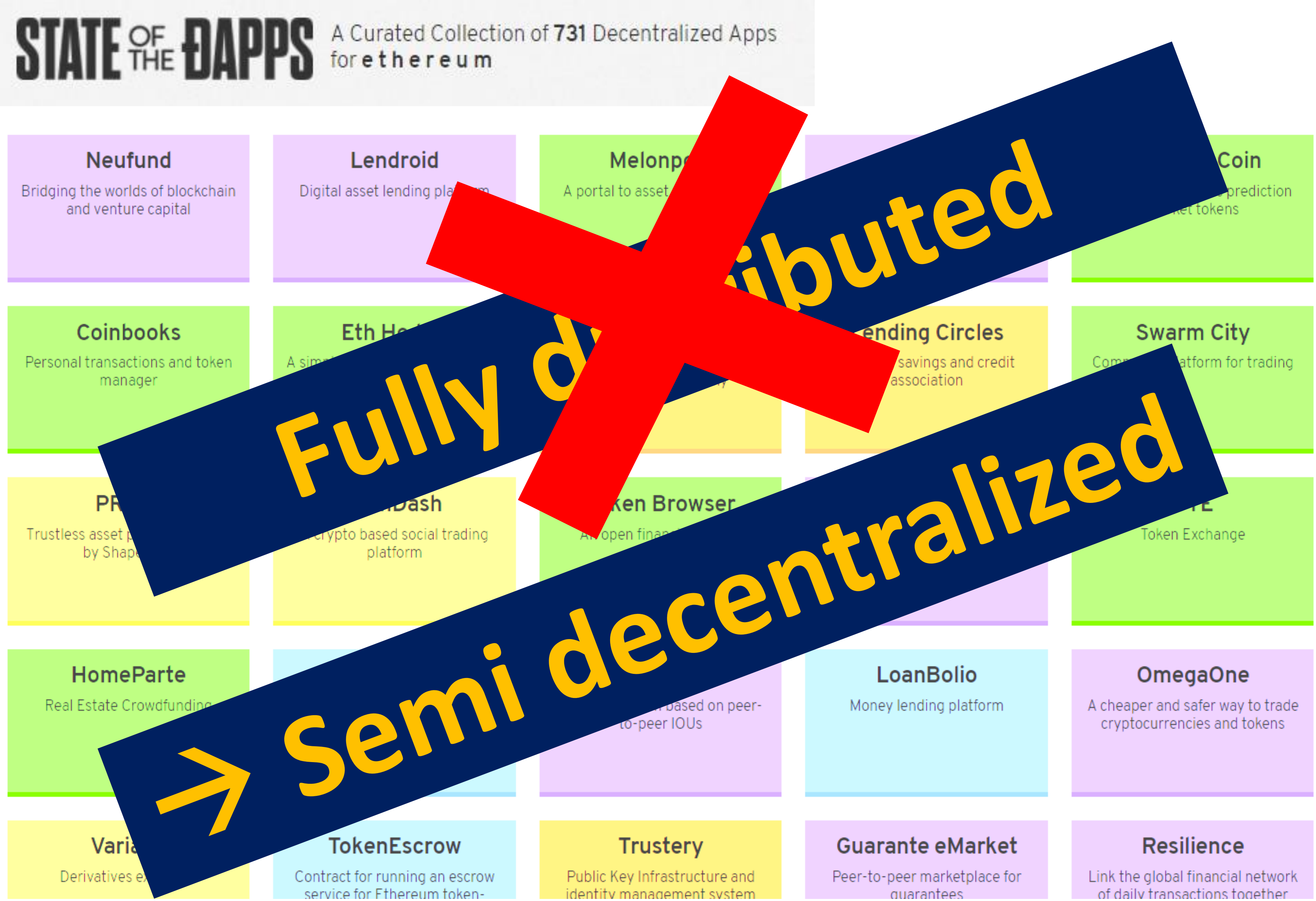
정권 탈취 쿠데타 집단

집권 목적 정치 집단

고전학파, 시장근본주의 기본 가정에 대한 부정

- 아담 스미스의 보이지 않는 손
- Walras의 일반균형이론
- 파레토 최적

각자가 이기적으로 행동해도
시장의 수요 공급 메커니즘에 따라
균형을 찾게 되고 자원은 최적 분배된다.



STATE OF THE ĐAPPS

A Curated Collection of **731** Decentralized Apps for ethereum

Neufund
Bridging the worlds of blockchain and venture capital

Lendroid
Digital asset lending pla… m

Melonp…
A portal to asset…

…Coin
…prediction
…ket tokens

Coinbooks
Personal transactions and token manager

Eth He…
A sim…

…ending Circles
…savings and credit association

Swarm City
Com… …atform for trading

PR…
Trustless asset p…
by Shap…

…Dash
…crypto based social trading platform

…ken Browser
An open fina…

…E
Token Exchange

HomeParte
Real Estate Crowdfunding

…based on peer-to-peer IOUs

LoanBolio
Money lending platform

OmegaOne
A cheaper and safer way to trade cryptocurrencies and tokens

Varia…
Derivatives ex…

TokenEscrow
Contract for running an escrow service for Ethereum token-

Trustery
Public Key Infrastructure and identity management system

Guarantee eMarket
Peer-to-peer marketplace for guarantees

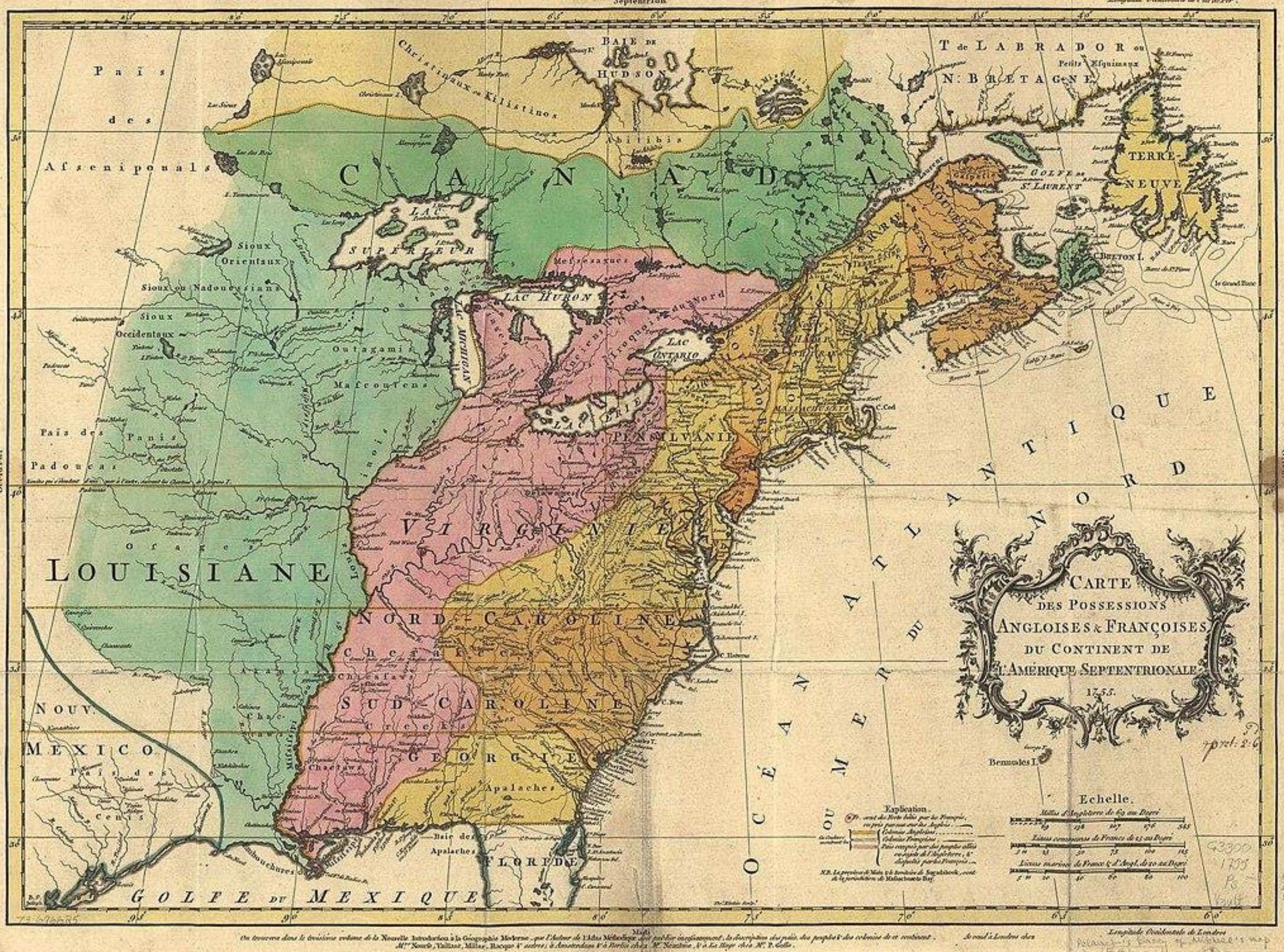
Resilience
Link the global financial network of daily transactions together

~~Fully distributed~~

→ Semi decentralized

Septentrion

Longitude Occidentale de l'Isle de Fer.



CARTE DES POSSESSIONS ANGLOISES & FRANÇOISES DU CONTINENT DE L'AMÉRIQUE SEPTENTRIONALE

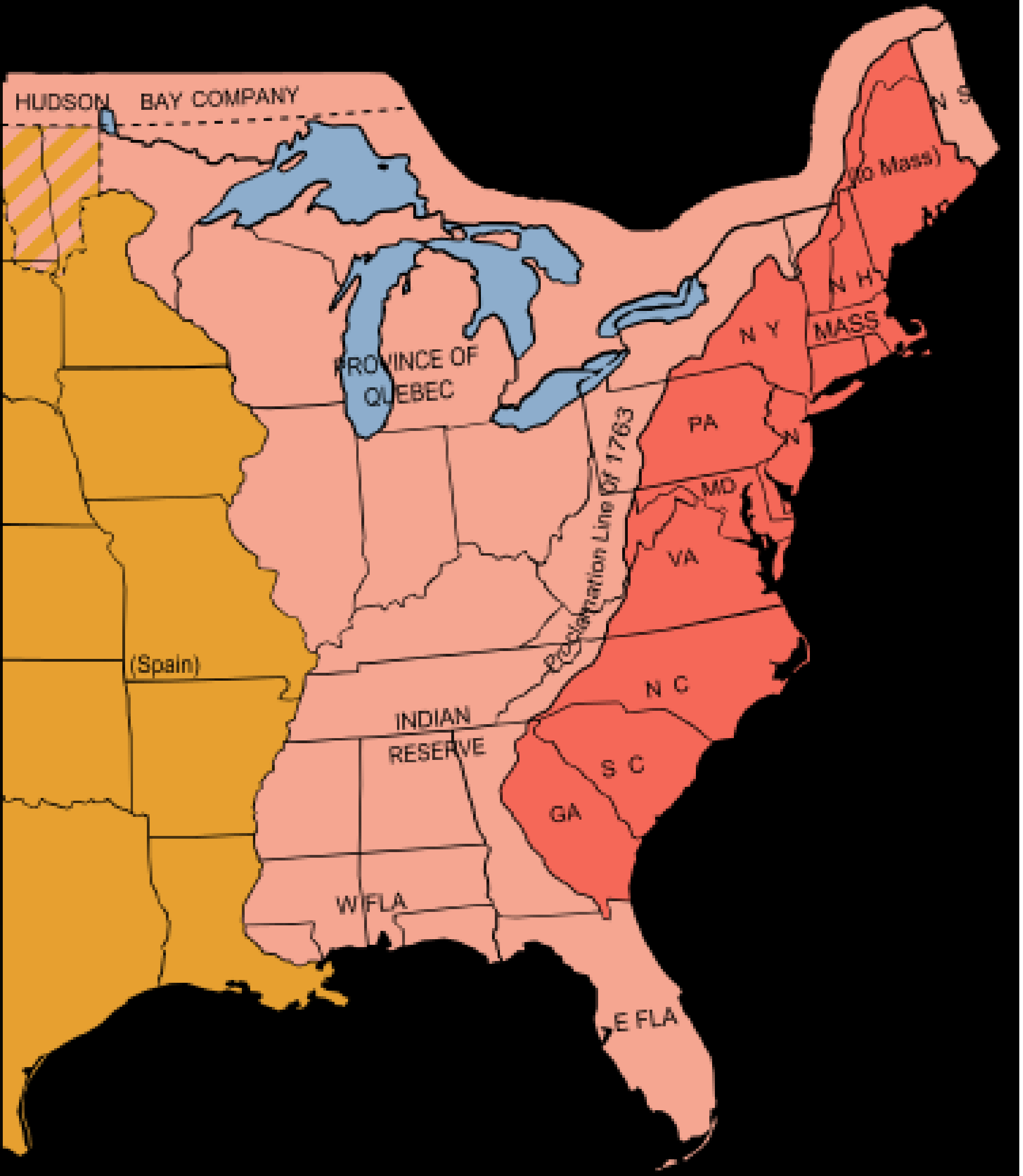
1755.

Explication.

Midi

On trouvera dans le troisième volume de la Nouvelle Introduction à la Géographie Moderne, par l'Auteur de l'Atlas Méthodique, doit publier incessamment, la description des païs, des peuples & des colonies de ce continent. Se vend à Londres chez Mrs. Nourse, Vaillant, Millar, Rocque & autres; à Amsterdam & à Berlin chez Mr. Neaulme, & à La Haye chez Mr. P. Gosse.

Longitude Occidentale de Londres



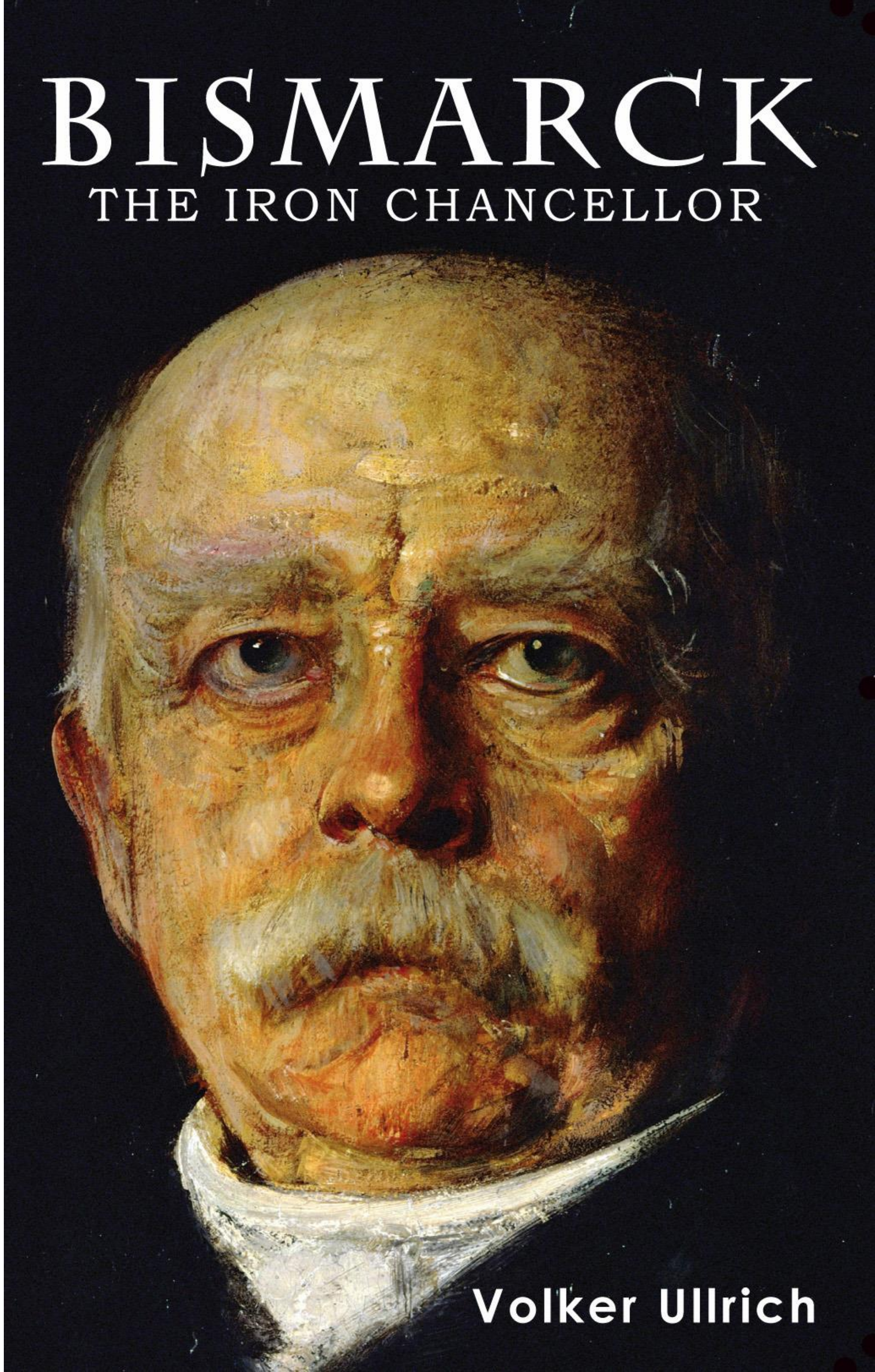
Declaration of Union

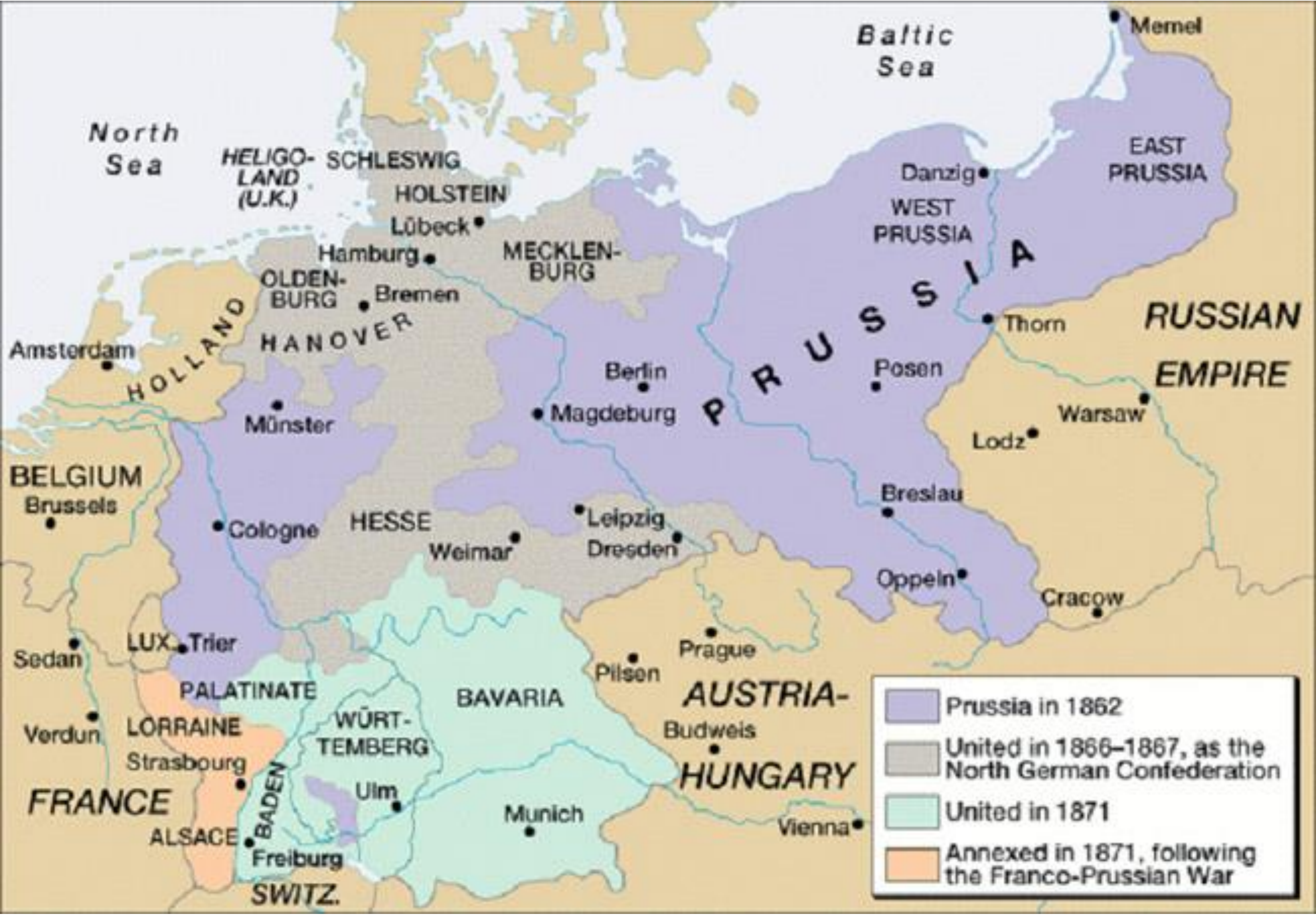
1776

1871년

독일 통일

봉건 계급 질서의 파괴

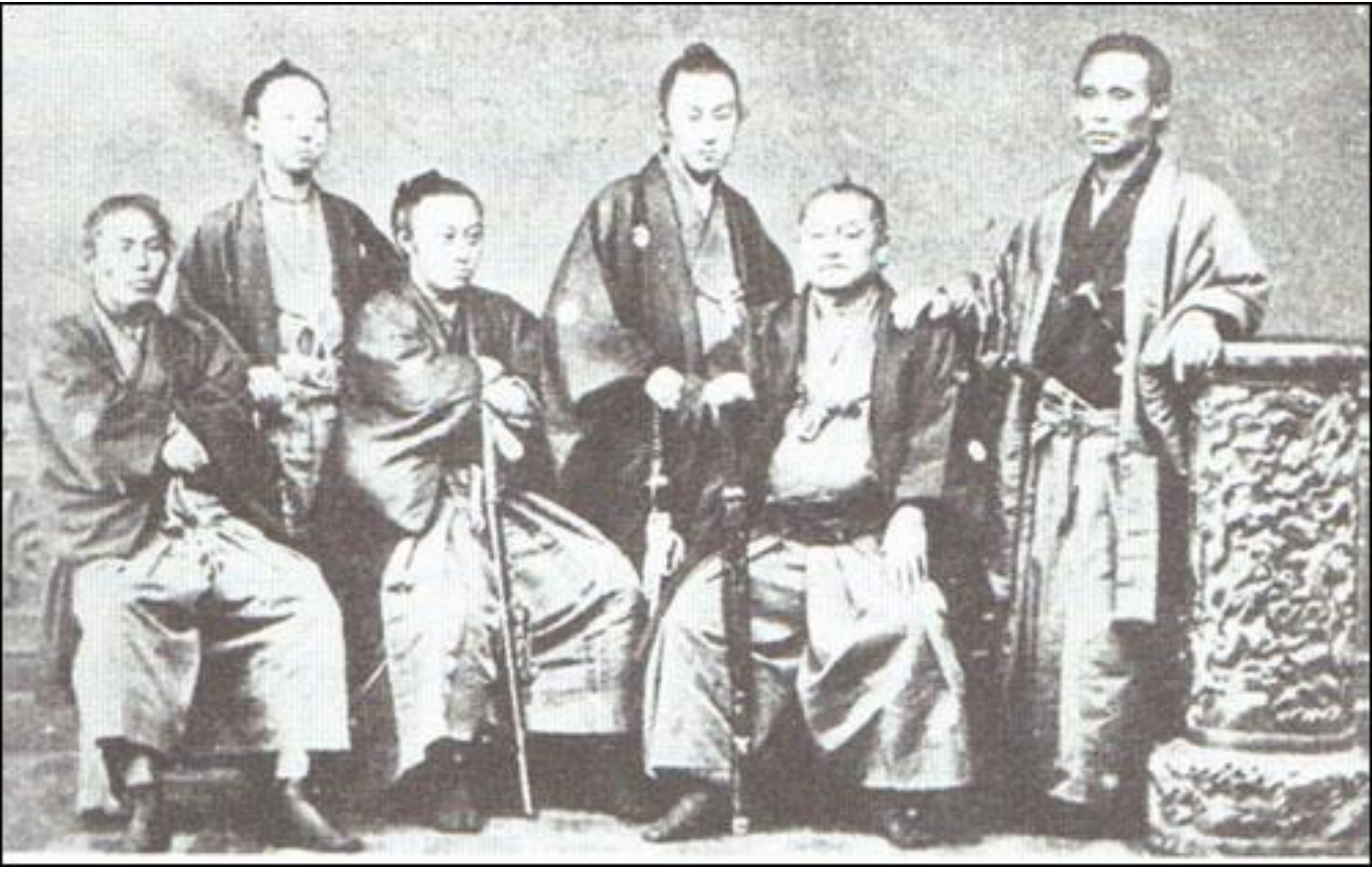



Baltic Sea
Memel
North Sea
HELIGOLAND (U.K.)
SCHLESWIG
HOLSTEIN
Lübeck
Hamburg
MECKLENBURG
OLDENBURG
Bremen
HANOVER
Danzig
EAST PRUSSIA
WEST PRUSSIA
PRUSSIA
Thorn
RUSSIAN EMPIRE
Amsterdam
HOLLAND
Berlin
Posen
Münster
Magdeburg
Warsaw
Lodz
BELGIUM
Brussels
Breslau
Cologne
HESSE
Leipzig
Weimar
Dresden
Oppeln
Cracow
LUX.
Trier
Sedan
Prague
Pilsen
PALATINATE
BAVARIA
AUSTRIA-HUNGARY
Verdun
LORRAINE
WÜRTTEMBERG
Budweis
Strasbourg
BADEN
Ulm
FRANCE
Munich
Vienna
ALSACE
Freiburg
SWITZ.
Prussia in 1862
United in 1866–1867, as the North German Confederation
United in 1871
Annexed in 1871, following the Franco-Prussian War

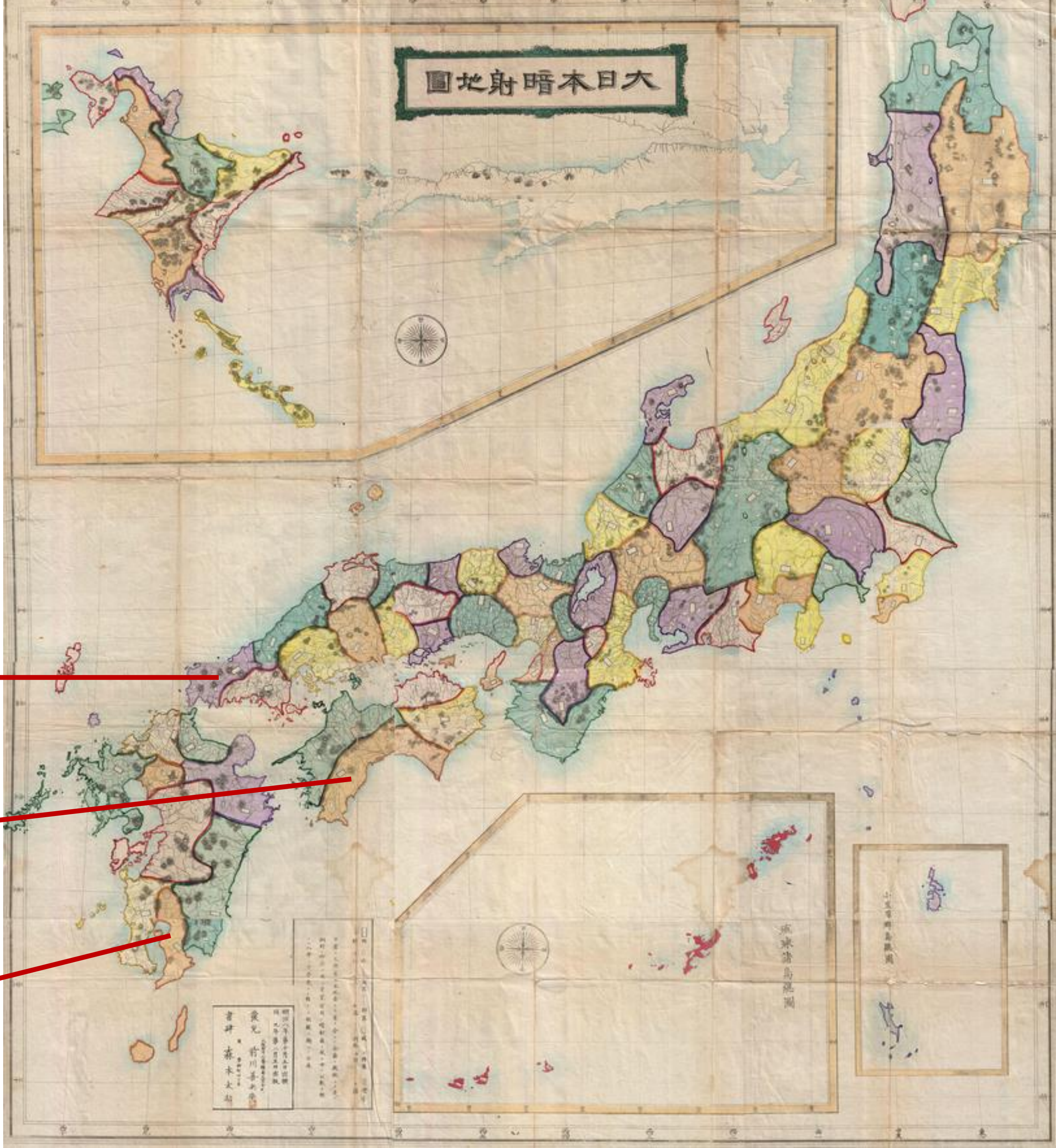
1871

메이지 유신 明治維新

폐번치현 廢藩置県



메이지유신을 주도한 사쓰마번·조슈번의 젊은 무사들. 맨 왼쪽이 이토우 히로부미다.
그도 하급 무사 집안의 자제였다. 이 사진은 1869년에 도쿄에서 촬영된 사진이다.

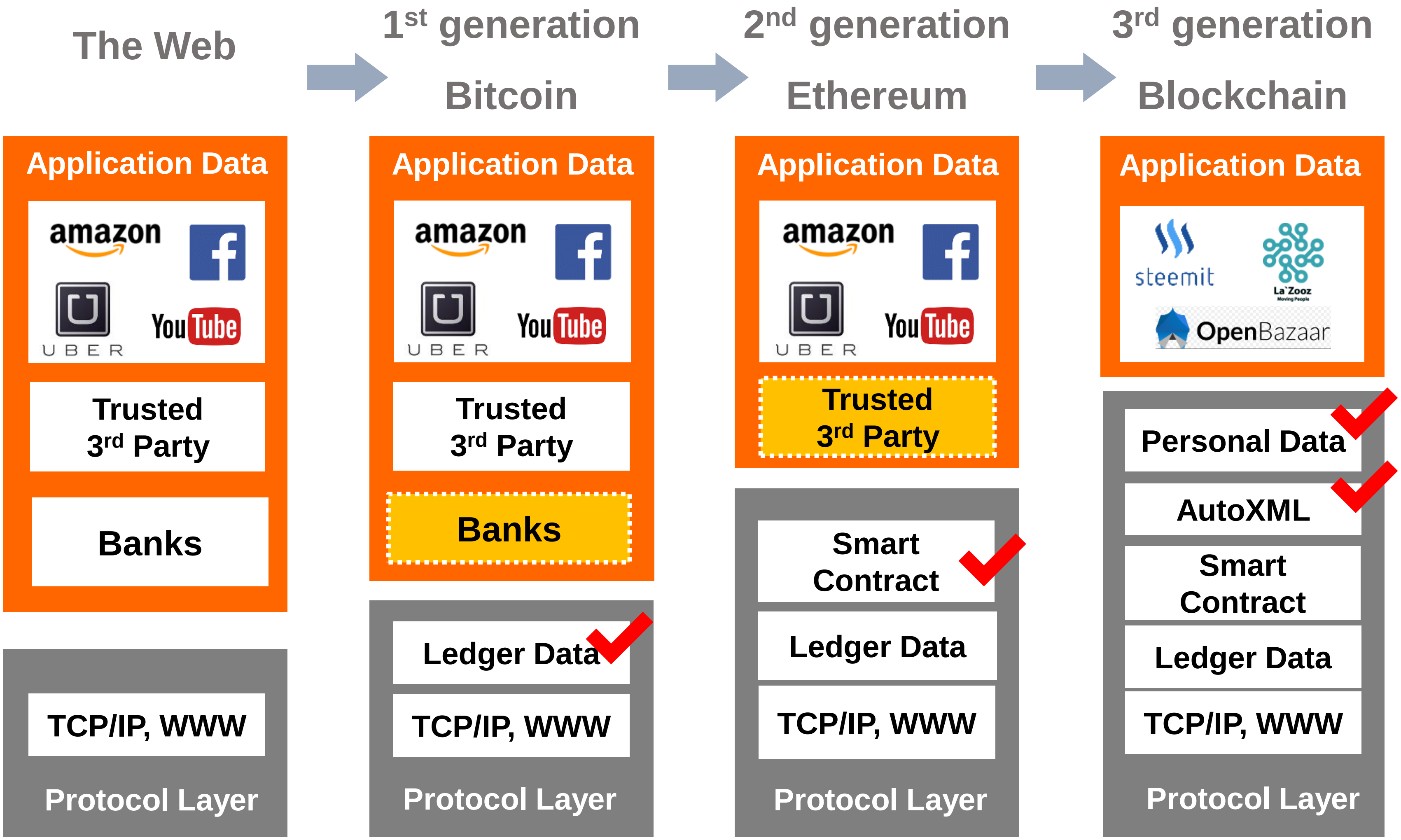


조슈, 야마구치
이또오 히로부미

도사번, 료마

사쓰마, 가고시마
사이고 다까모리

Blockchain Evolution & Intrinsic Value



The Web

Application Data

Trusted 3rd Party

Banks

TCP/IP, WWW

Protocol Layer

1st generation

Bitcoin

Application Data

Trusted 3rd Party

Banks

Ledger Data ✓

TCP/IP, WWW

Protocol Layer

2nd generation

Ethereum

Application Data

Trusted 3rd Party

Smart Contract ✓

Ledger Data

TCP/IP, WWW

Protocol Layer

3rd generation

Blockchain

Application Data

Personal Data ✓

AutoXML ✓

Smart Contract

Ledger Data

TCP/IP, WWW

Protocol Layer

Data Standardization

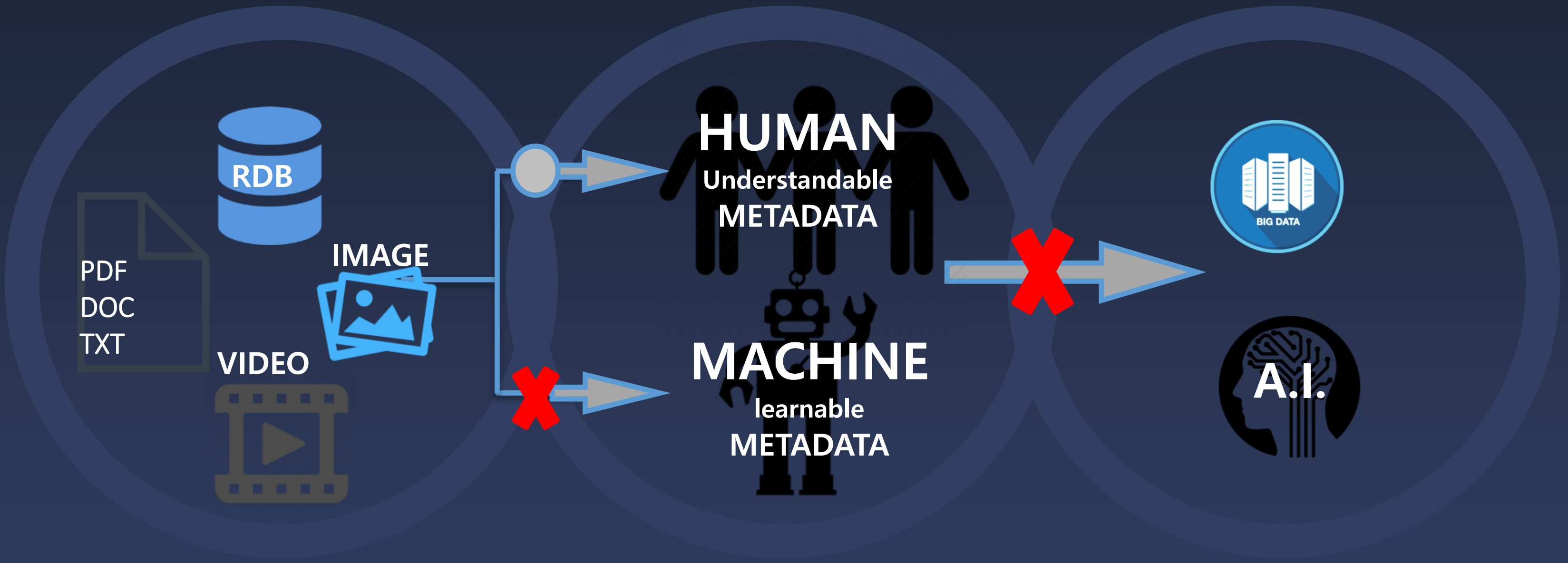
via

AutoXML

AutoXML

Advantages of AutoXML in Big Data/ AI

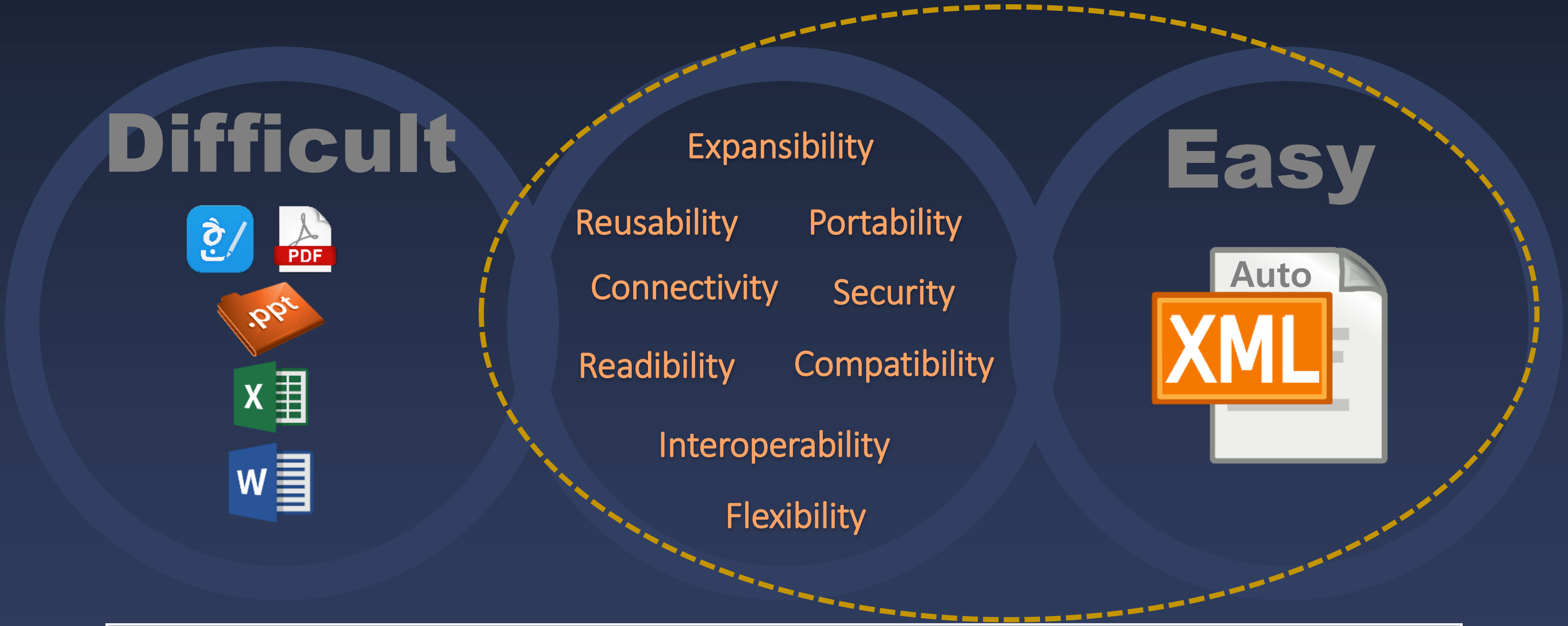
Problems with existing methods



Machine can’t read!

Because existing data sources are not understood by machines, they are difficult to use in Big Data and AI.

WHY AutoXML



Difficult

Expansibility

Reusability

Portability

Connectivity

Security

Readibility

Compatibility

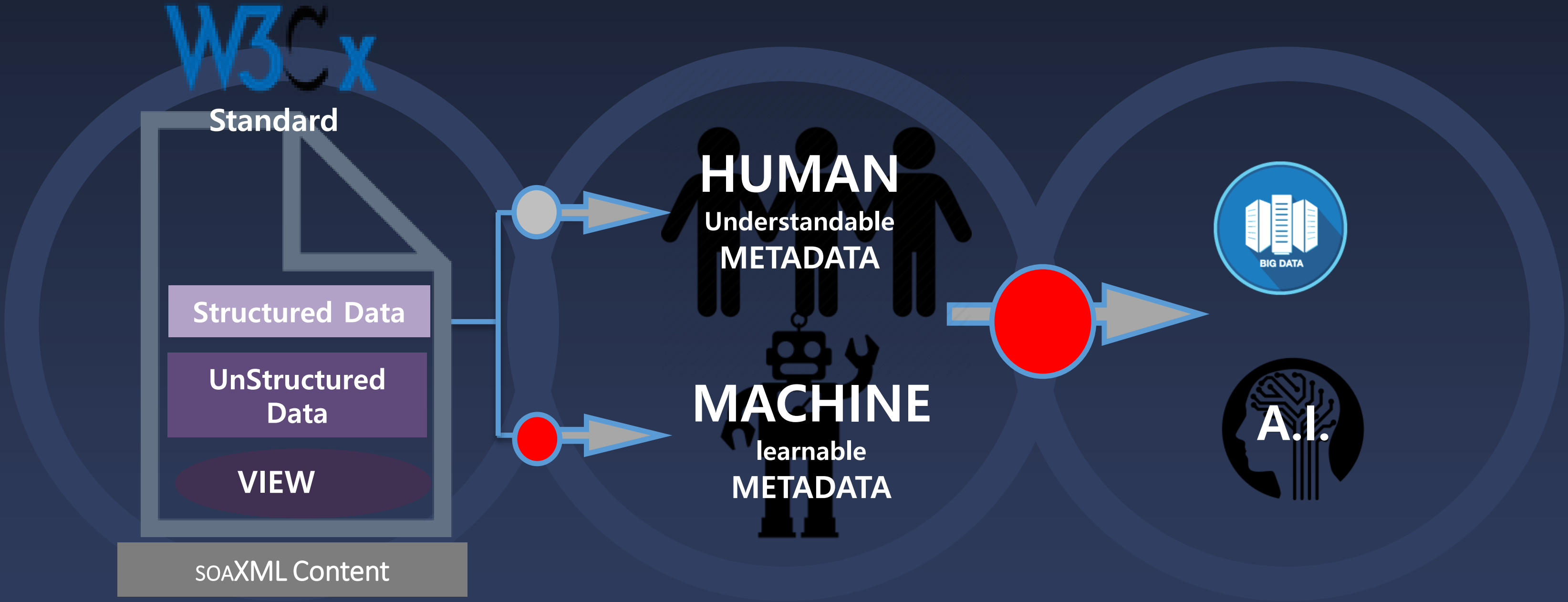
Interoperability

Flexibility

Easy

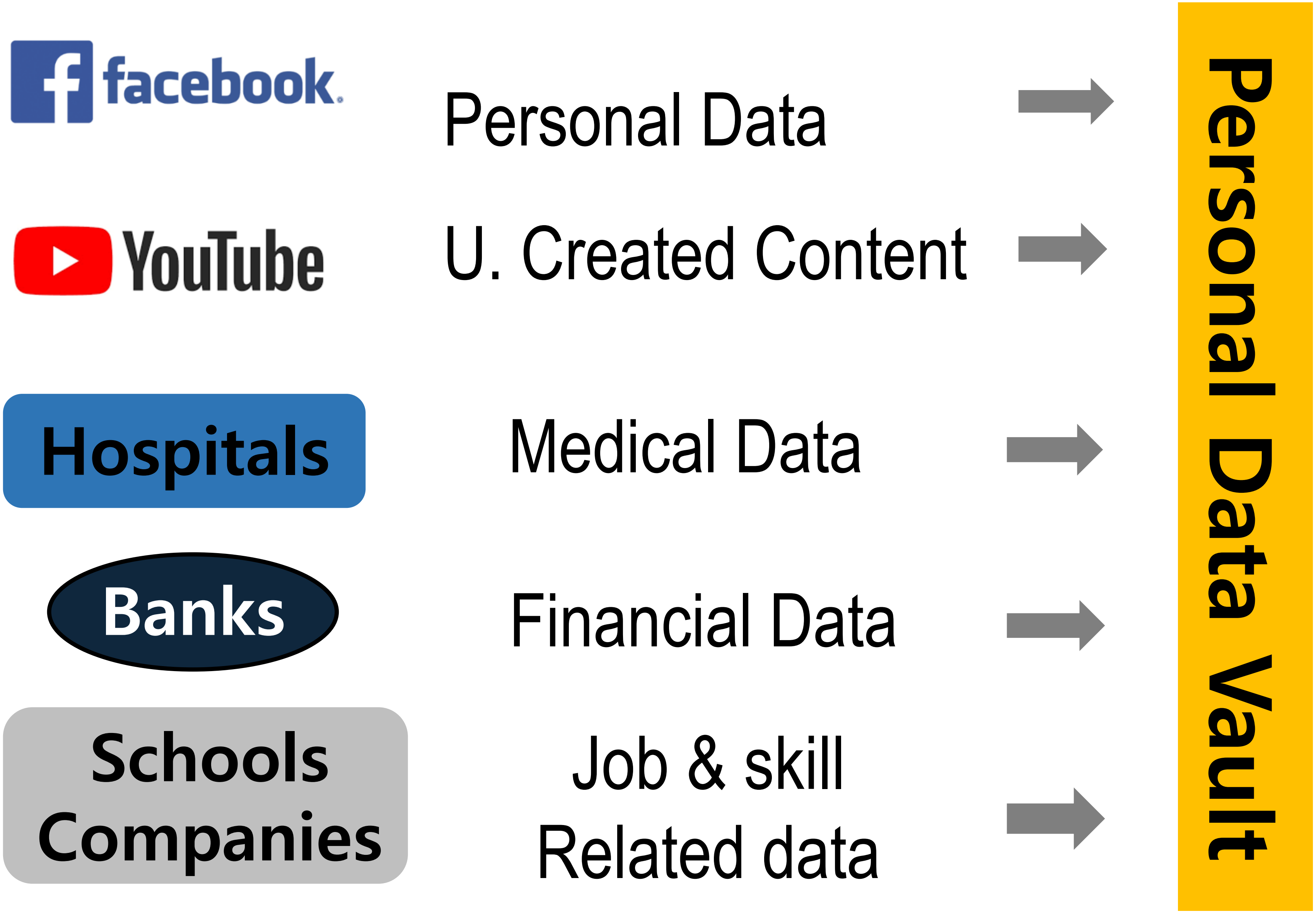
Machine CAN read!

AutoXML



Machine CAN read!

XML content created with AutoXML technology can be understood by both human and machine.



facebook — Personal Data →

YouTube — U. Created Content →

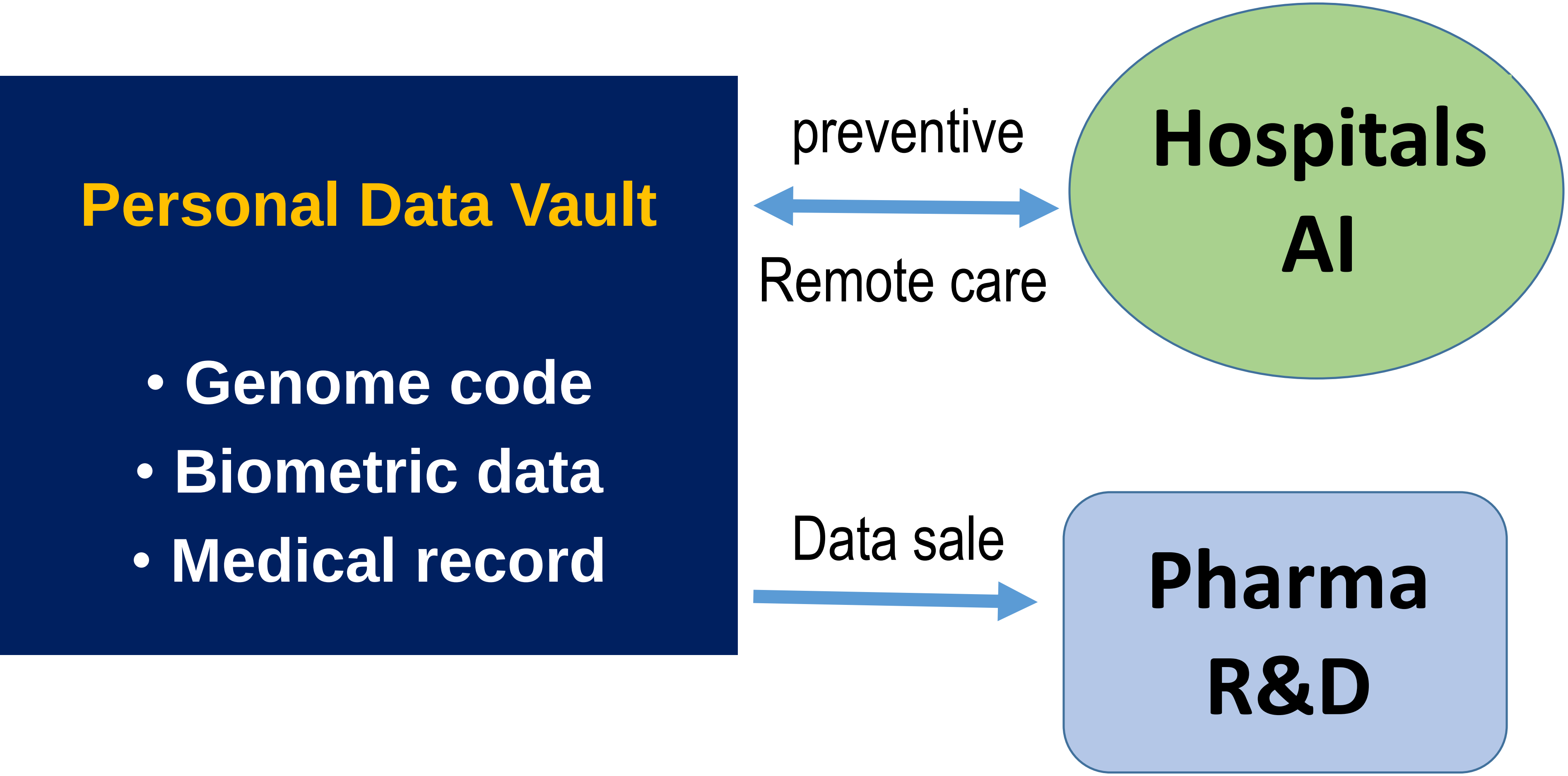
Hospitals — Medical Data →

Banks — Financial Data →

Schools Companies — Job & skill Related data →

Personal Data Vault

Medical & Health



Personal Data Vault

- Genome code
- Biometric data
- Medical record

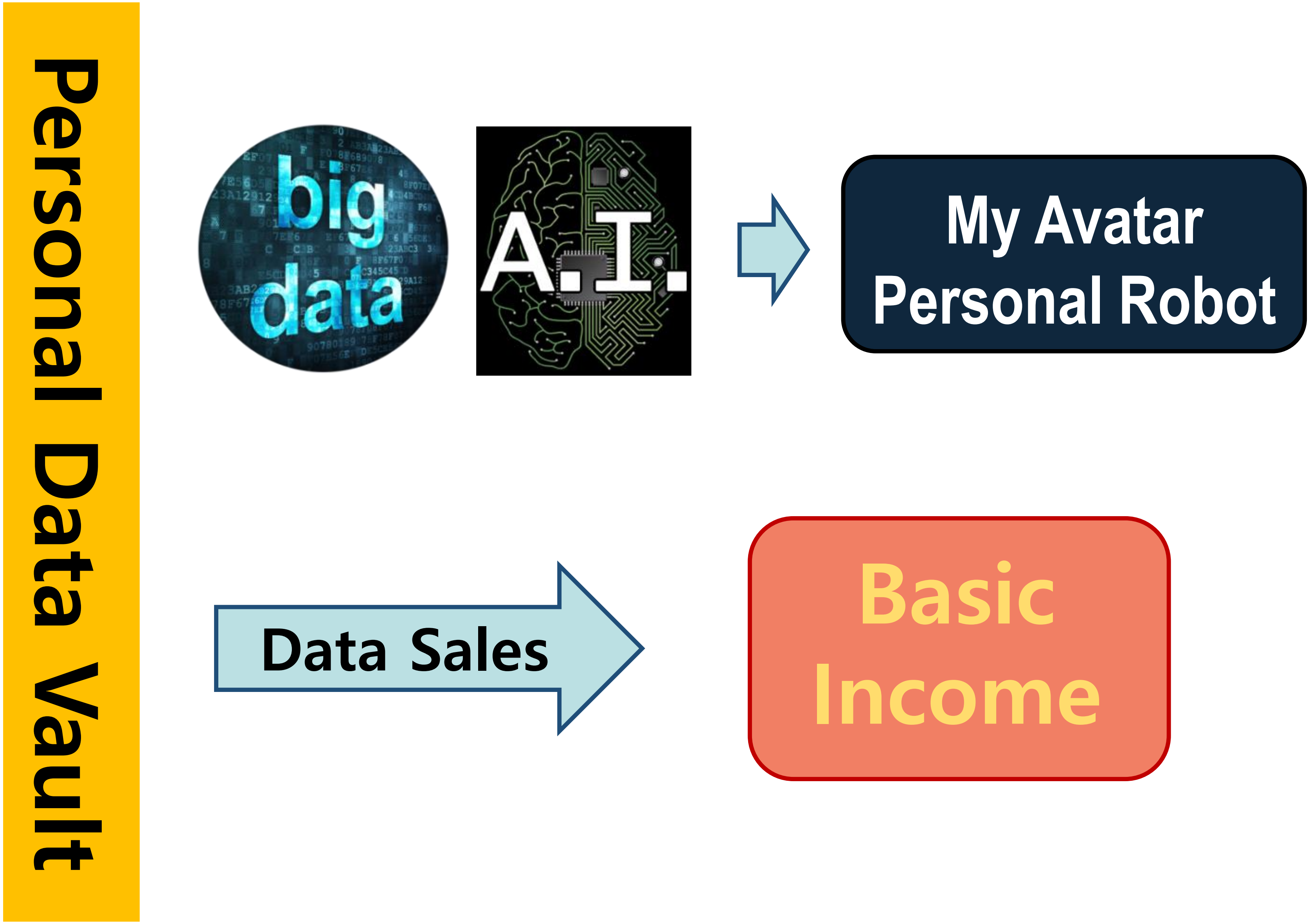
preventive

Remote care

Hospitals AI

Data sale

Pharma R&D



Personal Data Vault

My Avatar
Personal Robot

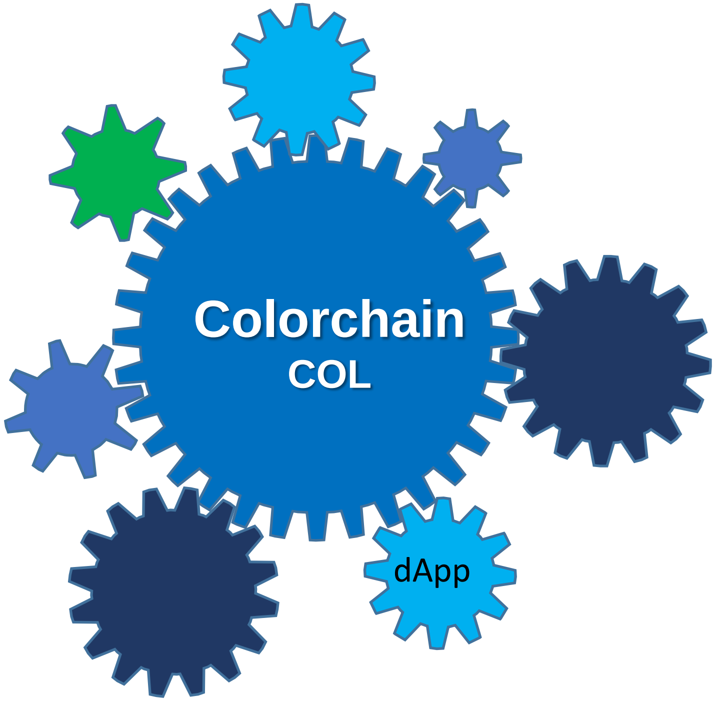
Data Sales

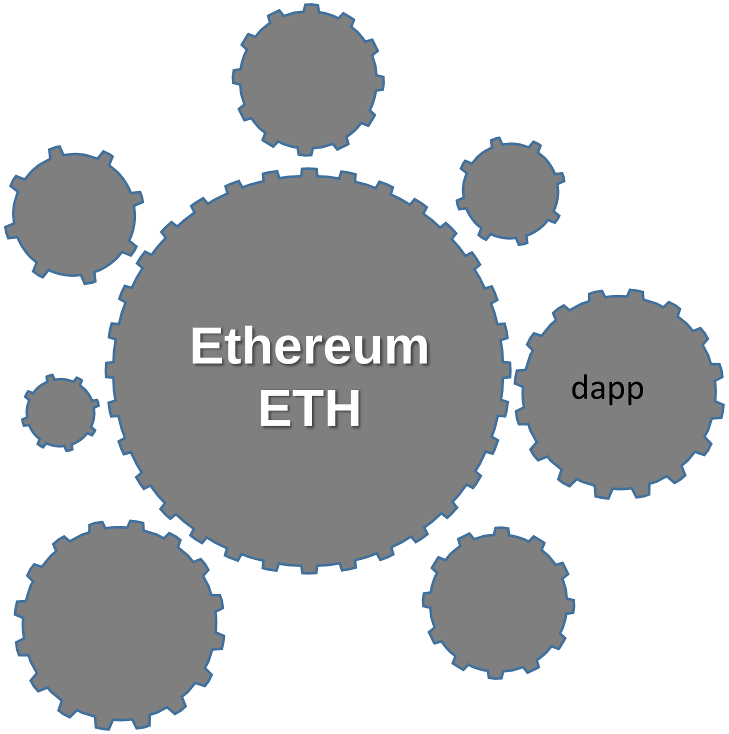
Basic
Income

Colorchain Ecosystem

Unified Currency
Unified Data Standard

Divided Currency
Fragmented Data





Semi-Decentralized

Fully Decentralized

Sungkyunkwan University

Networking for cryptocurrency

Hyoungshick Kim

Department of Software

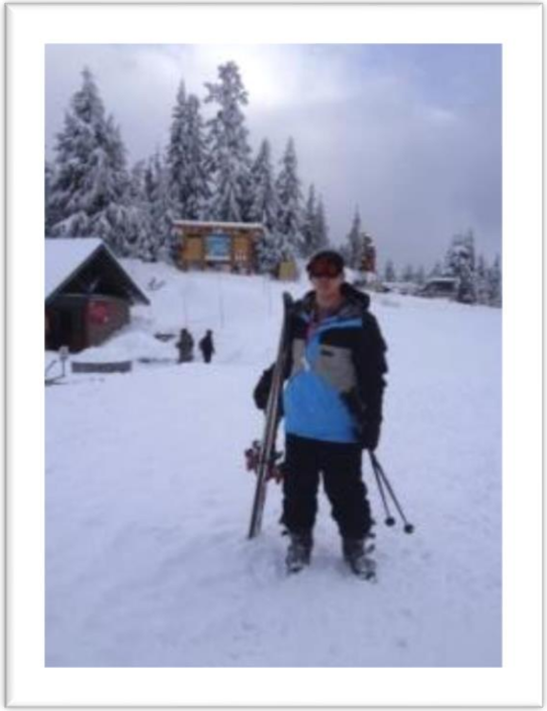
College of Software

Sungkyunkwan University

Hyoungshick Kim (김형식)

Assistant Professor in Department of Software, Sungkyunkwan University

- Education
  - ✓ Ph.D. in Computer Science, University of Cambridge
- Experiences
  - ✓ Professor, Sungkyunkwan University, Korea (2013 – present)
  - ✓ Postdoctoral Fellow, University of British Columbia, Canada (2012-2013)
  - ✓ Senior Engineer, Samsung Electronics (2004-2008)
- Research interests:
  - ✓ Security engineering
  - ✓ Usable security
  - ✓ Security vulnerability analysis
- Homepage: http://seclab.skku.edu/



- Lab members:
- Academic staff: 2
- PhD students: 5
- MS students: 12

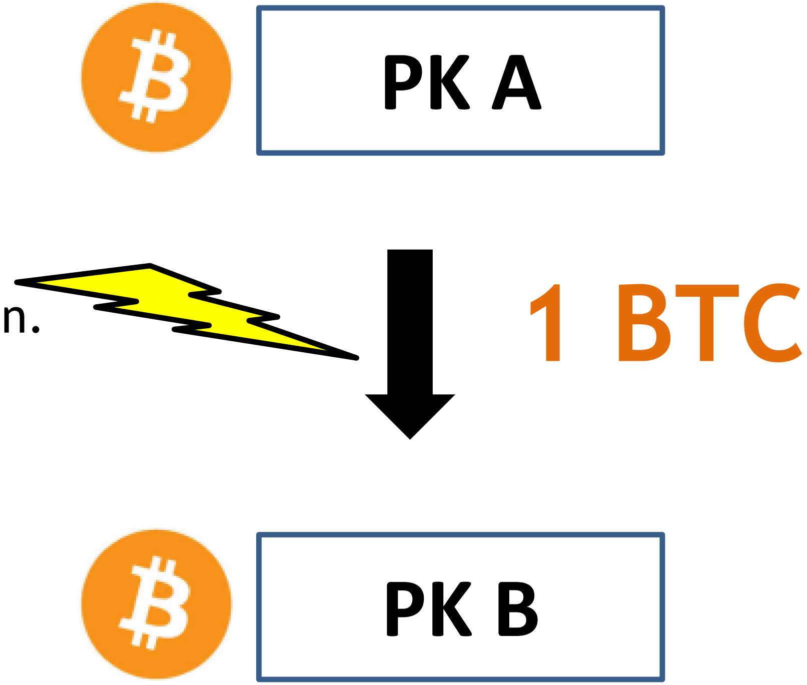
Bitcoin

- A distributed, decentralized digital currency system
- Invented by Satoshi Nakamoto 2008
- Private money based on
  - – cryptography
  - – a distributed transaction log (public ledger)
    - history shows how many bitcoins each user has

PK A

In a public ledger

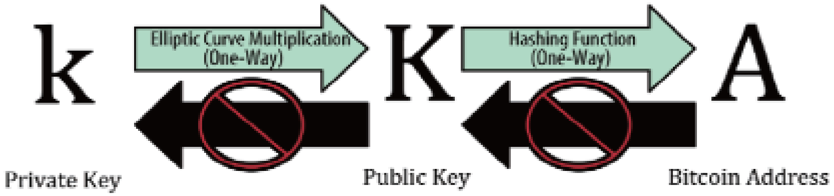
A's digital signature authorizes this transaction.

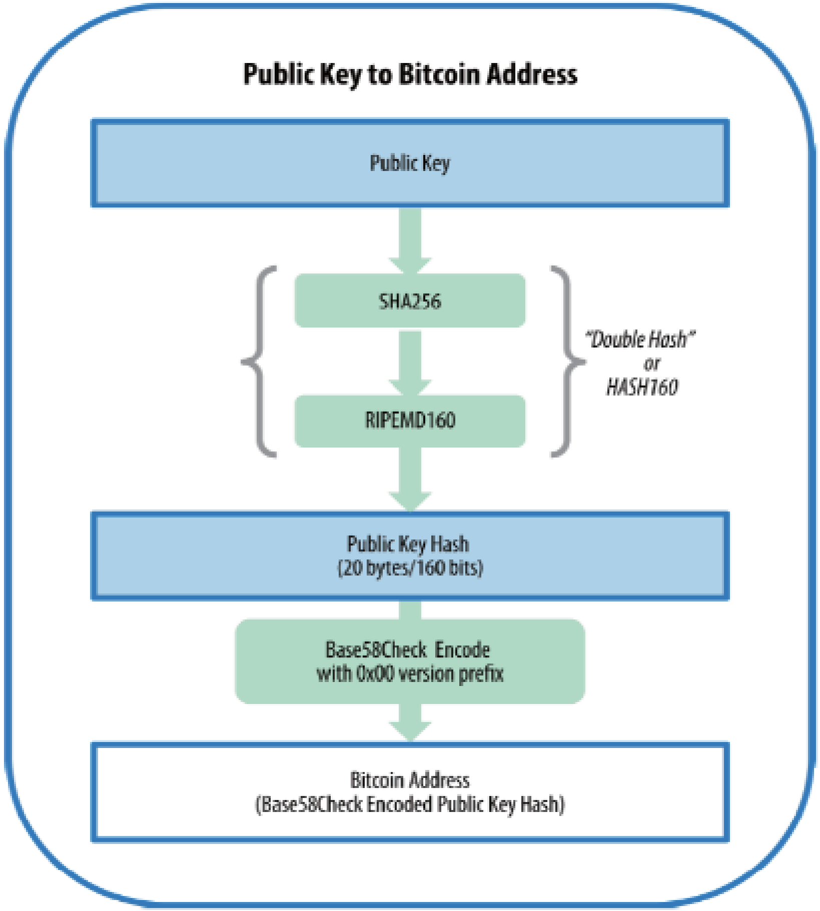


PK A: 1 BTC

PK B: 2 BTC

Bitcoin key and address



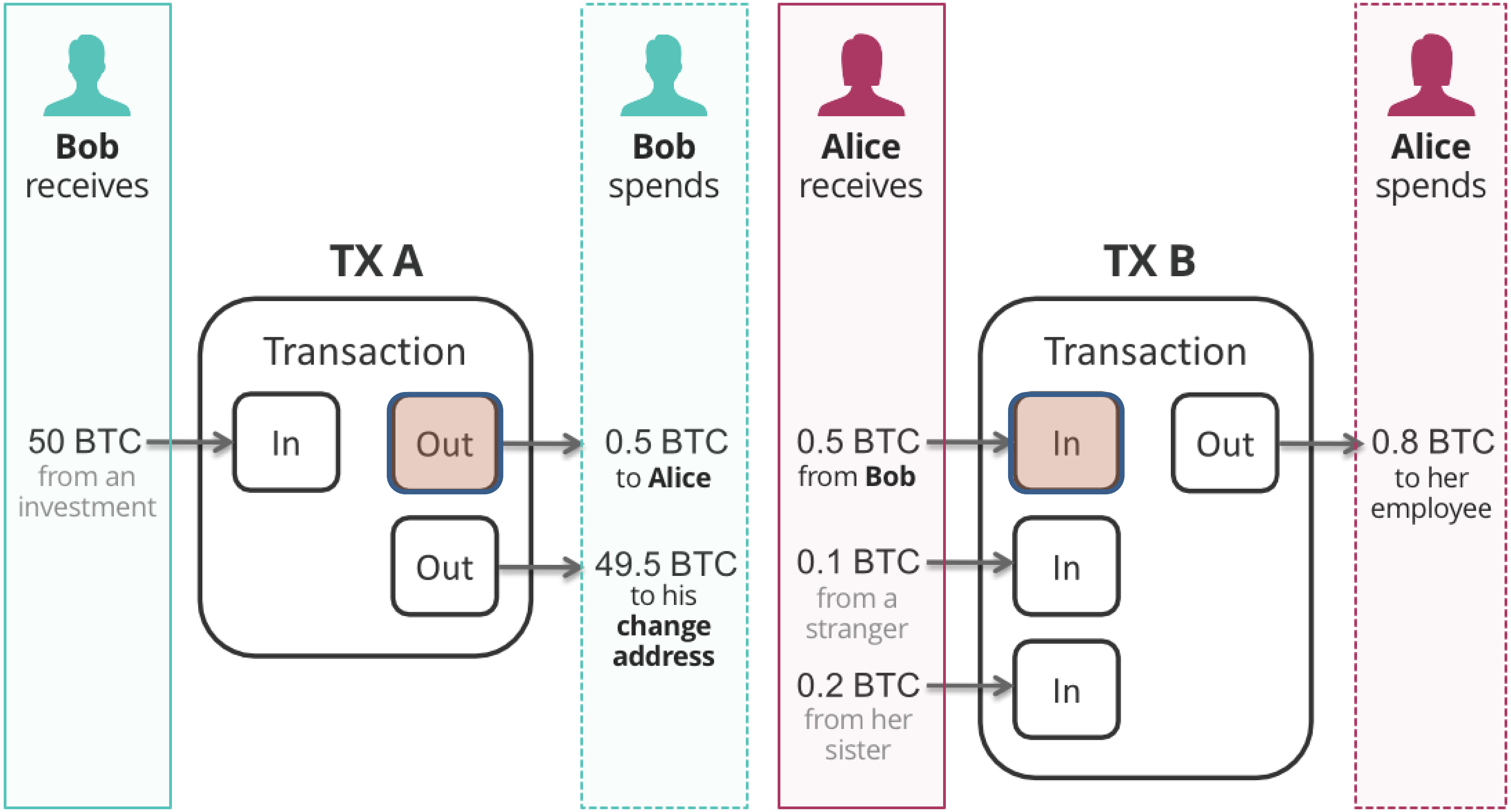


Double hash can be effective against
“length-extension” attack

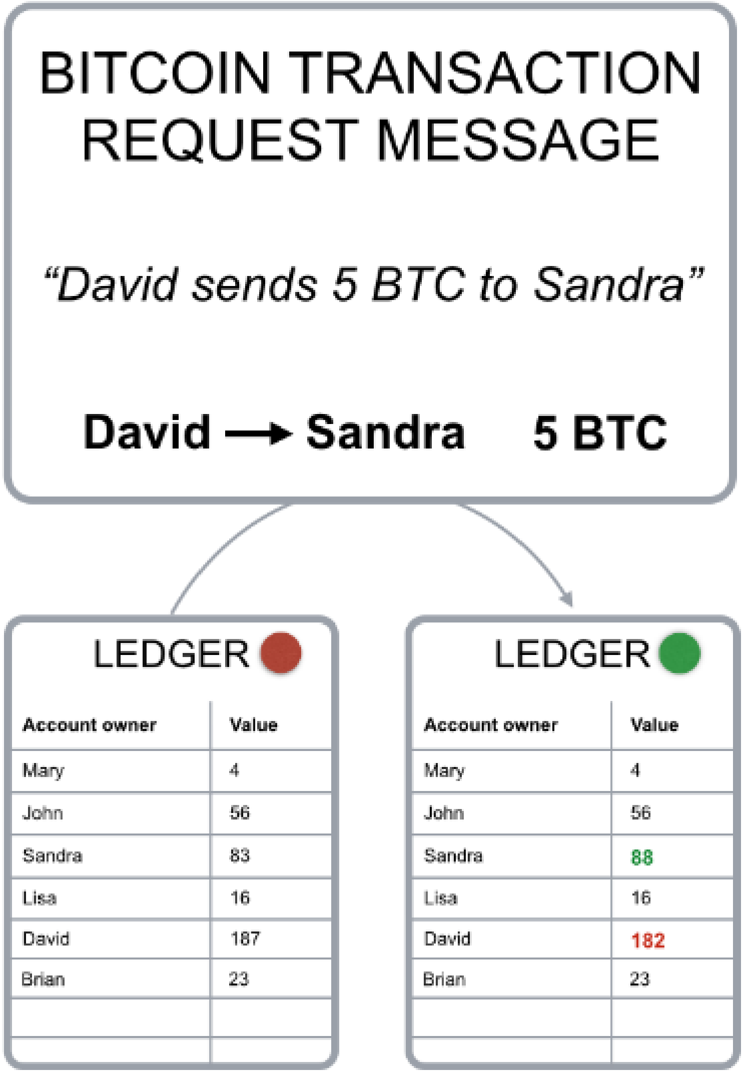
Base58 is Base64 without the 0 (number zero), O (capital o),
l (lower L), I (capital i), + and /.

Transactions in Bitcoin

A transaction is of the form "Send 0.5 Bitcoins from Bob to Alice"



Ledger is synchronized



BITCOIN TRANSACTION REQUEST MESSAGE

“David sends 5 BTC to Sandra”

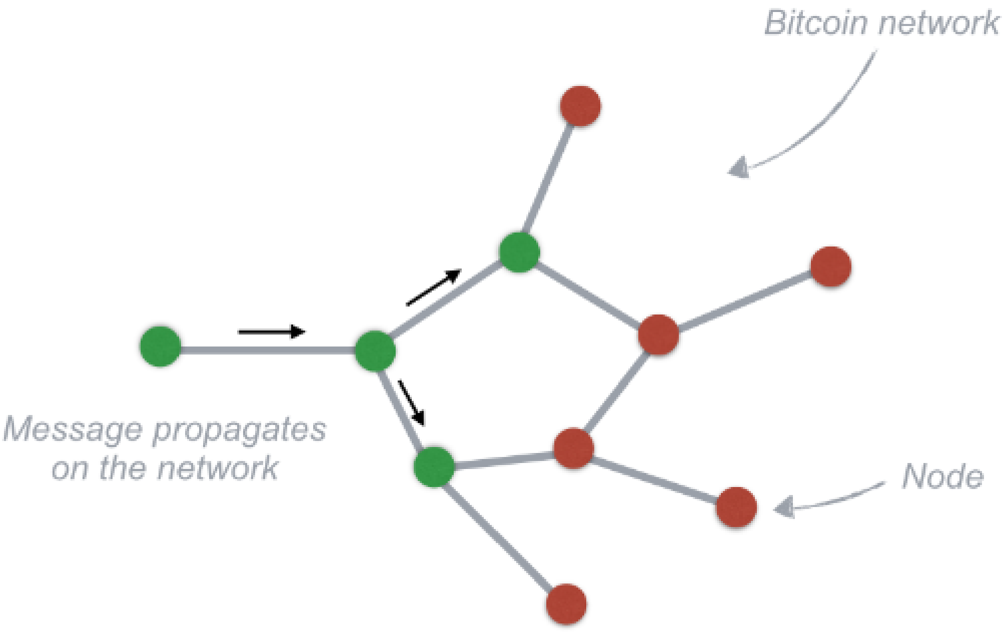
David ⟶ Sandra 5 BTC

LEDGER 🔴

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23

LEDGER 🟢

Account owner	Value
Mary	4
John	56
Sandra	**88**
Lisa	16
David	**182**
Brian	23

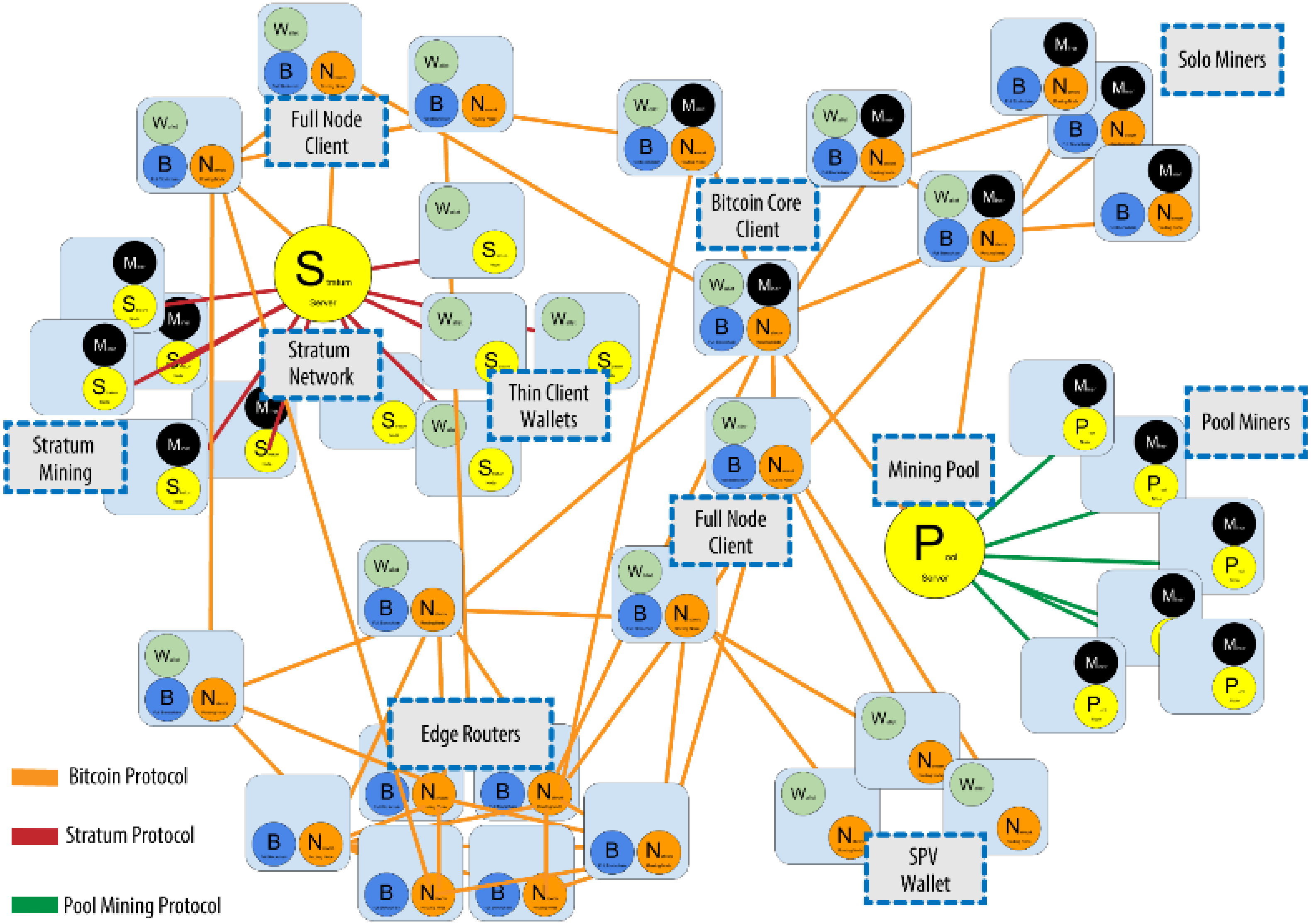


Each *node* receives the transaction request message, updates its own copy of the *ledger* and passes on the message to the nearby *nodes*.

Transaction agreement

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a proof-of-work for its block (The one to finish early will probably win).
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
6. Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Bitcoin P2P network



Full Node Client

Solo Miners

Bitcoin Core Client

Stratum Network

Thin Client Wallets

Stratum Mining

Pool Miners

Mining Pool

Full Node Client

Edge Routers

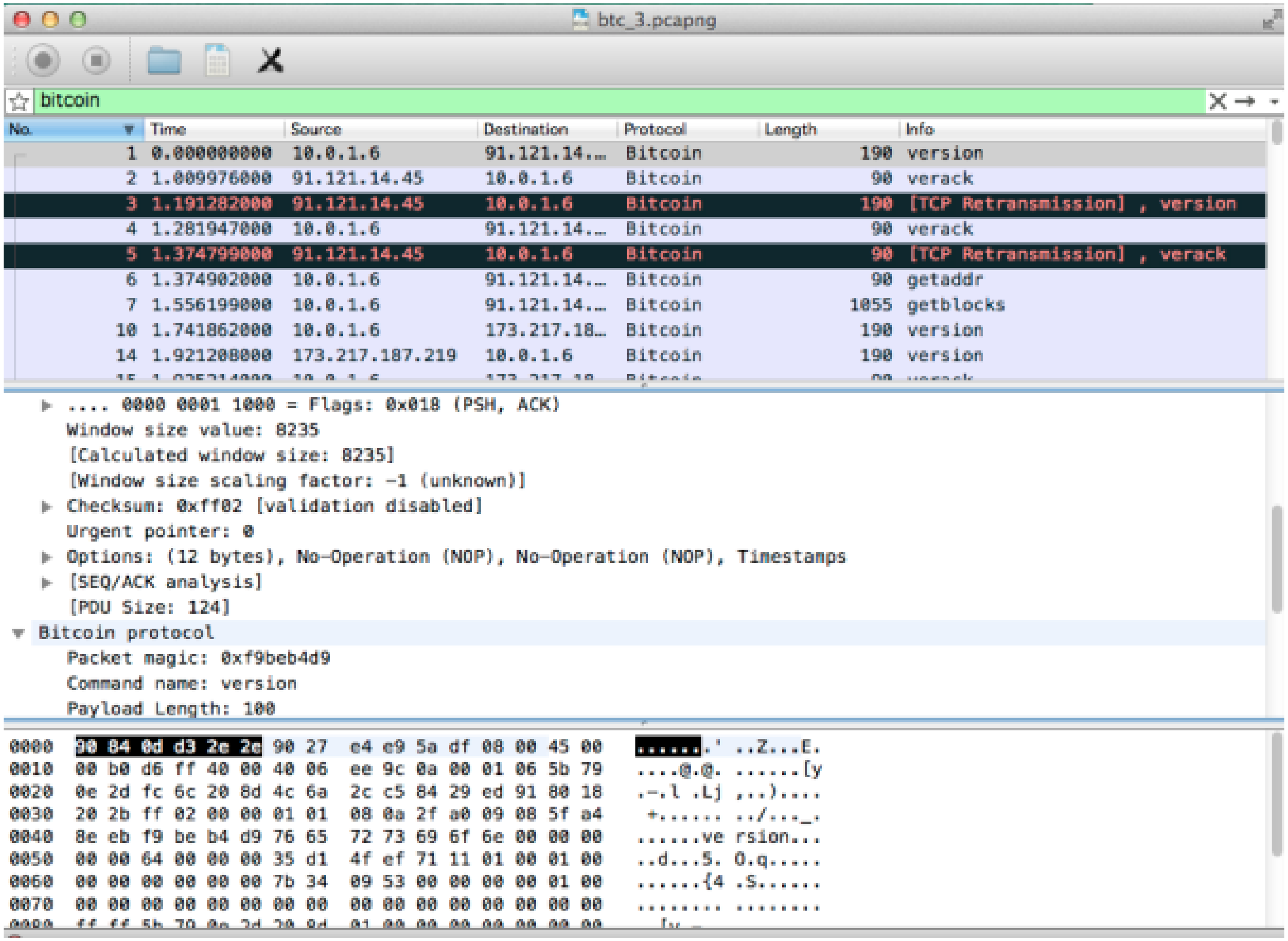
SPV Wallet

🟧 Bitcoin Protocol

🟥 Stratum Protocol

🟩 Pool Mining Protocol

Bitcoin message in Wireshark



bitcoin

```
No.      Time          Source            Destination    Protocol   Length  Info
      1  0.000000000   10.0.1.6          91.121.14...   Bitcoin       190  version
      2  1.009976000   91.121.14.45      10.0.1.6       Bitcoin        90  verack
      3  1.191282000   91.121.14.45      10.0.1.6       Bitcoin       190  [TCP Retransmission] , version
      4  1.281947000   10.0.1.6          91.121.14...   Bitcoin        90  verack
      5  1.374799000   91.121.14.45      10.0.1.6       Bitcoin        90  [TCP Retransmission] , verack
      6  1.374902000   10.0.1.6          91.121.14...   Bitcoin        90  getaddr
      7  1.556199000   10.0.1.6          91.121.14...   Bitcoin      1055  getblocks
     10  1.741862000   10.0.1.6          173.217.18...  Bitcoin       190  version
     14  1.921208000   173.217.187.219   10.0.1.6       Bitcoin       190  version
```

```
  ▶ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 8235
    [Calculated window size: 8235]
    [Window size scaling factor: -1 (unknown)]
  ▶ Checksum: 0xff02 [validation disabled]
    Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
    [PDU Size: 124]
▼ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: version
    Payload Length: 100
```

```
0000  00 84 0d d3 2e 2e 90 27  e4 e9 5a df 08 00 45 00   .......' ..Z...E.
0010  00 b0 d6 ff 40 00 40 06  ee 9c 0a 00 01 06 5b 79   ....@.@. ......[y
0020  0e 2d fc 6c 20 8d 4c 6a  2c c5 84 29 ed 91 80 18   .-.l .Lj ,..)....
0030  20 2b ff 02 00 00 01 01  08 0a 2f a0 09 08 5f a4    +...... ../..._.
0040  8e eb f9 be b4 d9 76 65  72 73 69 6f 6e 00 00 00   ......ve rsion...
0050  00 00 64 00 00 00 35 d1  4f ef 71 11 01 00 01 00   ..d...5. O.q.....
0060  00 00 00 00 00 00 7b 34  09 53 00 00 00 00 01 00   ......{4 .S......
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Bitcoin node

- A bitcoin node is a collection of functions:
  - routing, the blockchain database, mining, and wallet services.

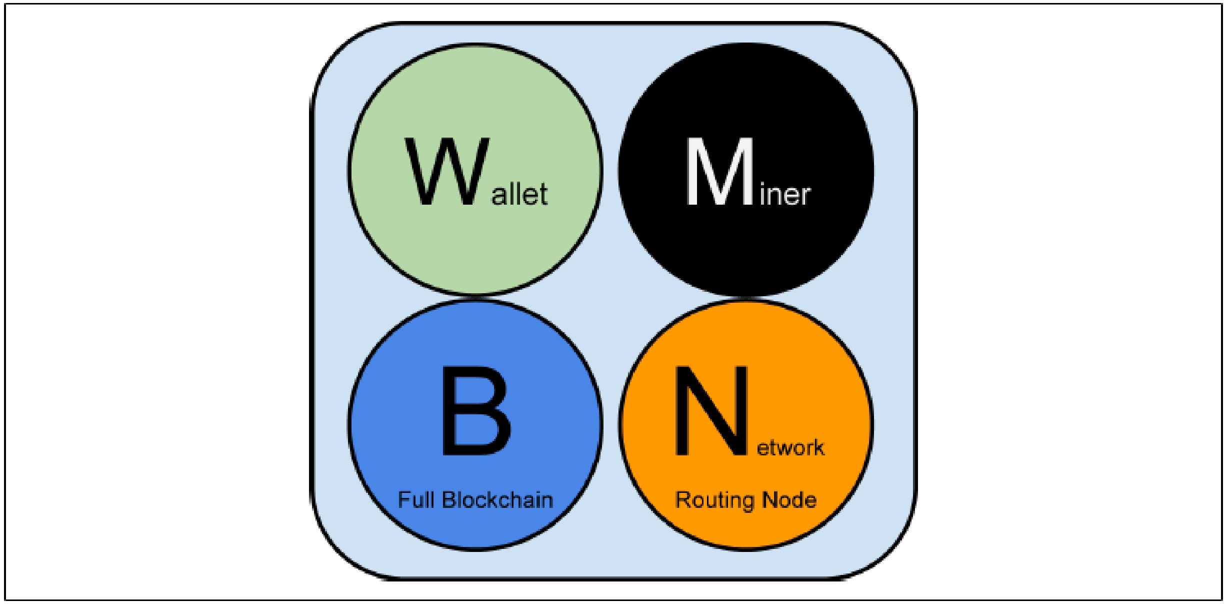
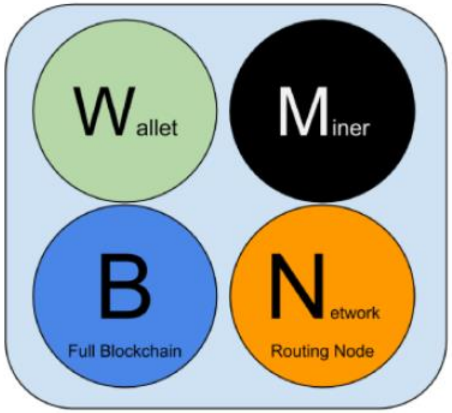
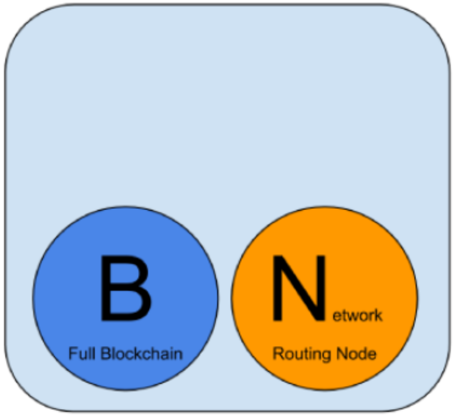


Figure 8-1. A bitcoin network node with all four functions: wallet, miner, full blockchain database, and network routing

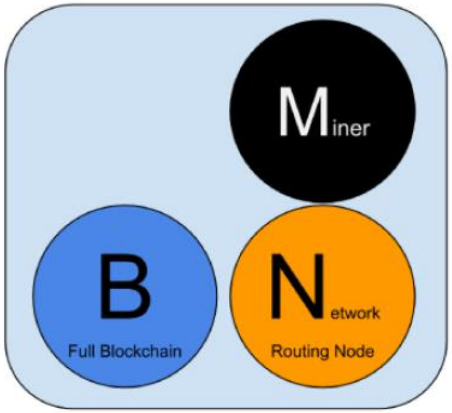
Node types and roles



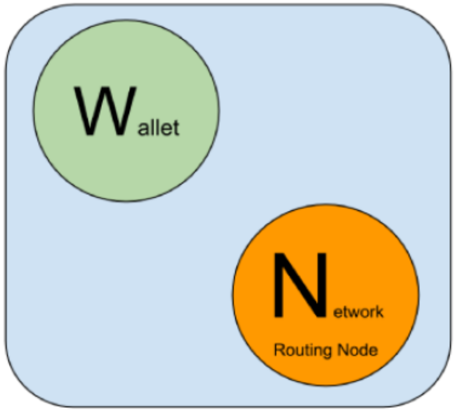
Reference Client



Full Block Chain Node



Solo Miner



Lightweight (SPV) wallet

Network discovery

- How does a new node find peers?

1. "**DNS seeds**" which are DNS servers that provide a list of IP addresses of Bitcoin nodes
   - The Bitcoin Core client contains the names of five different DNS seeds
   - **-dnsseed** (by default)

2. Known IP address of at least one Bitcoin node
   - After the initial seed node is used to form introductions, the client will disconnect from it and use the newly discovered peers.
   - **-seednode**

Handshake

- To connect to a known peer, nodes establish a TCP connection (usually to port 8333)
- The node will start a “handshake” by transmitting a version message
- The node receiving a version message will examine the reported nVersion and, if compatible, it will acknowledge the version message by sending a verack

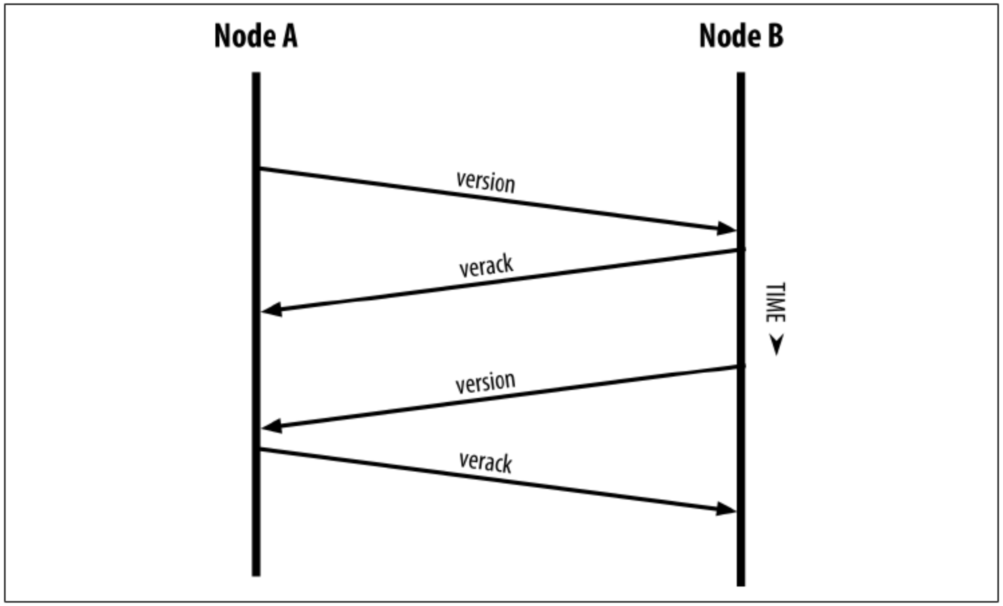


Figure 8-4. The initial handshake between peers

Updating peers

- Once one or more connections are established, the new node will send an addr message containing its own IP address to its neighbors
- The new node can send getaddr message to the neighbors, asking them to return a list of IP addresses of other peers

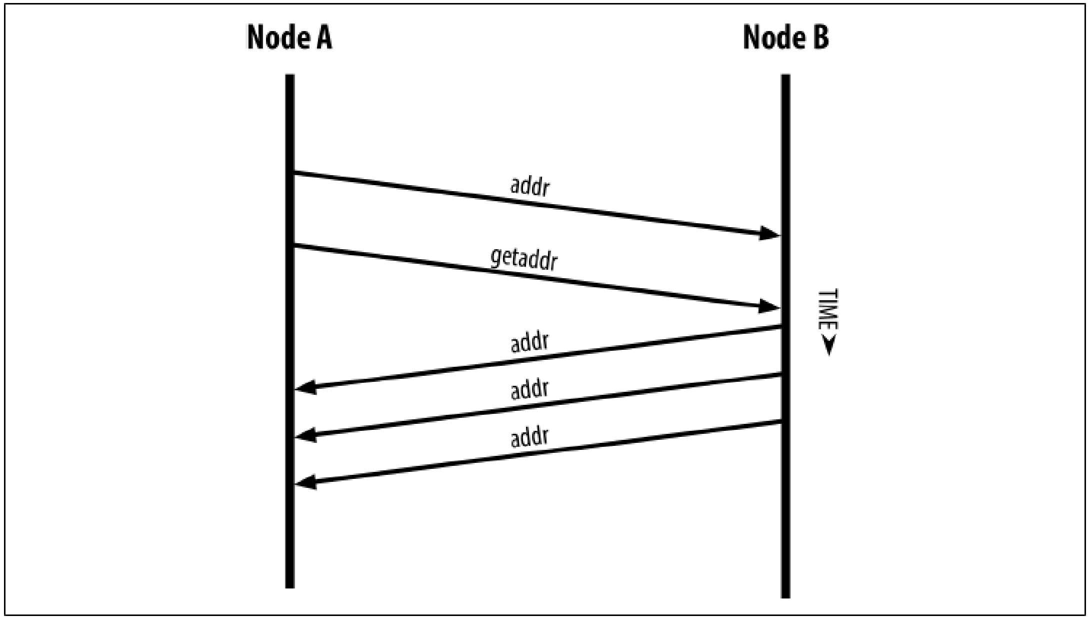


Figure 8-5. Address propagation and discovery

Full nodes

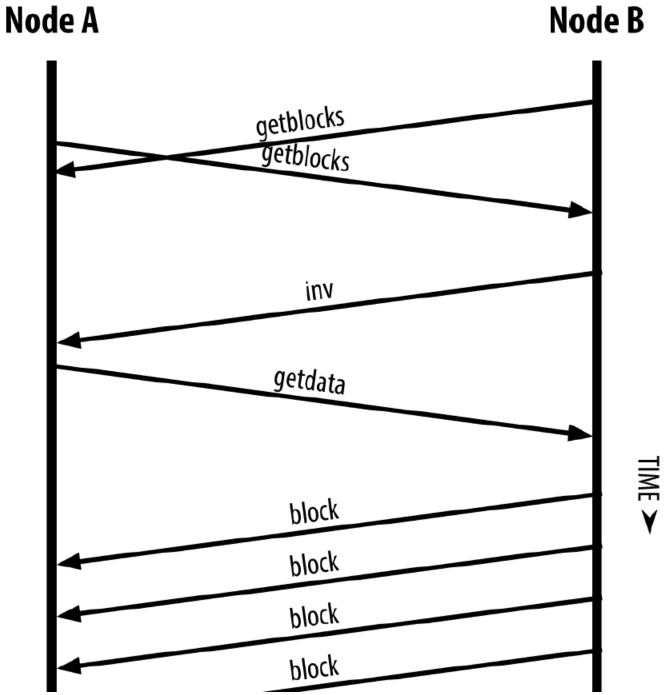
- Full blockchain nodes maintain a **complete and up-to-date copy of the bitcoin blockchain** with all the transactions

- A full blockchain node can independently verify any transaction without reliance on any other node or source of information

- Full blockchain node relies on the network to receive updates about new blocks of transactions, which are incorporated into its local copy of the blockchain

Synchronizing the blockchain

- Nodes exchange a ***getblocks*** message that contains the hash of the top block on their local blockchain
- The node that has the longer blockchain shares the first 500 blocks with other nodes (***inv*** containing hashes of blocks)



SPV nodes

- For space- and power-constrained devices, a simplified payment verification (SPV) method is used to allow them to operate **without storing the full blockchain**

- SPV nodes download only the block headers and do not download the transactions included in the block
  - 1,000 times smaller than full blockchain

Synchronizing the headers

- To get the block headers, SPV nodes use a ***getheaders*** message instead of *getblocks*
  - The responding peer will send up to 2,000 block headers using a single ***headers*** message

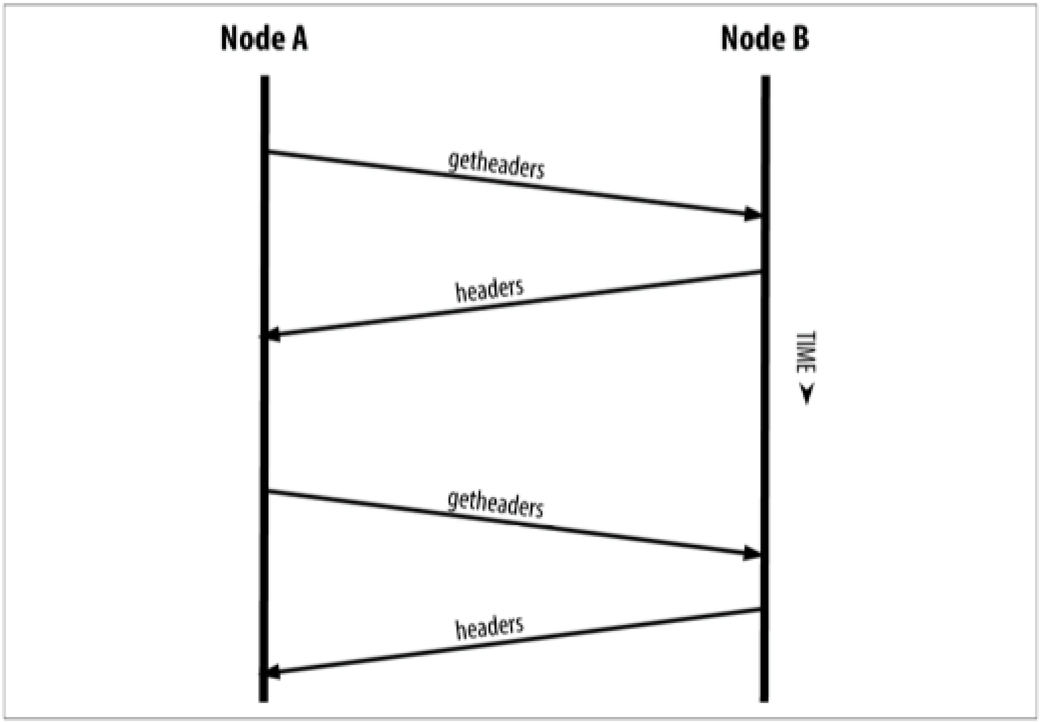


Figure 8-7. SPV node synchronizing the block headers

Operations of SPV nodes

- SPV nodes need to retrieve specific transactions using ***getdata*** message in order to selectively verify them

- SPV node’s requests for specific data can inadvertently reveal the likability between its network address and wallet address
  - For example, a third party monitoring a network could keep track of all the transactions requested by a wallet and use those to associate bitcoin addresses with network address.

Use of Bloom filters

- Bloom Filters
  - A probabilistic data structure that is used to test membership of an element.
  - SPV nodes ask their peers **for transactions matching a specific pattern using Bloom filters**, without revealing precisely which addresses they are interested in.

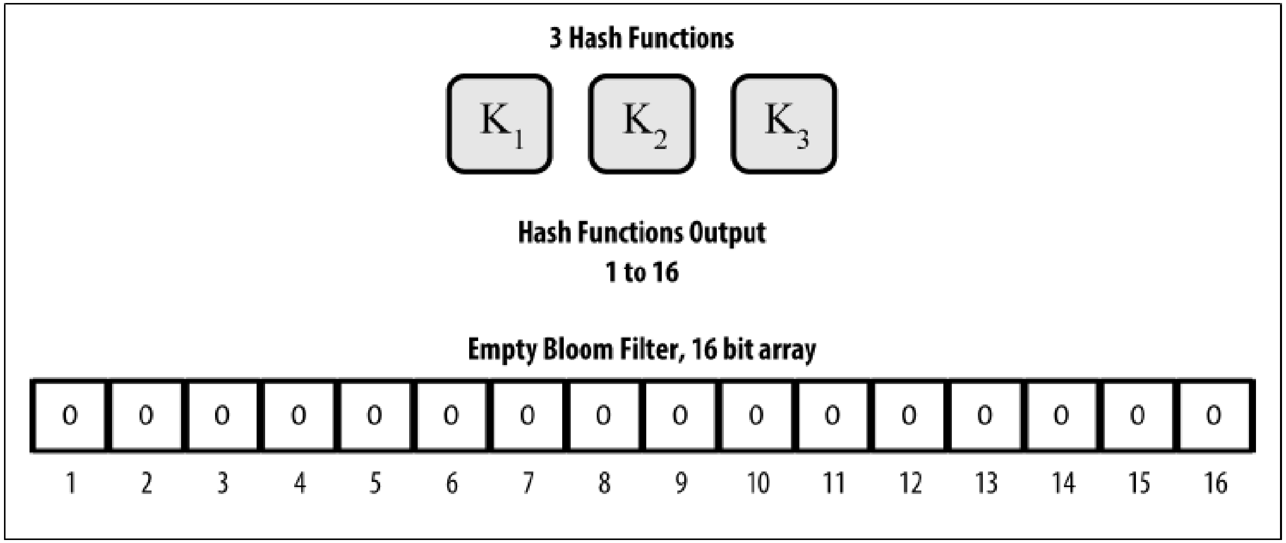


Figure 8-8. An example of a simplistic bloom filter, with a 16-bit field and three hash functions

How Bloom filters work (1)

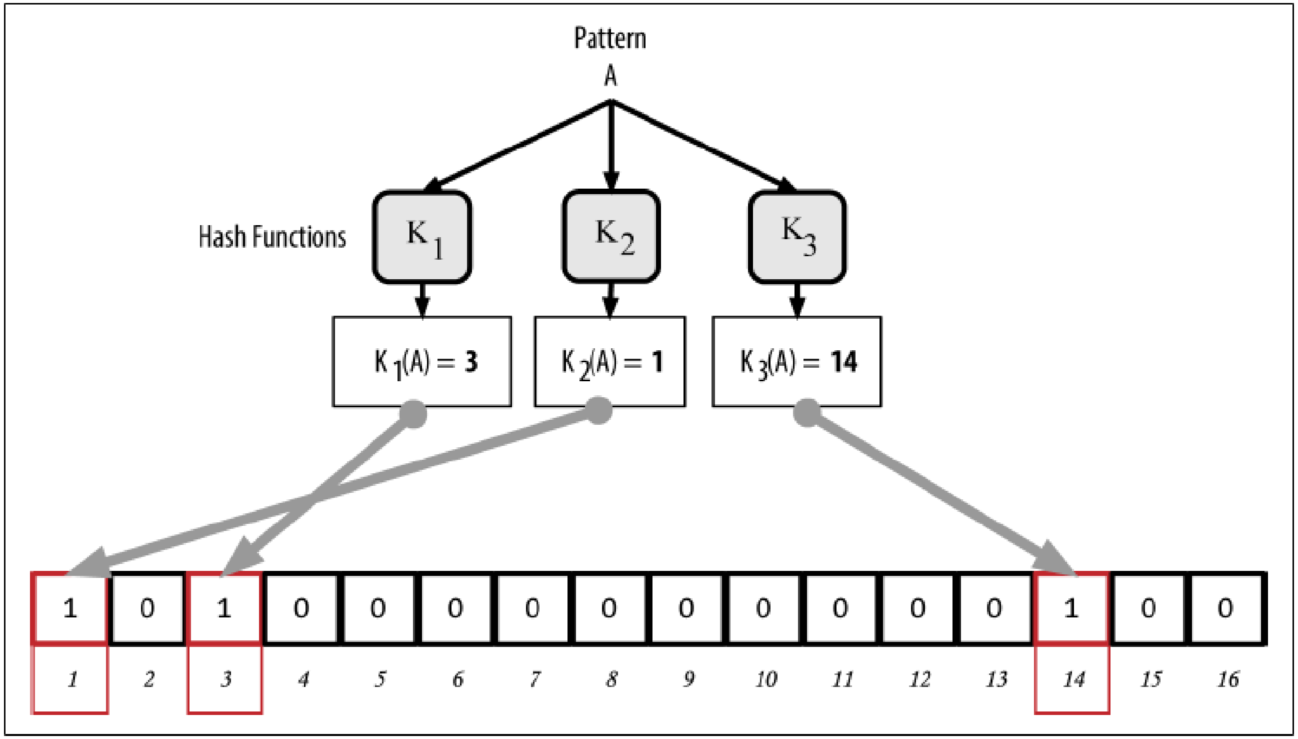
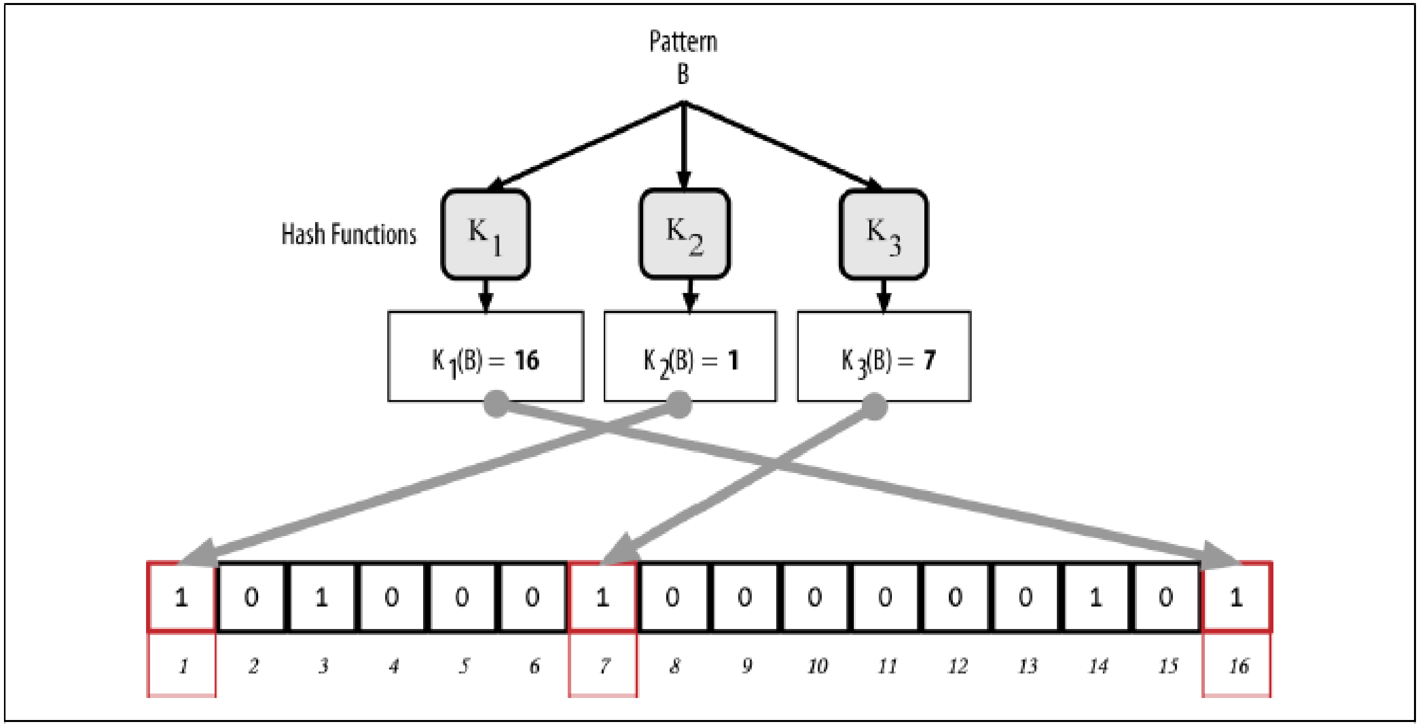


Figure 8-9. Adding a pattern "A" to our simple bloom filter

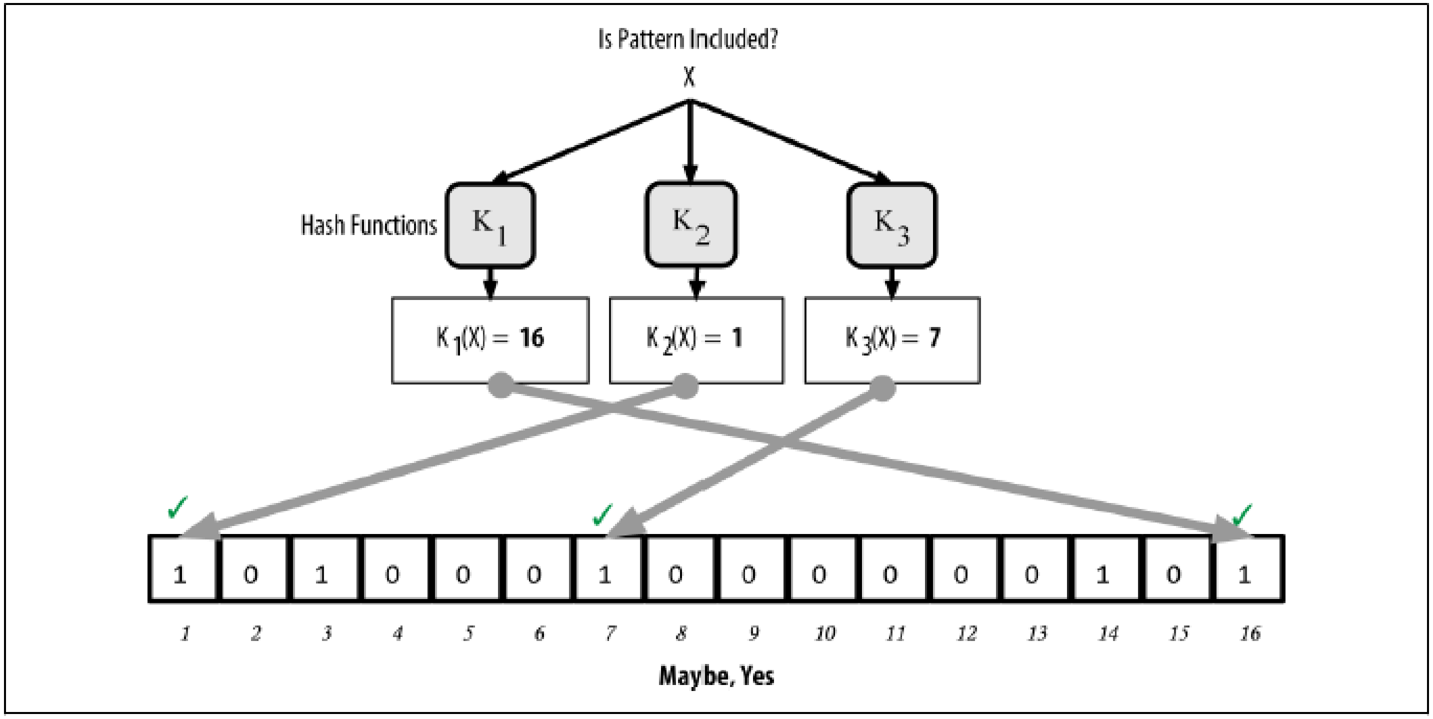
How Bloom filters work (2)



1	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Figure 8-10. Adding a second pattern "B" to our simple bloom filter

How Bloom filters work (3)



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1

Figure 8-11. Testing the existence of pattern "X" in the bloom filter. The result is a probabilistic positive match, meaning "Maybe."

How to use Bloom filters

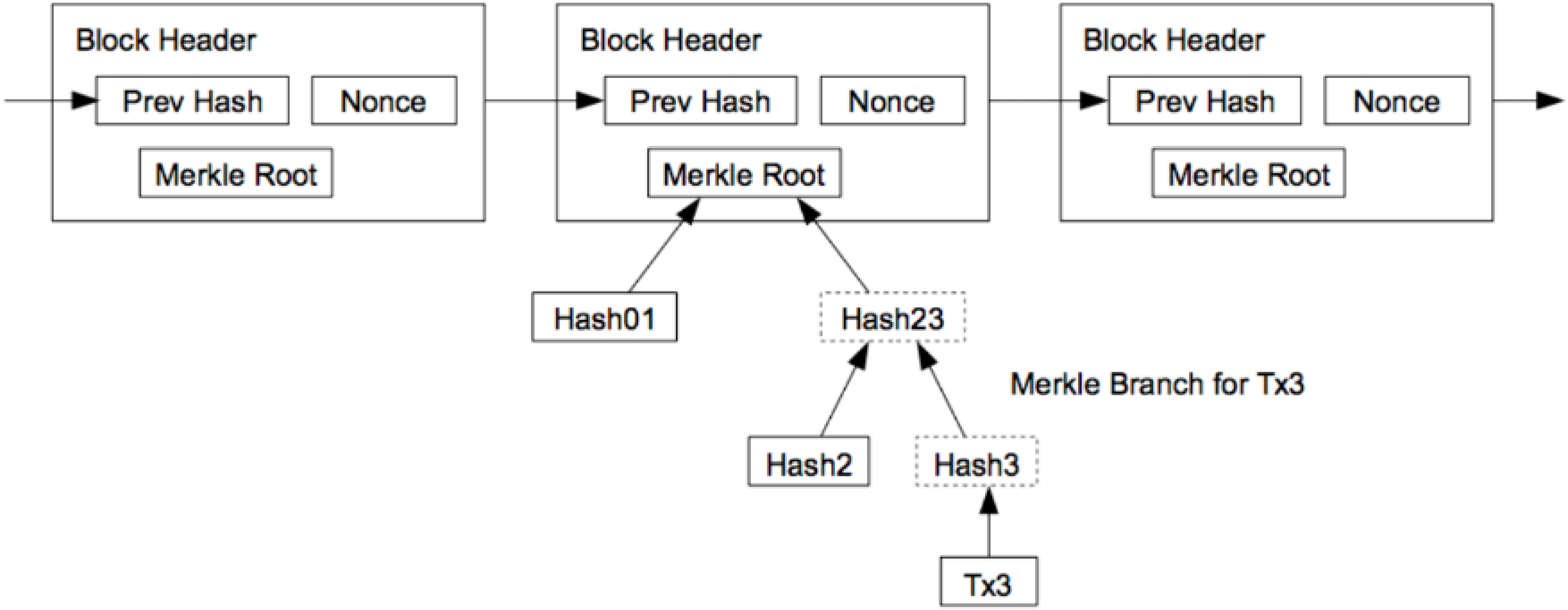
- A SPV node adds TXID, Script hash, and PubKey hash (from any UTXO controlled by its wallet) to the bloom filter

- The SPV node sends the bloom filter to a full node using the message filterload

- If the filter has been loaded, then full nodes will send a modified form of blocks, called a Merkle block that contains only block headers for blocks matching the filter and a Merkle path for each matching transaction

Merkle block and path

- SPV node can check whether the transaction (Tx3) is included in the block.
- Only need Hash01 and Hash2 to verify; not the entire Tx's.



Encrypted connections

- The original implementation of bitcoin communicates entirely in the clear. It raises a privacy concern for SPV nodes.
- Two solutions that provide encryption of the communications:
  - Tor (The Onion Routing network) transport: since Core v0.12
  - P2P authentication and encryption (BIP-150 and BIP-151)
    - BIP-150 uses ECDSA (Each node’s public key must be pre-shared over a different channel)
    - BIP-151 uses ECDH to generate symmetric encryption keys

BIP: Bitcoin Improvement Proposal is a design document for introducing features or information to Bitcoin.

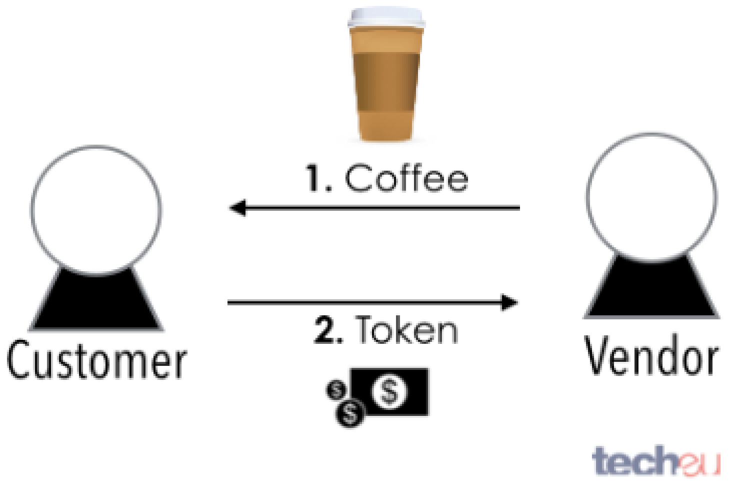
Transaction pool

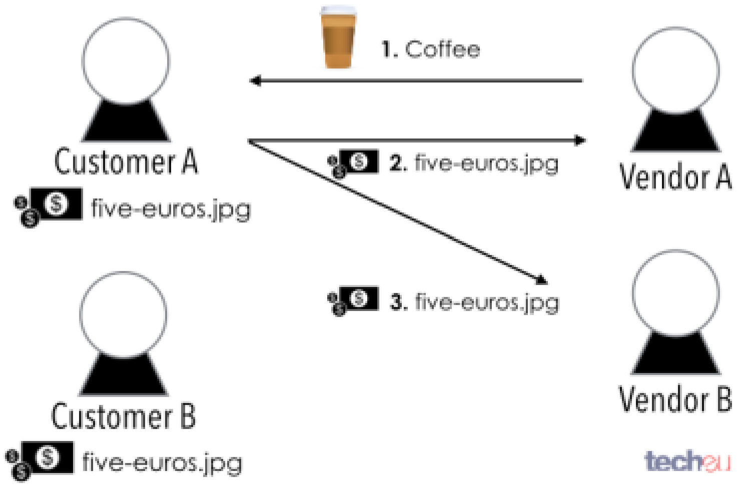
- Almost every node on the Bitcoin network maintains a temporary list of unconfirmed transactions called the memory pool, mempool, or *transaction pool*

- Nodes use this pool to keep track of transactions that are known to the network but are not yet included in the blockchain.

- For example, a wallet node will use the transaction pool to track incoming payments to the user’s wallet that have been received on the network but are not yet confirmed.

Double spending issue

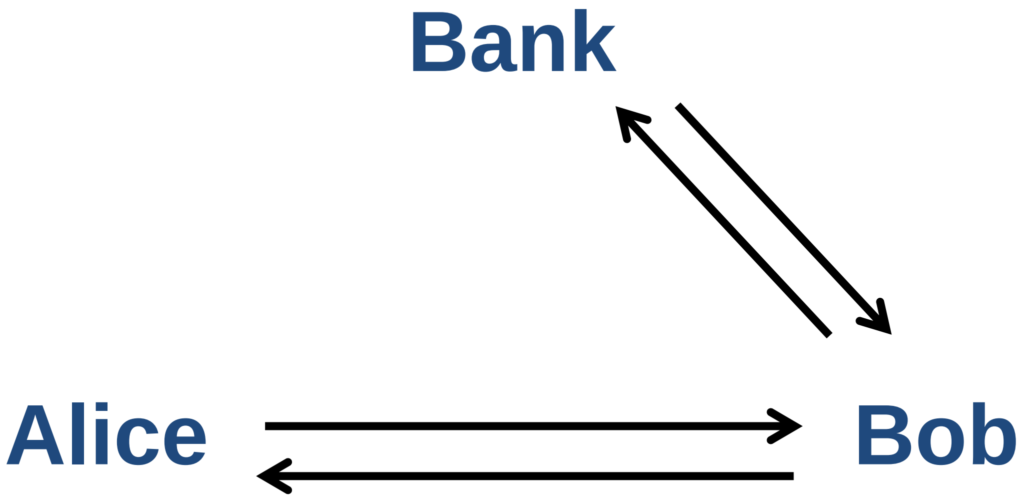




Digital objects can be copied many times.

How can we prevent this?

How traditional e-cash handled problem

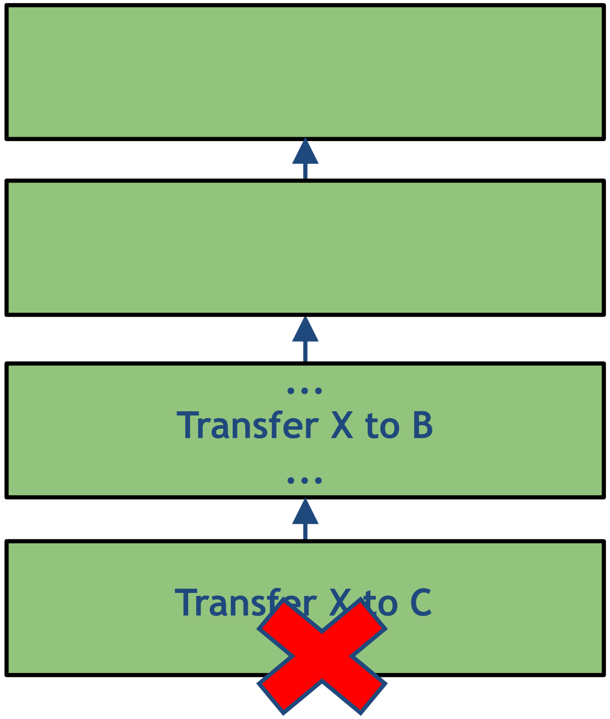


- When Alice pays Bob with a coin, Bob validates that coin hasn't been spend with trusted third party

Bank maintains a linearizable log of transactions

Can we solve it in decentralized environment?

Maintain a global public append-only log!
The only way is to be aware of all transactions.



The blockchain –a public ledger of all transactions.

(In Bitcoin, the log is extended in increments of blocks, each of which may contain thousands of transactions.)

Consensus of the block state is needed

- The system must agree on some “canonical order” of transactions
- Who will be responsible for managing blocks?
- Think of this mechanism as being like some kind of “voting”

Election based on “work”

- Rather than “count” IP addresses, bitcoin “counts” the amount of CPU time / electricity that is expended
- Economic defense against sybil attacks

> **“The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”**
>
> **- Satoshi Nakamoto**

- Proof-of-work: Cryptographic “proof” that certain amount of CPU work was performed

Hashcash – Proof of Work

To demonstrate work on x, find y such that

$$H(x, y) < z,$$

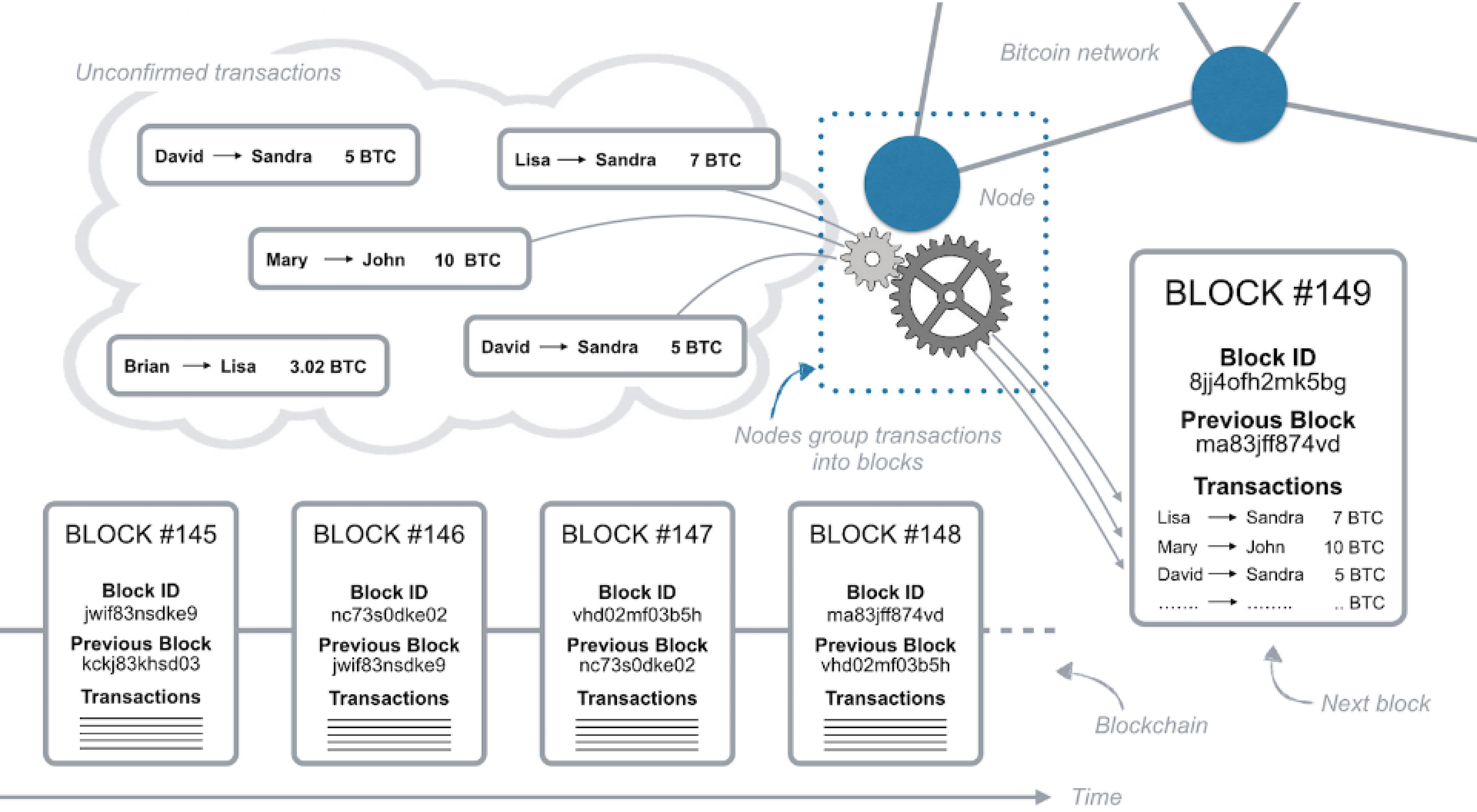
for some pre-determined bound z.

The core idea is that before accepting a transaction, the sender must first demonstrate a “cost” via a computationally “hard” problem that can simultaneously be easily verified.

Application: spam email prevention

“Hashcash,” Adam Back, 1997 (http://www.hashcash.org/papers/announce.txt).

Bitcoin network overview



Unconfirmed transactions

David → Sandra 5 BTC

Lisa → Sandra 7 BTC

Mary → John 10 BTC

Brian → Lisa 3.02 BTC

David → Sandra 5 BTC

Bitcoin network

Node

Nodes group transactions into blocks

BLOCK #149

Block ID
8jj4ofh2mk5bg

Previous Block
ma83jff874vd

Transactions

Lisa	→	Sandra	7 BTC
Mary	→	John	10 BTC
David	→	Sandra	5 BTC
....	→	....	.. BTC

BLOCK #145

Block ID
jwif83nsdke9

Previous Block
kckj83khsd03

Transactions

BLOCK #146

Block ID
nc73s0dke02

Previous Block
jwif83nsdke9

Transactions

BLOCK #147

Block ID
vhd02mf03b5h

Previous Block
nc73s0dke02

Transactions

BLOCK #148

Block ID
ma83jff874vd

Previous Block
vhd02mf03b5h

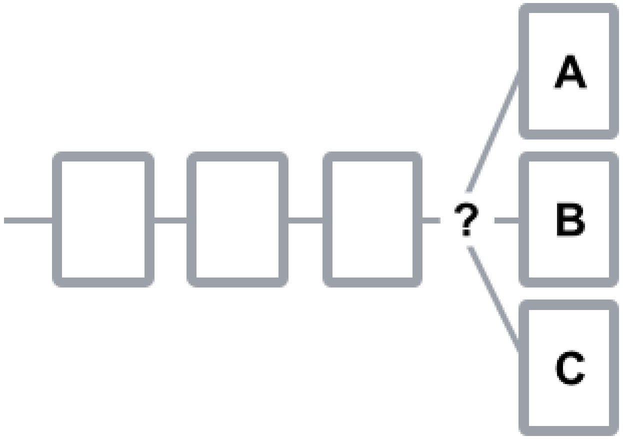
Transactions

Blockchain

Next block

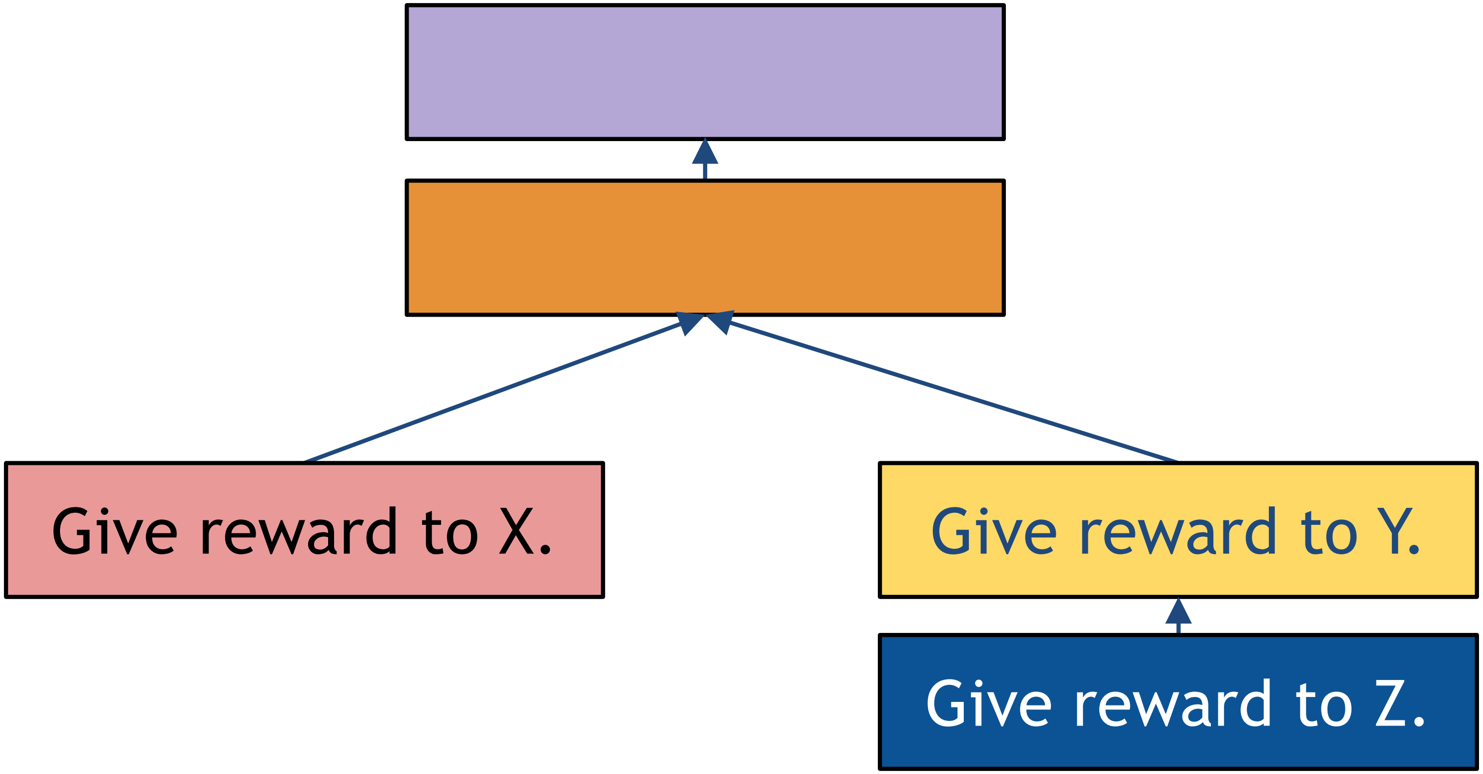
Time

Problem remains: forking

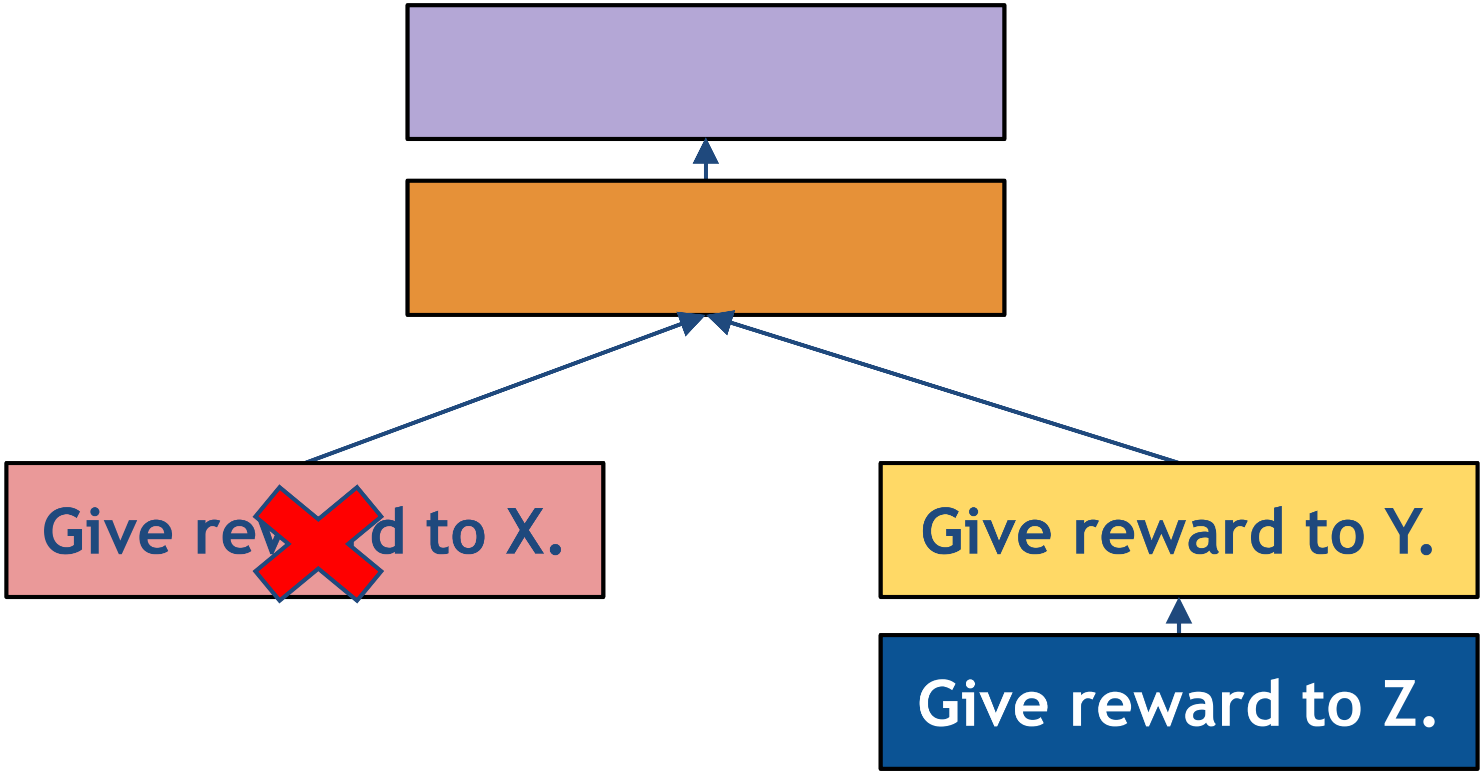


Sometimes multiple nodes solve the mathematical problem at the same time.

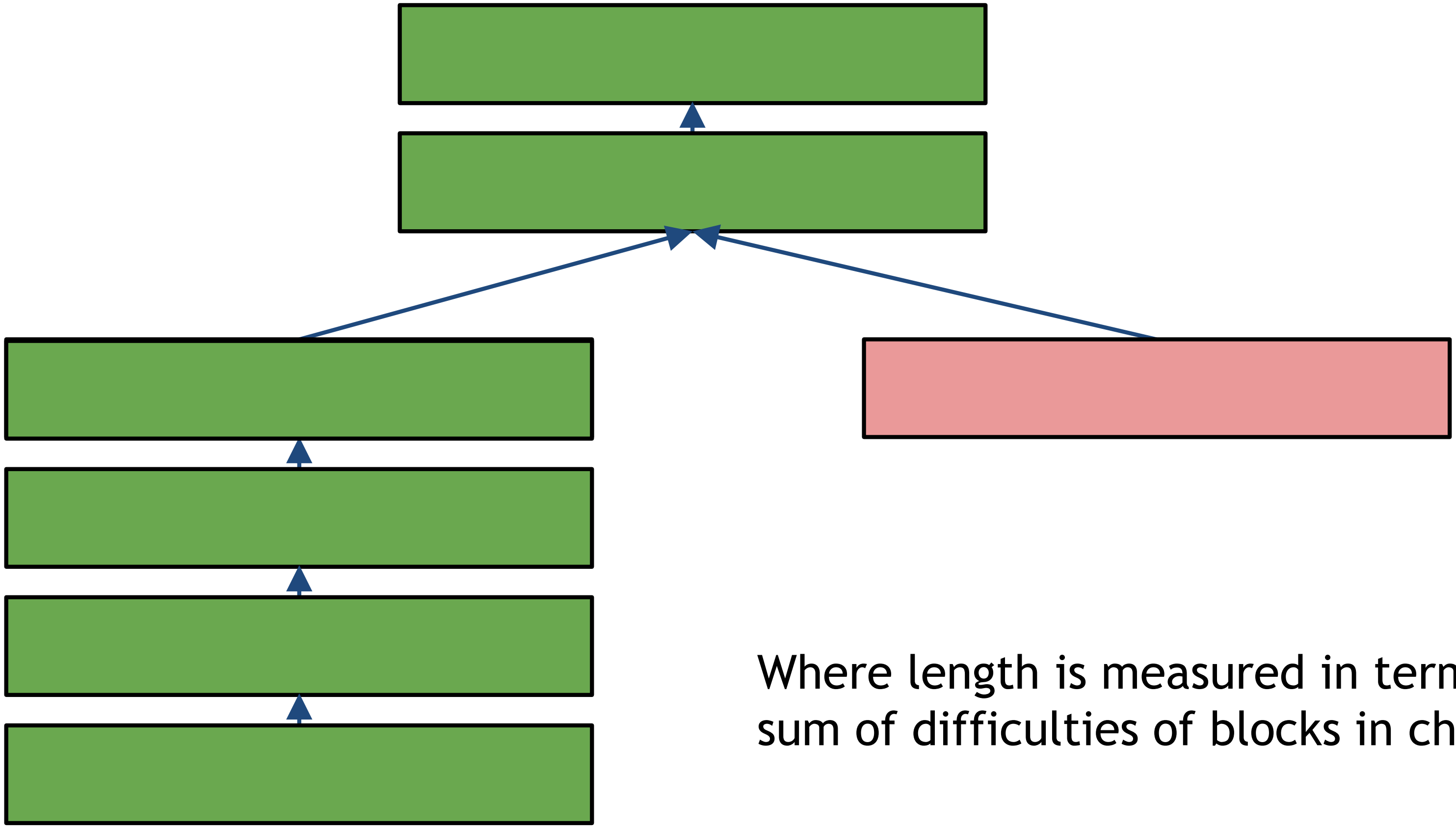
A *fork* can occur when two miners publish blocks simultaneously. Such blocks are almost always in conflict.



Effort spent on a fork that eventually loses is wasted.



More generally, longest chain wins.



Where length is measured in terms of sum of difficulties of blocks in chain.

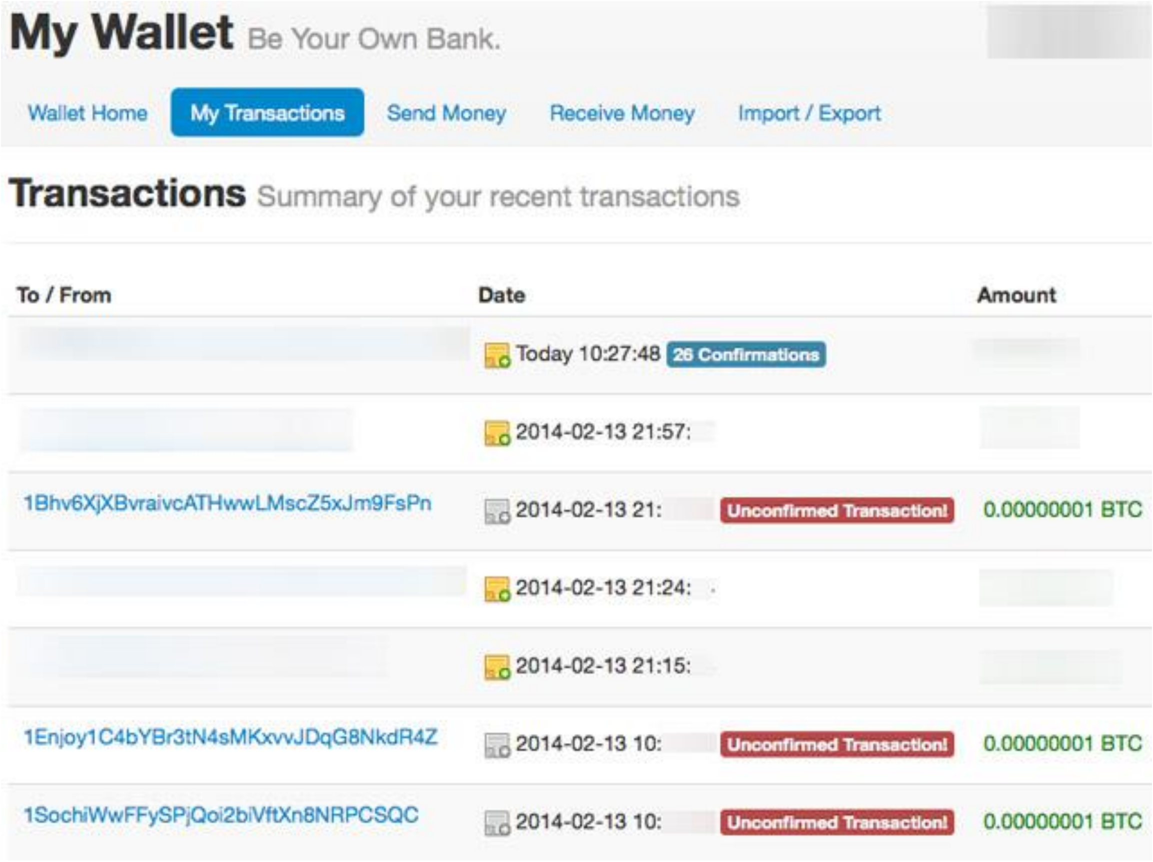
Transaction confirmations

- A transaction is said to have received *k* confirmations if it has been published in a block that has been added to the blockchain, and *k-1* more blocks have also been added.

- A transactions is typically considered "confirmed" once it has 6 confirmations (the success rate of double spending is less than 0.1% against the attacker with the hashrate of 10%).

- Newly minted Bitcoins (i.e., in COINBASE transaction) are typically considered confirmed once they have received 100 confirmations.

Transaction confirmation (in real-world)



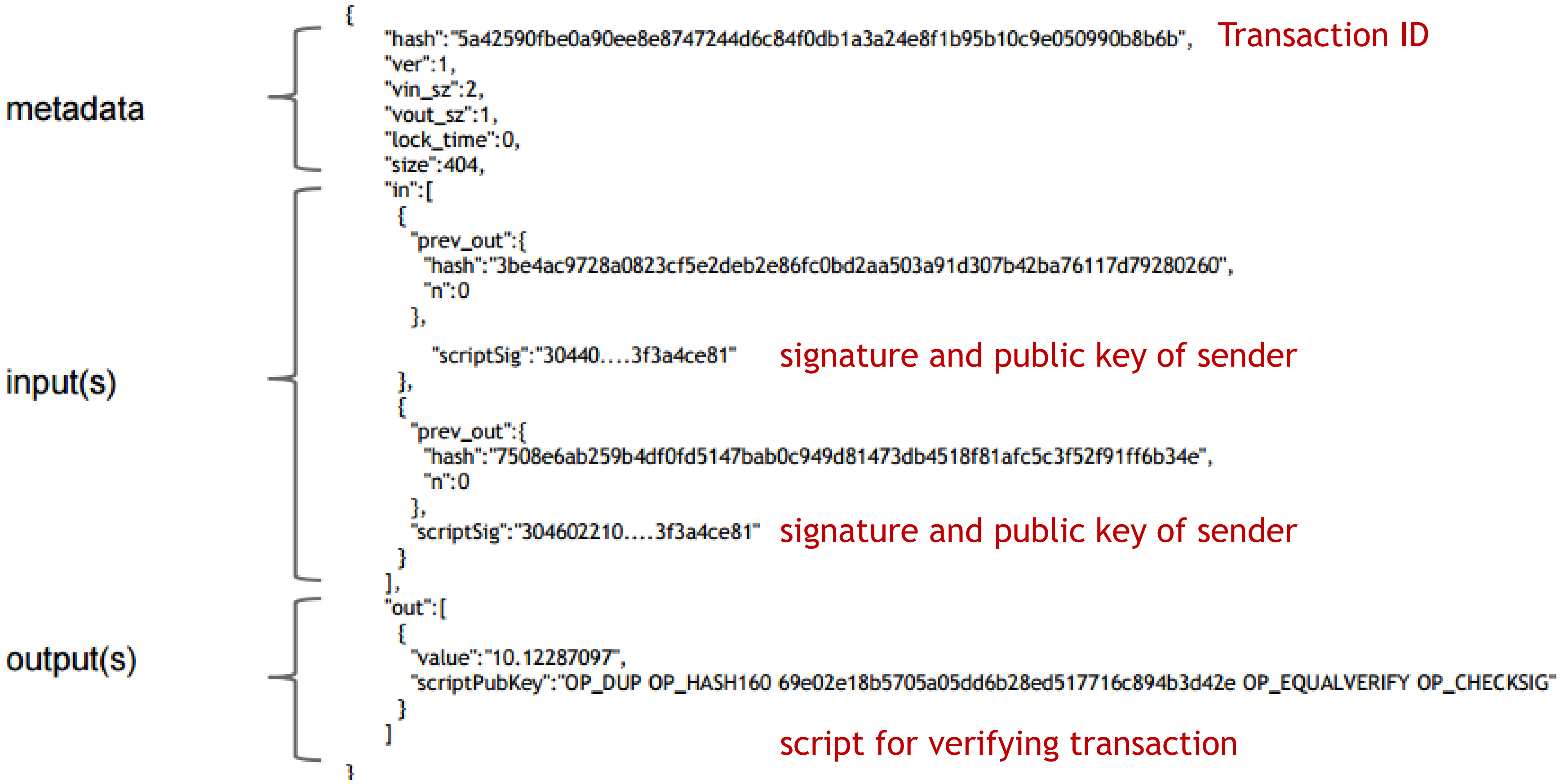
Transactions Summary of your recent transactions

To / From	Date		Amount
[redacted]	Today 10:27:48	26 Confirmations	[redacted]
[redacted]	2014-02-13 21:57:		[redacted]
1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn	2014-02-13 21:	Unconfirmed Transaction!	0.00000001 BTC
[redacted]	2014-02-13 21:24:		[redacted]
[redacted]	2014-02-13 21:15:		[redacted]
1Enjoy1C4bYBr3tN4sMKxvvJDqG8NkdR4Z	2014-02-13 10:	Unconfirmed Transaction!	0.00000001 BTC
1SochiWwFFySPjQoi2biVftXn8NRPCSQC	2014-02-13 10:	Unconfirmed Transaction!	0.00000001 BTC

Practical limitation

- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer. Because if you wait longer it becomes more secure. For large $$$, you wait for six blocks (1 hour).

A real Bitcoin transaction



```
{
    "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
    "ver":1,
    "vin_sz":2,
    "vout_sz":1,
    "lock_time":0,
    "size":404,
    "in":[
      {
        "prev_out":{
          "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
          "n":0
        },
          "scriptSig":"30440....3f3a4ce81"
      },
      {
        "prev_out":{
          "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
          "n":0
        },
        "scriptSig":"304602210....3f3a4ce81"
      }
    ],
    "out":[
      {
        "value":"10.12287097",
        "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
      }
    ]
}
```

metadata

input(s)

output(s)

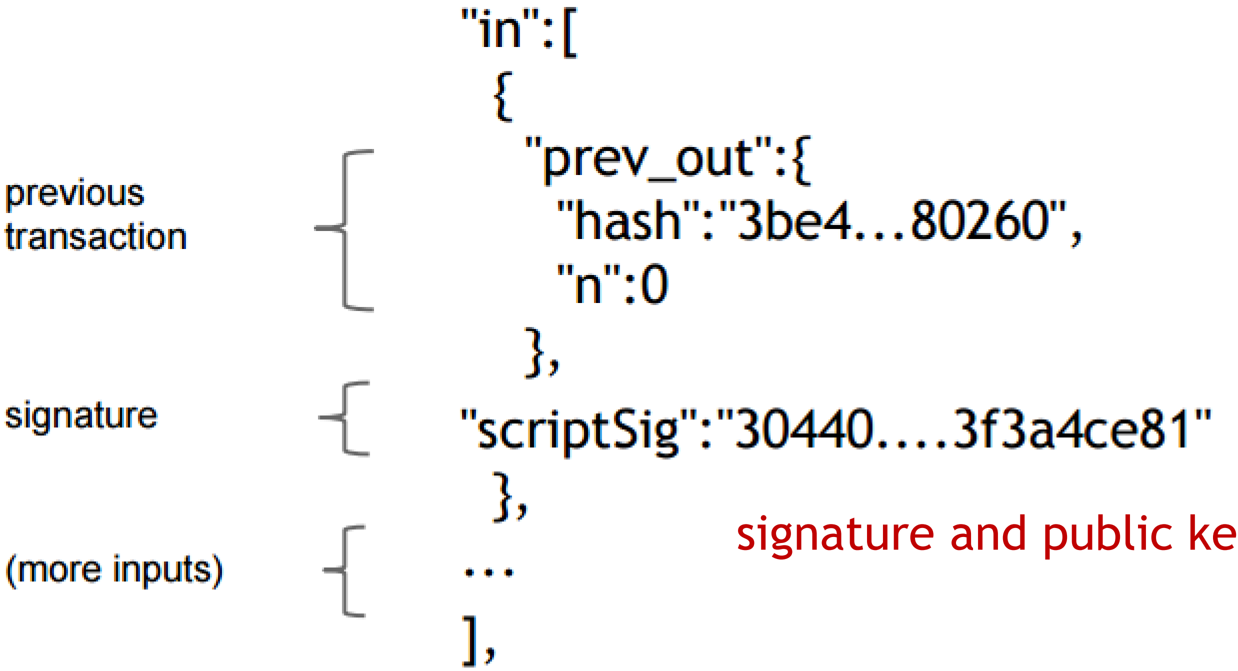
Transaction ID

signature and public key of sender

signature and public key of sender

script for verifying transaction

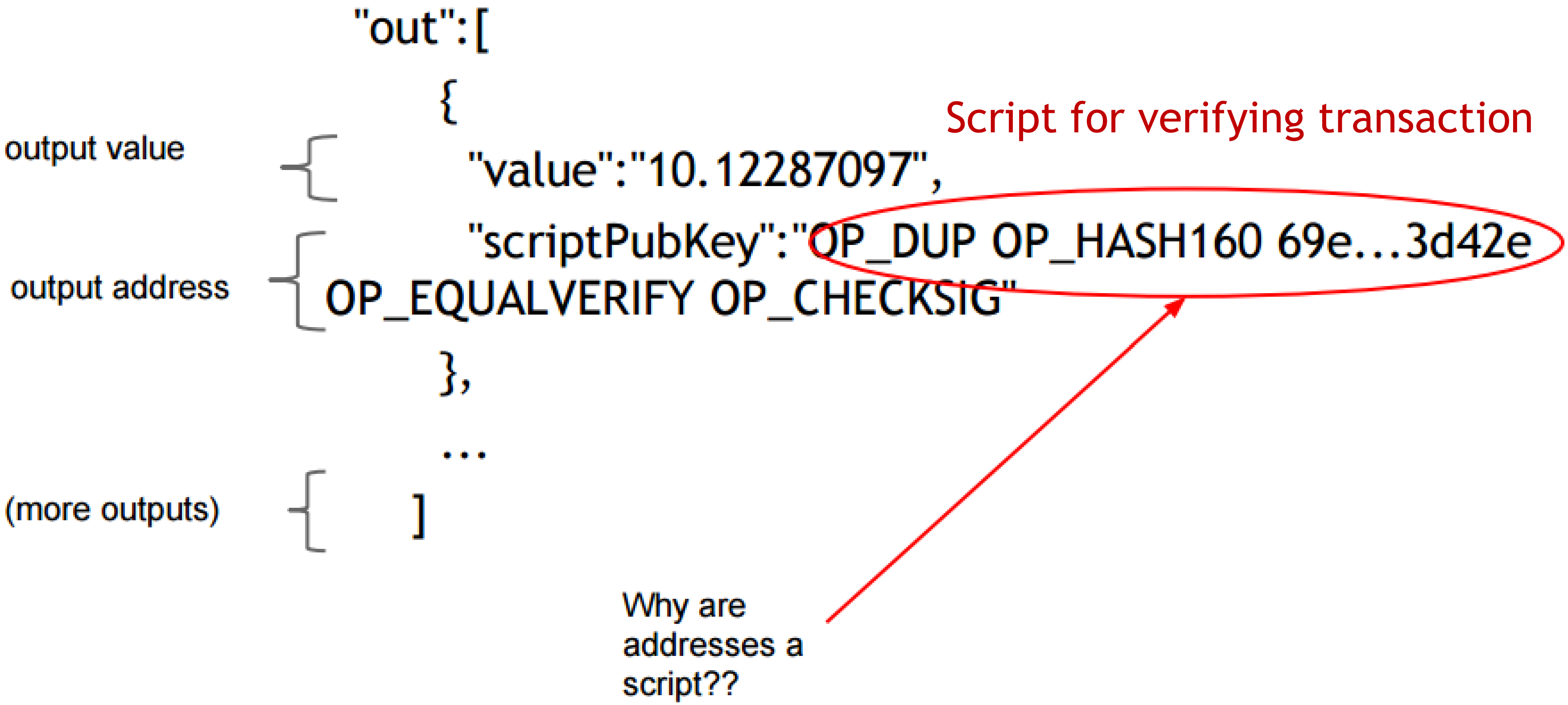
Transaction inputs



```
"in":[
 {
   "prev_out":{
     "hash":"3be4...80260",
     "n":0
   },
"scriptSig":"30440....3f3a4ce81"
 },
...
],
```

signature and public key of sender

Transaction outputs



```
"out":[
      {
        "value":"10.12287097",
        "scriptPubKey":"OP_DUP OP_HASH160 69e...3d42e
OP_EQUALVERIFY OP_CHECKSIG"
      },
      ...
    ]
```

output value

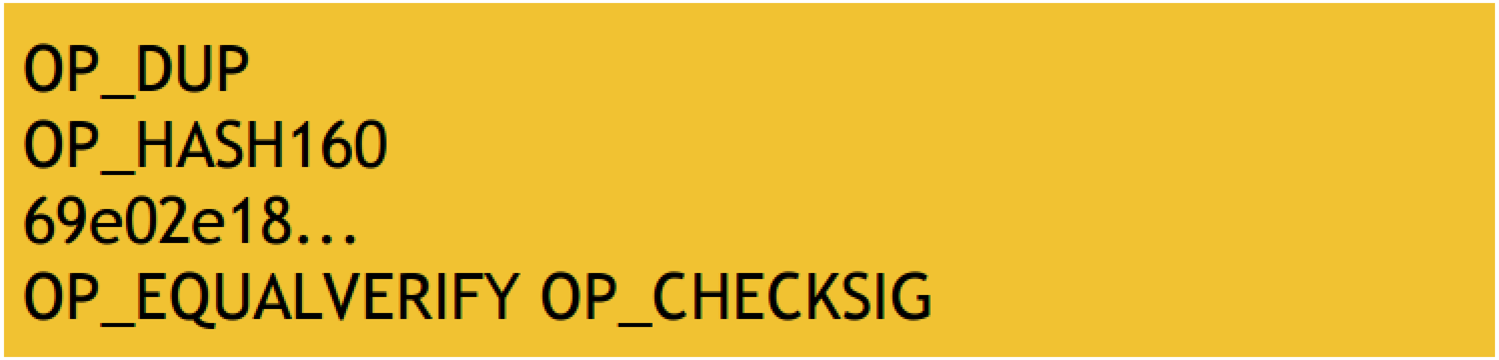
output address

(more outputs)

Script for verifying transaction

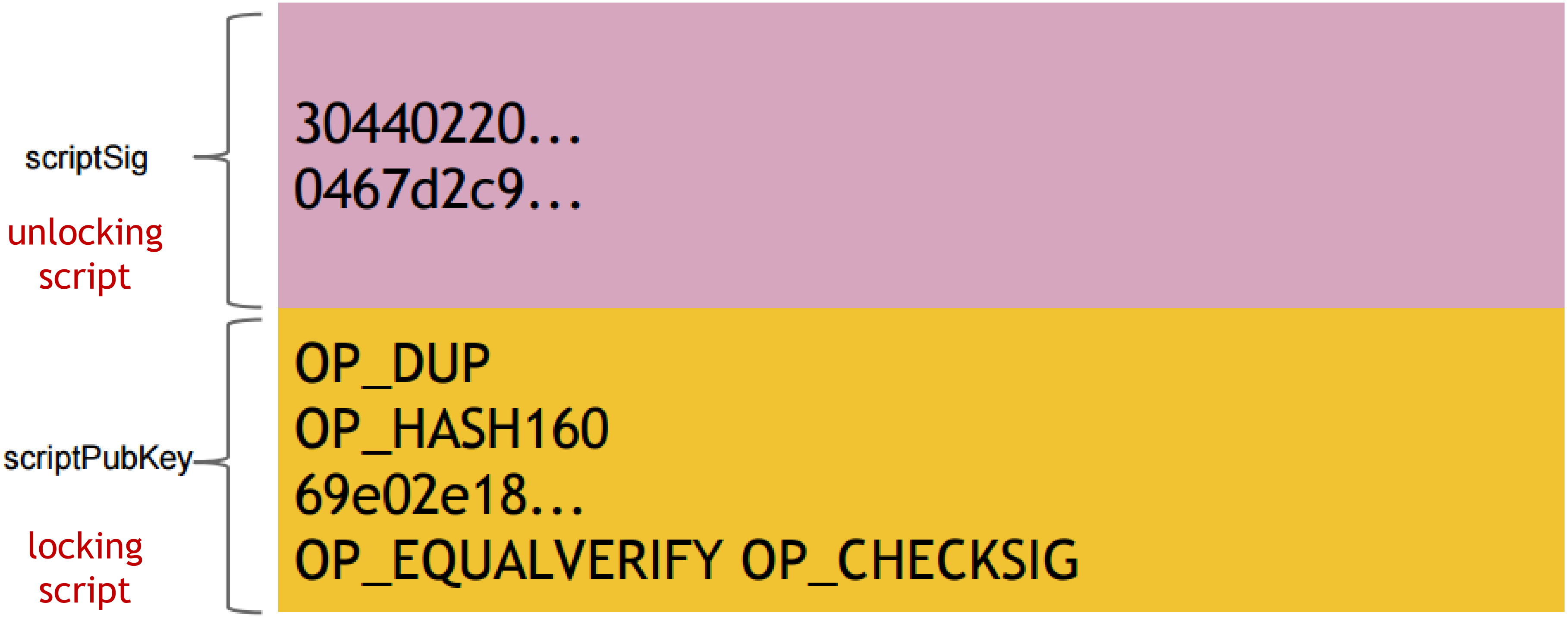
Why are addresses a script??

Output “addresses” are really scripts



```
OP_DUP
OP_HASH160
69e02e18...
OP_EQUALVERIFY OP_CHECKSIG
```

Input "addresses" are *also* scripts



scriptSig

unlocking script

```
30440220...
0467d2c9...
```

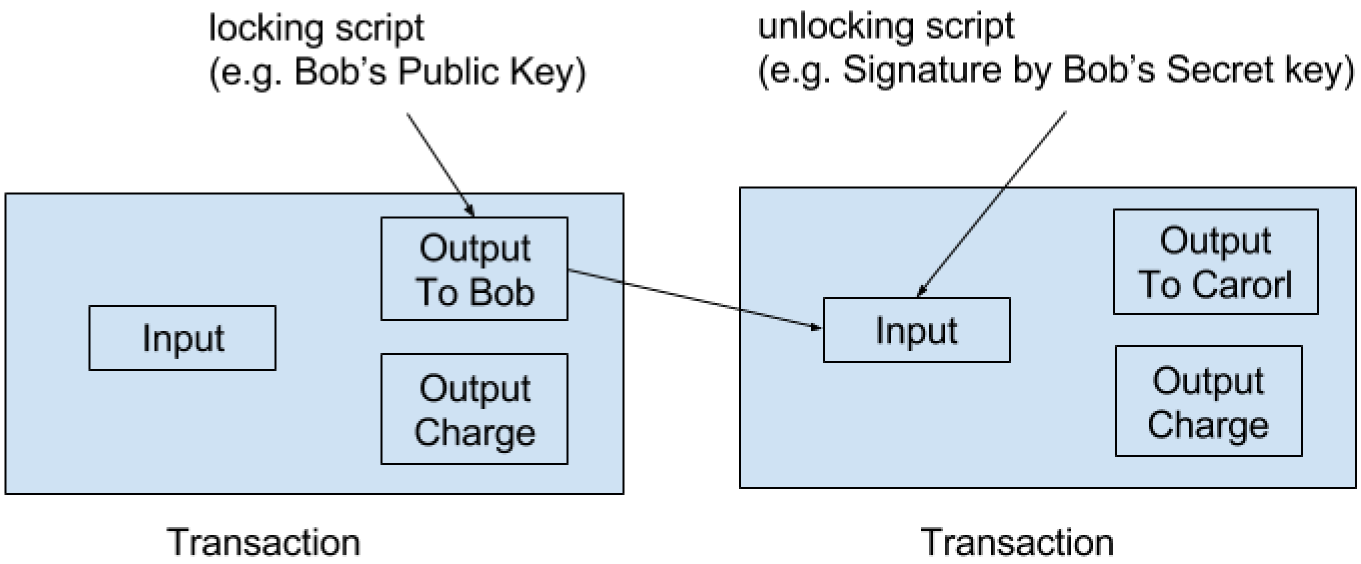
scriptPubKey

locking script

```
OP_DUP
OP_HASH160
69e02e18...
OP_EQUALVERIFY OP_CHECKSIG
```

TO VERIFY: Concatenated script must execute completely with no errors

Concatenated scripts



locking script
(e.g. Bob's Public Key)

unlocking script
(e.g. Signature by Bob's Secret key)

Input

Output
To Bob

Output
Charge

Transaction

Input

Output
To Carorl

Output
Charge

Transaction

Unlocking Script
(scriptSig)

+

Locking Script
(scriptPubKey)

```
<sig> <PubK>    DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
```

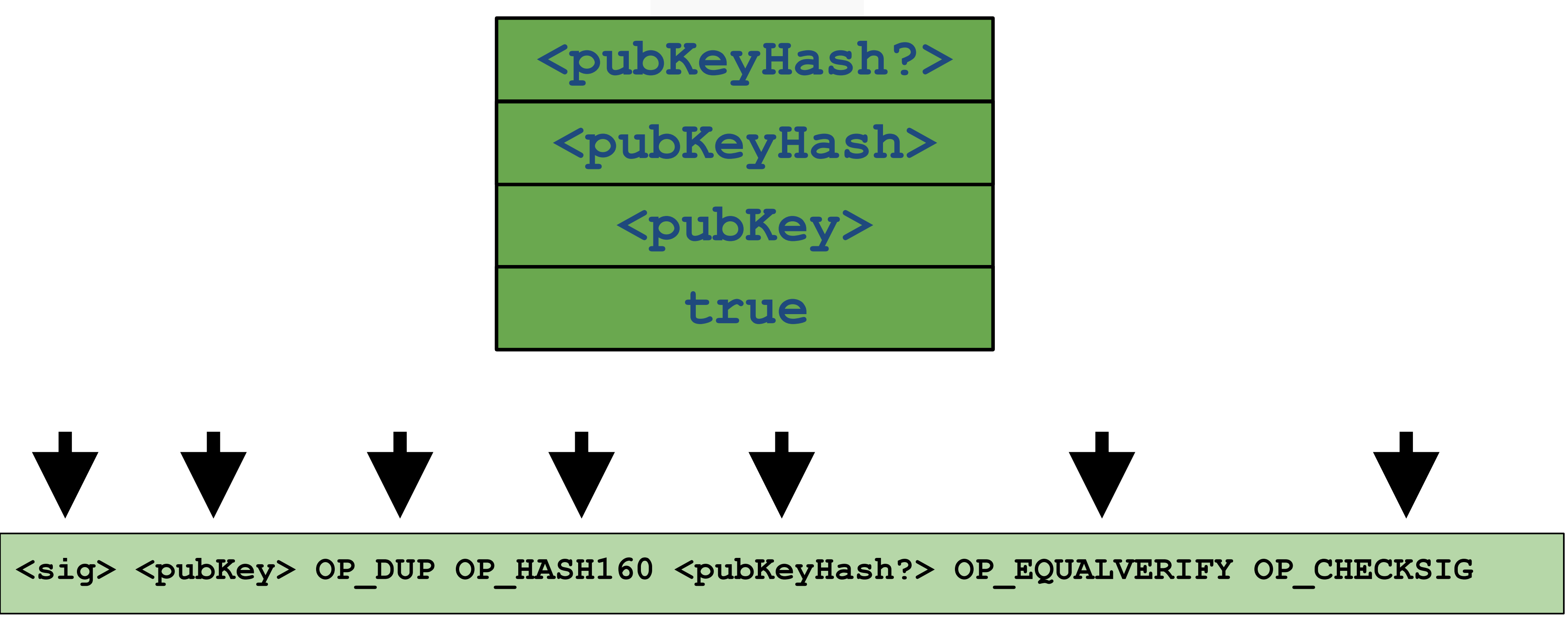
Unlock Script
(scriptSig) is provided
by the user to resolve
the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the
encumbrance that must be fulfilled to spend the output

Common script operations

OP_DUP	Duplicates the top item on the stack
OP_HASH160	Hashes twice: first using SHA-256 and then RIPEMD-160
OP_EQUALVERIFY	Returns true if the inputs are equal. Returns false and marks the transaction as invalid if they are unequal
OP_CHECKSIG	Checks that the input signature is a valid signature using the input public key for the hash of the current transaction
OP_CHECKMULTISIG	Checks that the k signatures on the transaction are valid signatures from k of the specified public keys.

Executing scripts



<pubKeyHash?>

<pubKeyHash>

<pubKey>

true

```
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash?> OP_EQUALVERIFY OP_CHECKSIG
```

Bitcoin scripting language

Design goals

- Built for Bitcoin (inspired by Forth)
- Stack-based
- Simple, finite
- No looping
- Support for cryptography

Bitcoin script instructions

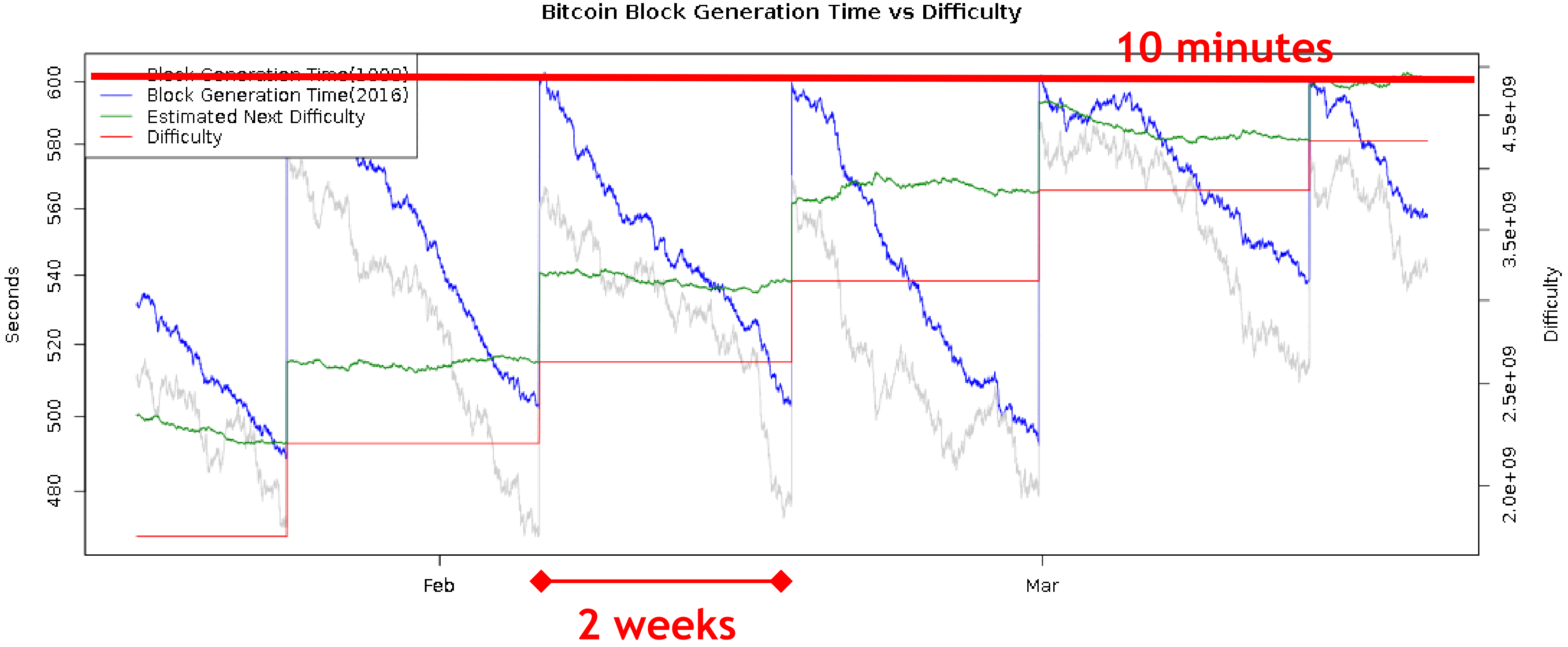
256 opcodes total (15 disabled, 75 reserved)

- Arithmetic
- If/then
- Logic/data handling
- Crypto!
  - Hashes
  - Signature verification
  - Multi-signature verification

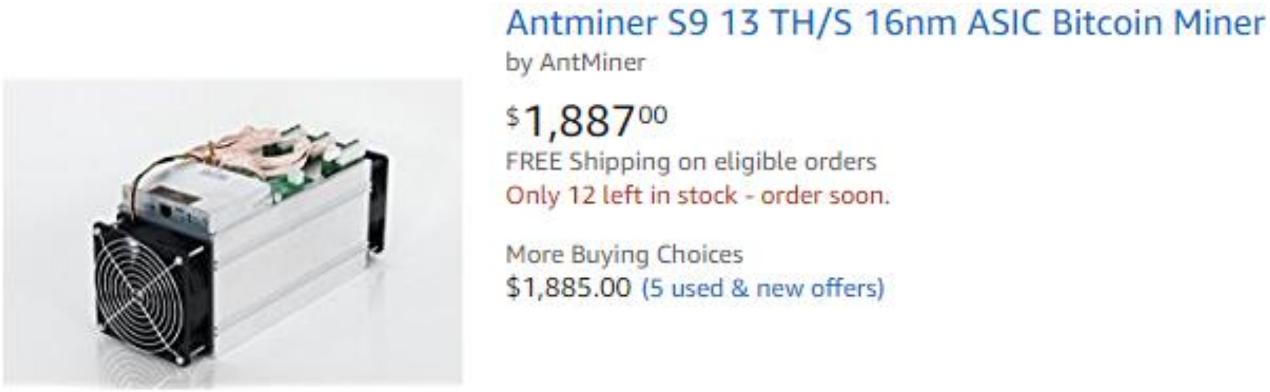
Mining policies

- Rate limiting on the creation of a new block
  - A block created every 10 mins (six blocks every hour)
    - ✓ How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- *N* new bitcoins per each new block: credited to the miner → incentives for miners
  - *N* was 50 initially. In 2013, N=25. In 2016, N=12.5.
  - Halved every 210,000 blocks (≈ every four years)
  - Thus, the total number of bitcoins will not exceed 21 million.

Difficulty adjustment



Bitcoin mining hardware



Antminer S9 13 TH/S 16nm ASIC Bitcoin Miner

by AntMiner

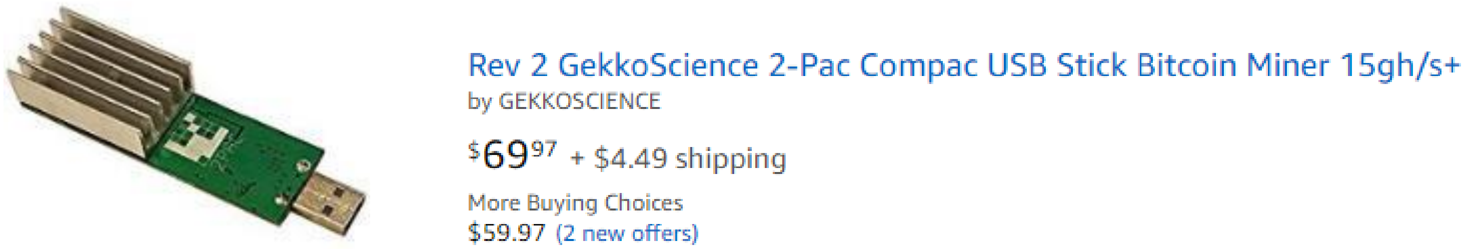
$1,887.00

FREE Shipping on eligible orders

Only 12 left in stock - order soon.

More Buying Choices

$1,885.00 (5 used & new offers)



Rev 2 GekkoScience 2-Pac Compac USB Stick Bitcoin Miner 15gh/s+

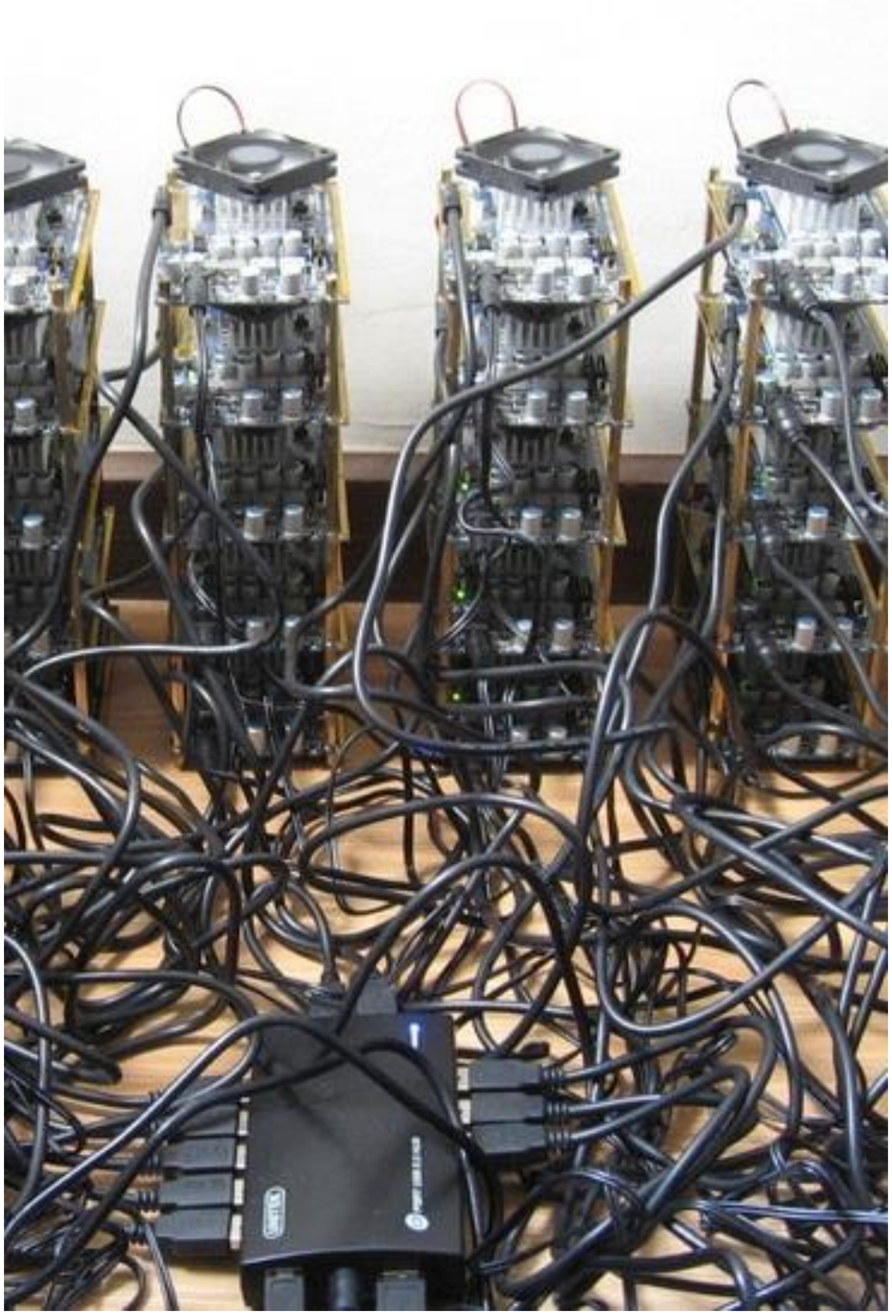
by GEKKOSCIENCE

$69.97 + $4.49 shipping

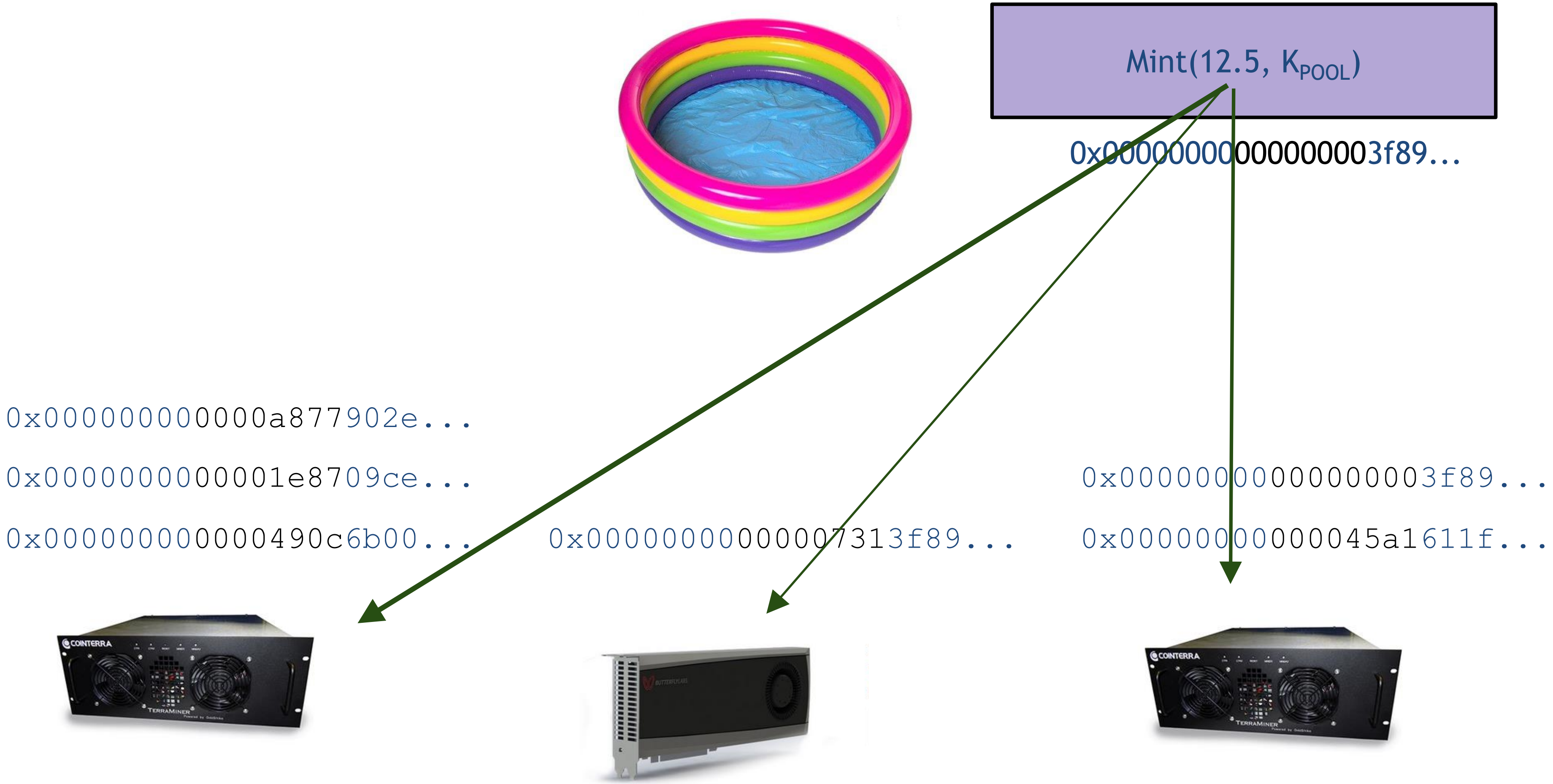
More Buying Choices

$59.97 (2 new offers)

It’s important to remember that Bitcoin mining is competitive and today it is not a good idea for the average person to mine. If you want bitcoins then you are better off buying bitcoins.



Mining pools



Mint(12.5, K_{POOL})

0x00000000000000003f89...

0x000000000000a877902e...

0x0000000000001e8709ce...

0x000000000000490c6b00...

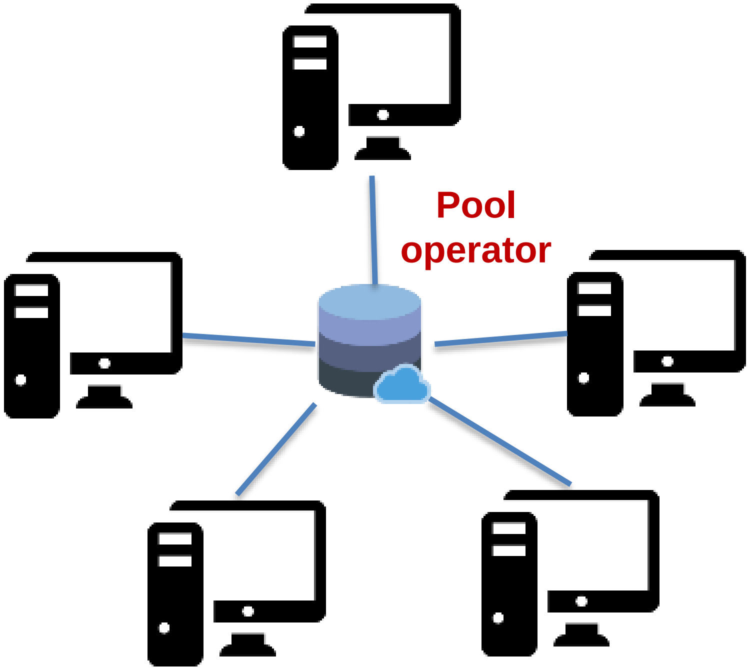
0x00000000000007313f89...

0x00000000000000003f89...

0x00000000000045a1611f...

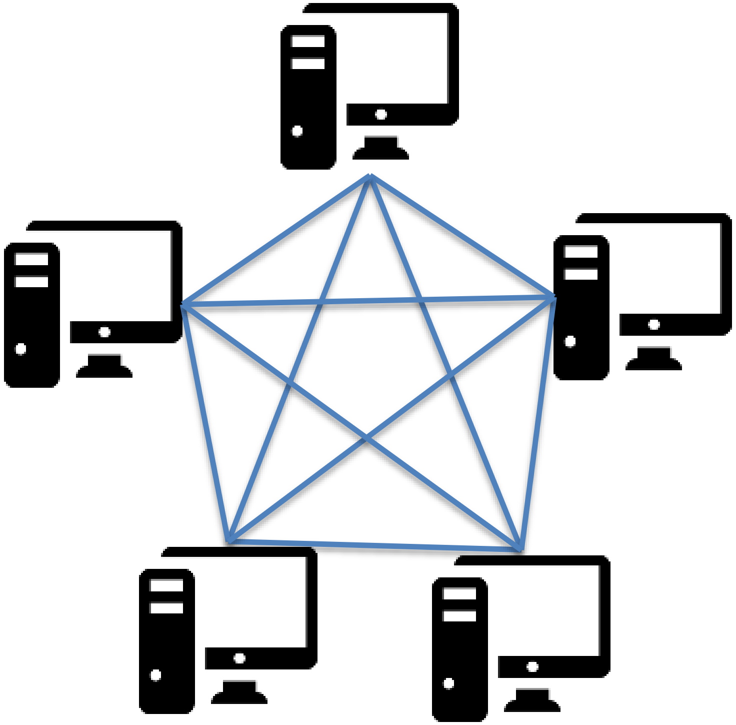
Prove work with “near-valid blocks”

Two popular strategies



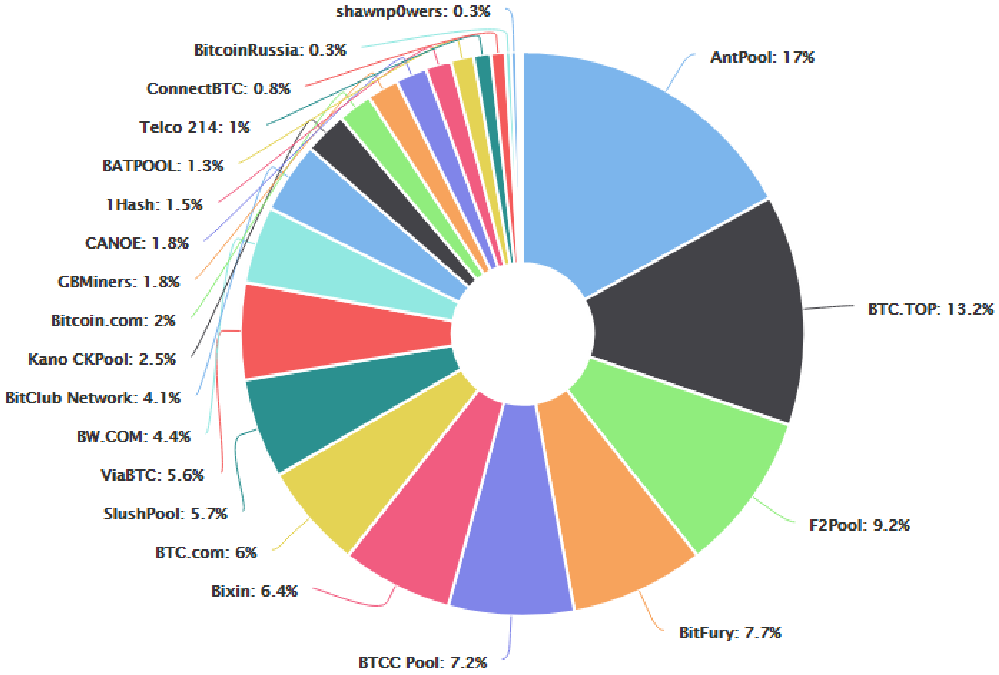
Pool operator

Managed pools



P2P pools

Mining pools in real-world

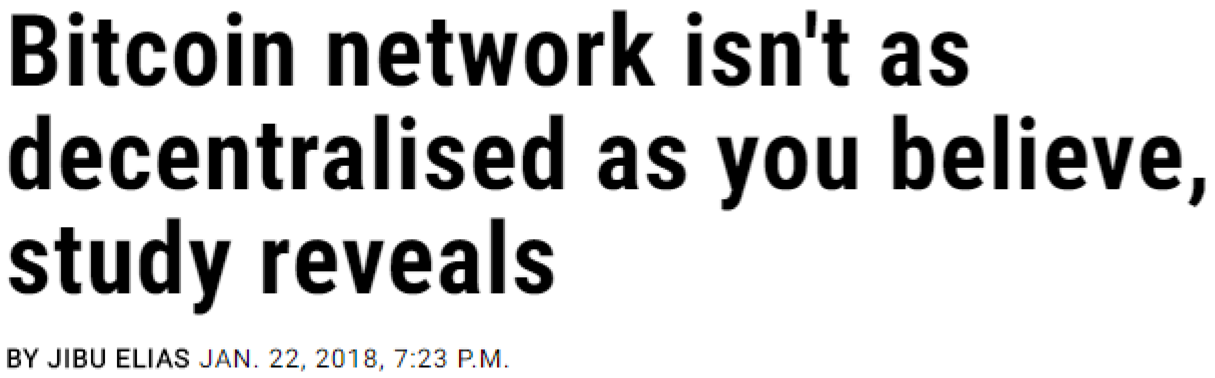


June 6, 2017

At times in the past, one pool, Ghash.IO had over 51% of the computing power.

51% attack: If one guild has more power than all others combined, they can extend their fork faster than any other fork, reaping all rewards and transaction fees, and choosing which transactions to confirm.

https://blockchain.info/pools



Bitcoin network isn't as decentralised as you believe, study reveals

BY JIBU ELIAS JAN. 22, 2018, 7:23 P.M.

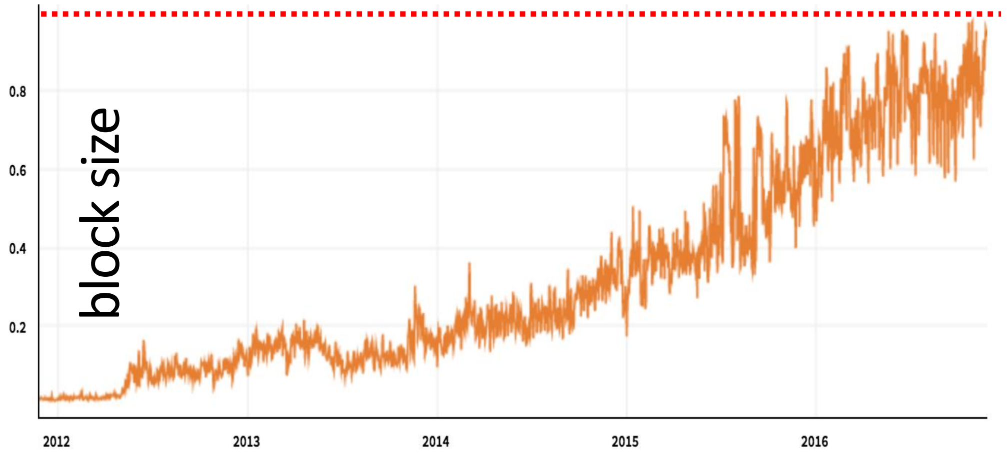
The researchers found that the **top four Bitcoin-mining operations had more than 53% of the system's average mining capacity** and with Etherium, top three miners accounted for 61% of the system's average weekly capacity.

Bitcoin has many more nodes that are closer geographically than Ethereum or any other cryptocurrencies. "Ethereum's most likely latencies are centered around 120ms, while Bitcoin nodes tend to be clustered around 50ms. Only 13% of Ethereum latencies are under 100ms, while Bitcoin has a surprisingly high 46%."

Decentralization in Bitcoin and Ethereum Networks, Gencer et al., Financial Cryptography, 2017.

Scalability of Bitcoin

- Scaling limitations
  - 1 block = 1 MB max
  - 1 block ~ 2000 txns
  - 1 block ~ 10 min
  - So, 3-4 txns / sec
  - Log grows linearly



- VISA peak load comparison
  - Typically 2,000 txns / sec
  - Peak load in 2013: 47,000 txns / sec

There’s no easy fix

- Increasing block size improves throughput
  - Result: Bigger blocks take longer to propagate in the network
- Reducing the block interval reduces latency
  - Result: leads to instability where the system is in disagreement
- Introducing the lightening network

Fast relay network

- A “**Bitcoin Relay Network**” is an overlay network that attempts to minimize the latency in the transmission of blocks between miners.
  - A **hub-and-spoke model** consisted of several specialized nodes hosted on the AWS and served to connect the majority of miners and mining pools

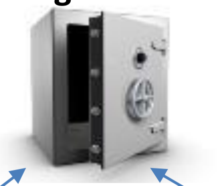
- Fast transmission time
  - **FIBRE** (Fast Internet Bitcoin Relay Engine): UDP-based relay network that implements compact block optimization to further reduce the amount of data transmitted and the network latency
  - **Falcon** (“cut-through-routing” instead of “store-and-forward”): Nodes forward each packet as soon as they receive it

- Lightening network

State channels (1)

- Take small transactions out of the main blockchain (off chain)
- Suppose Bob buys a coffee regularly at Starbucks
- It is inefficient to use the main blockchain for small transactions
- The solution is to set up a multi-signature address that is shared by Bob and Starbucks

Multi-signature address



Multi-signature address is like a vault that can only be opened when both parties agree. This is a "payment channel".

Bob deposits 0.05BTC

Starbucks deposits 0.00BTC

Payment Channel Ledger	
Bob	0.05
Starbucks	0.00

State channels (2)

- Bob goes to Starbucks and orders an expresso which costs 0.005BTC
- State channel ledger is updated off chain

State Channel Ledger	
Bob	0.05
Starbucks	0.00

- Bob and Starbucks sign the updated balance sheet and each keep a copy of the ledger
- There is no limit on the number of transactions per second because these transactions are happening off chain

State channels (3)

- State channel can be closed at any time
- Either party simply needs to take the latest ledger which is signed by both parties and broadcast it to the network
- Miners verify the signatures on the ledger and then release the funds (single transaction to close). This is an on-chain transaction.

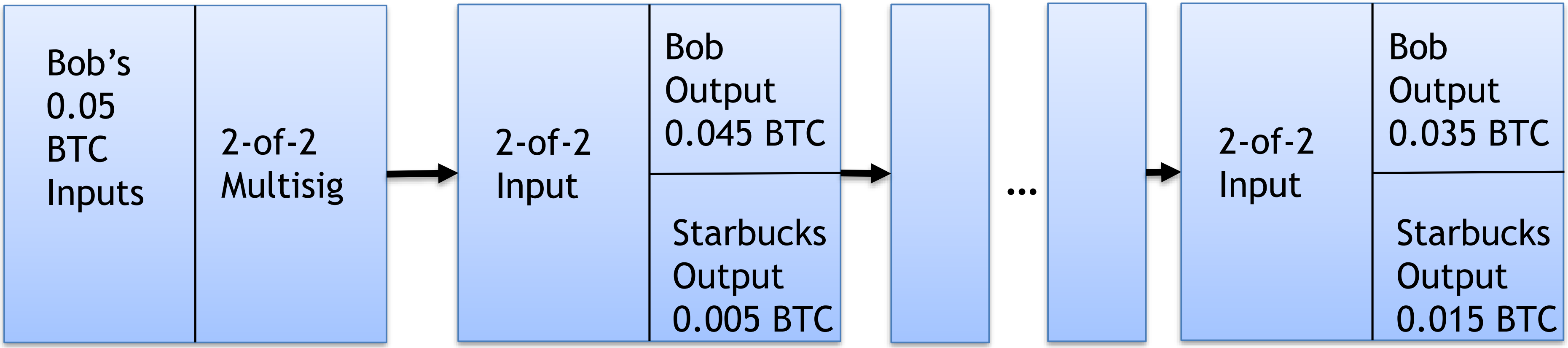
0.015 to Bob

Payment Channel Ledger	
Bob	0.05
Starbucks	0.00

0.035 to SB

State channels (4)

- The channel can be closed either cooperatively, by submitting a final settlement transaction to the blockchain.
- The settlement transaction represents the final state of the channel and is settled on the blockchain.



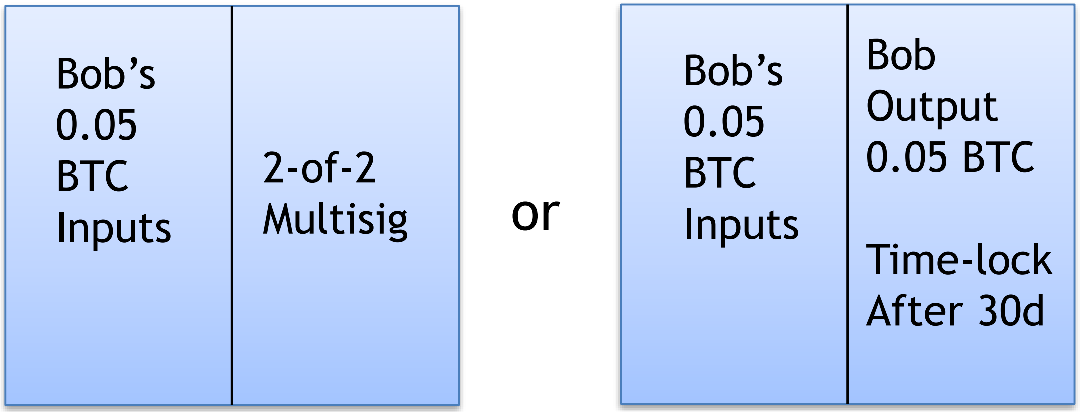
Funding transaction
(On-chain)

Settlement transaction
(On-chain)

Use of timelock

- Using the timelock expiration, Bob can redeem the refund transaction even if Starbucks disappears.

```
IF
        2 <Bob's pubkey> <Starbucks's pubkey> 2 CHECKMULTISIG
ELSE
        "30d" CHECKSEQUENCEVERIFY DROP <Bob's pubkey> CHECKSIG
ENDIF
```



Bob's 0.05 BTC Inputs | 2-of-2 Multisig

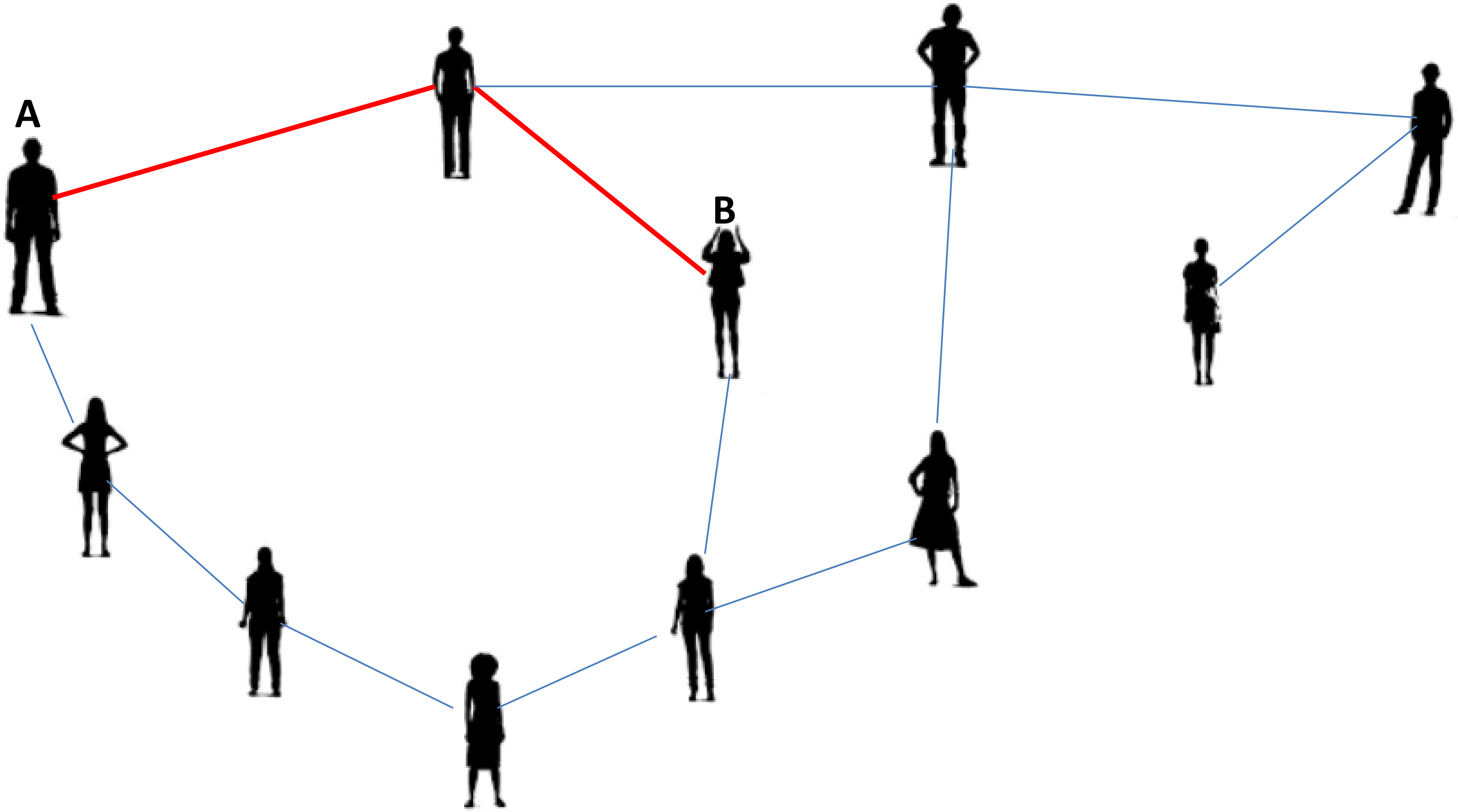
or

Bob's 0.05 BTC Inputs | Bob Output 0.05 BTC

Time-lock After 30d

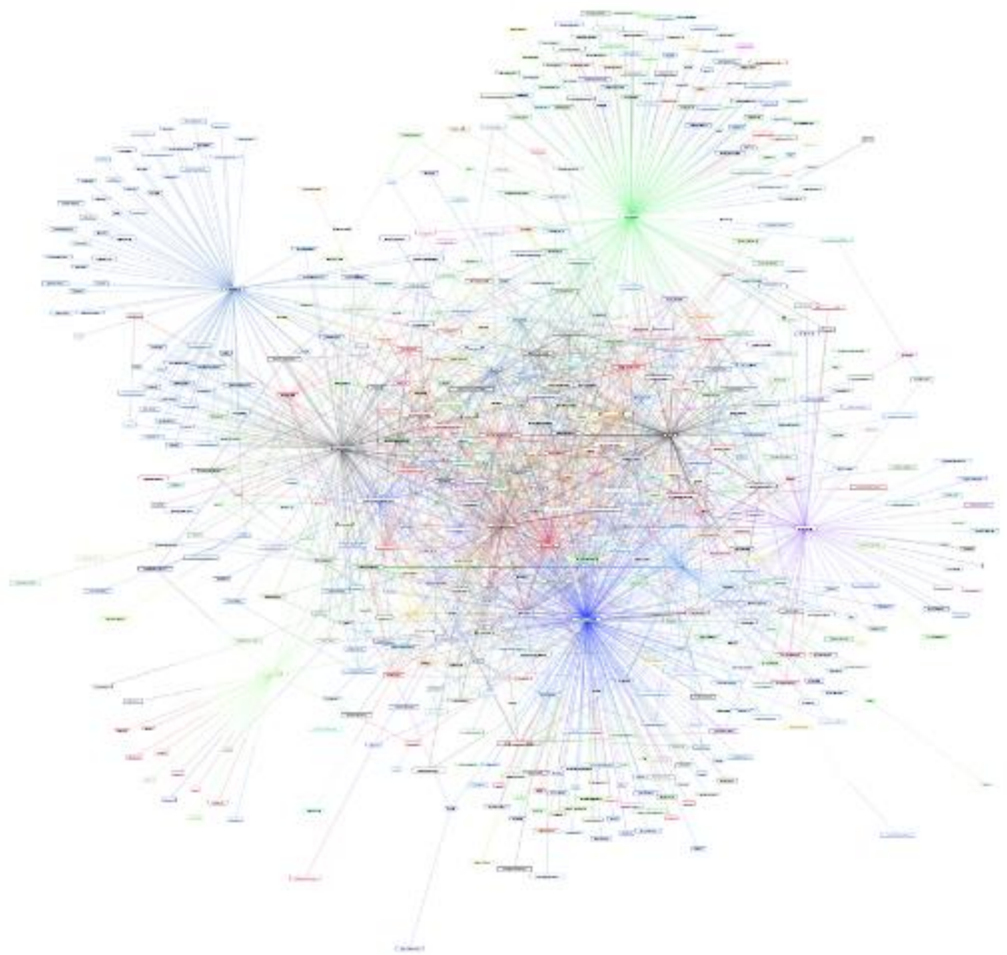
Lightening network

Network finds the fastest and cheapest way to connect A to B. It is also important that the channels have enough funds to do the transaction.



Lighting network mainnet

- Actual payments were used within lightning channels.
- February 22, 2018: 833 nodes and 1612channels



https://lnmainnet.gaben.win/

Questions?

Sungkyunkwan
Campus
Social
Institute
University's
establishment
now
Graduate
constructed
Professors
English
Building
Anniversary
Joseon
located
Engineering
Global
Education
campus
Sciences
University
Confucian
Korea
Seoul
Natural
Suwon
School
university
Korean
edit
established
Humanities
lecturers
Advanced
Science
schools
Administration
ASLE-Korea
Academic
also
two
four
capital
city
Zone
trees
symbol
Hall
Course
Language
heart
one
years

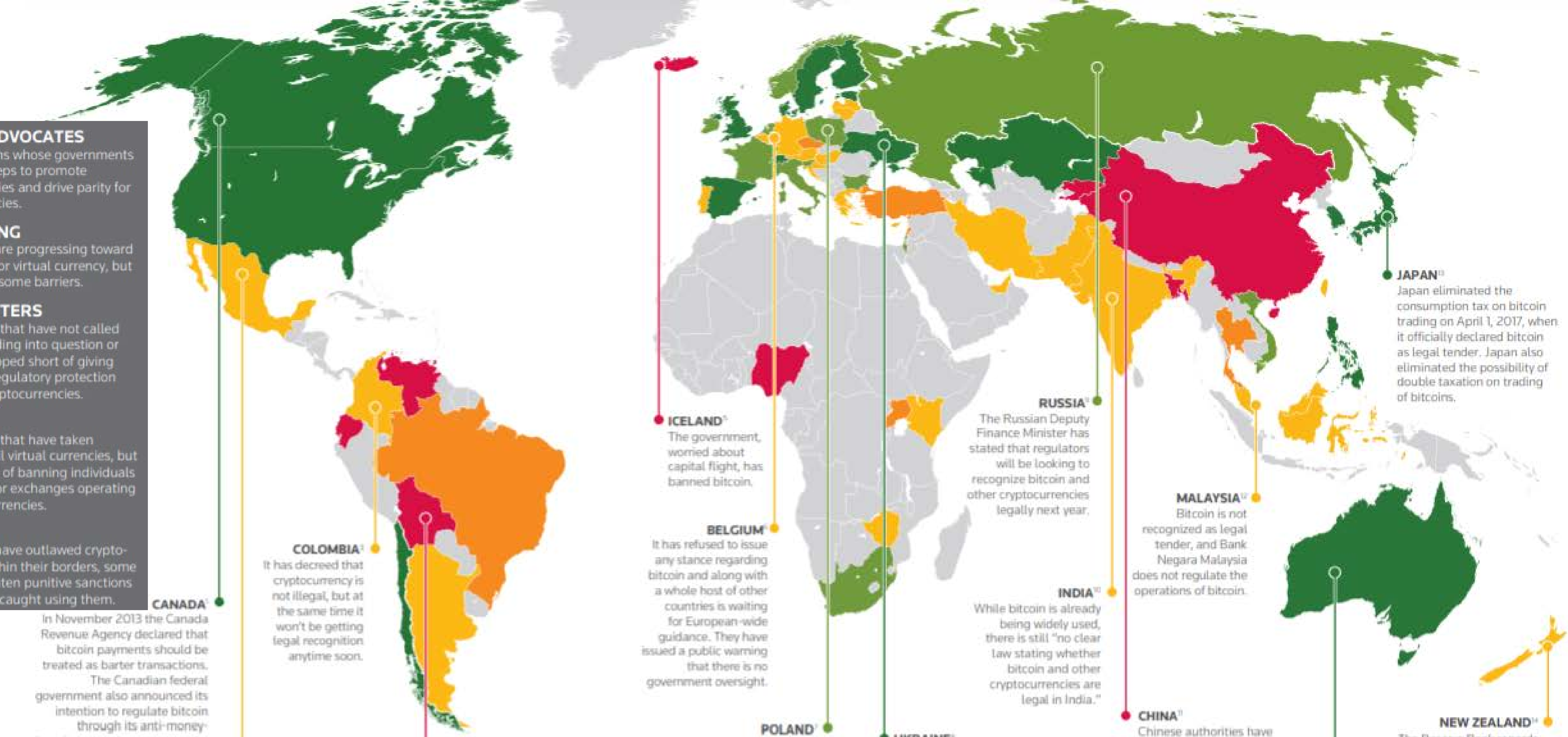
암호화폐와 정책

고려대학교 정보보호대학원

김형중

khj-@korea.ac.kr

2018. 04. 19



● **GLOBAL ADVOCATES**
Pioneer nations whose governments have taken steps to promote cryptocurrencies and drive parity for virtual currencies.

● **DEVELOPING**
Nations that are progressing toward equal status for virtual currency, but there are still some barriers.

● **FENCE-SITTERS**
Governments that have not called individual trading into question or that have stopped short of giving any legal or regulatory protection to users of cryptocurrencies.

● **HOSTILE**
Governments that have taken steps to curtail virtual currencies, but stopped short of banning individuals from trading or exchanges operating with cryptocurrencies.

● **BANNED**
Nations that have outlawed cryptocurrencies within their borders, some of which threaten punitive sanctions to individuals caught using them.

CANADA[1]
In November 2013 the Canada Revenue Agency declared that bitcoin payments should be treated as barter transactions. The Canadian federal government also announced its intention to regulate bitcoin through its anti-money-laundering and counterterrorist financing legislation.

MEXICO[2]
The Mexican government has not banned the use of alternative digital currencies outright, but instead is in talks with government regulators to try and introduce their own form of bitcoin and their own blockchain specific to Mexico.

COLOMBIA[3]
It has decreed that cryptocurrency is not illegal, but at the same time it won't be getting legal recognition anytime soon.

BOLIVIA[4]
The Bolivian government has banned the use of bitcoin in the belief that it will allow tax evasion and monetary instability.

ICELAND[5]
The government, worried about capital flight, has banned bitcoin.

BELGIUM[6]
It has refused to issue any stance regarding bitcoin and along with a whole host of other countries is waiting for European-wide guidance. They have issued a public warning that there is no government oversight.

POLAND[7]
The Polish government has officially recognized the trading and mining of virtual currencies as an "official economic activity," but has said that regulation should come from the EU.

UKRAINE[8]
Despite vague government regulations and political uncertainty in some areas, a major bank announced the ability to purchase bitcoins in any of its nationwide ATM terminals.

RUSSIA[9]
The Russian Deputy Finance Minister has stated that regulators will be looking to recognize bitcoin and other cryptocurrencies legally next year.

INDIA[10]
While bitcoin is already being widely used, there is still "no clear law stating whether bitcoin and other cryptocurrencies are legal in India."

CHINA[11]
Chinese authorities have banned token sales and local exchanges are closing down.

MALAYSIA[12]
Bitcoin is not recognized as legal tender, and Bank Negara Malaysia does not regulate the operations of bitcoin.

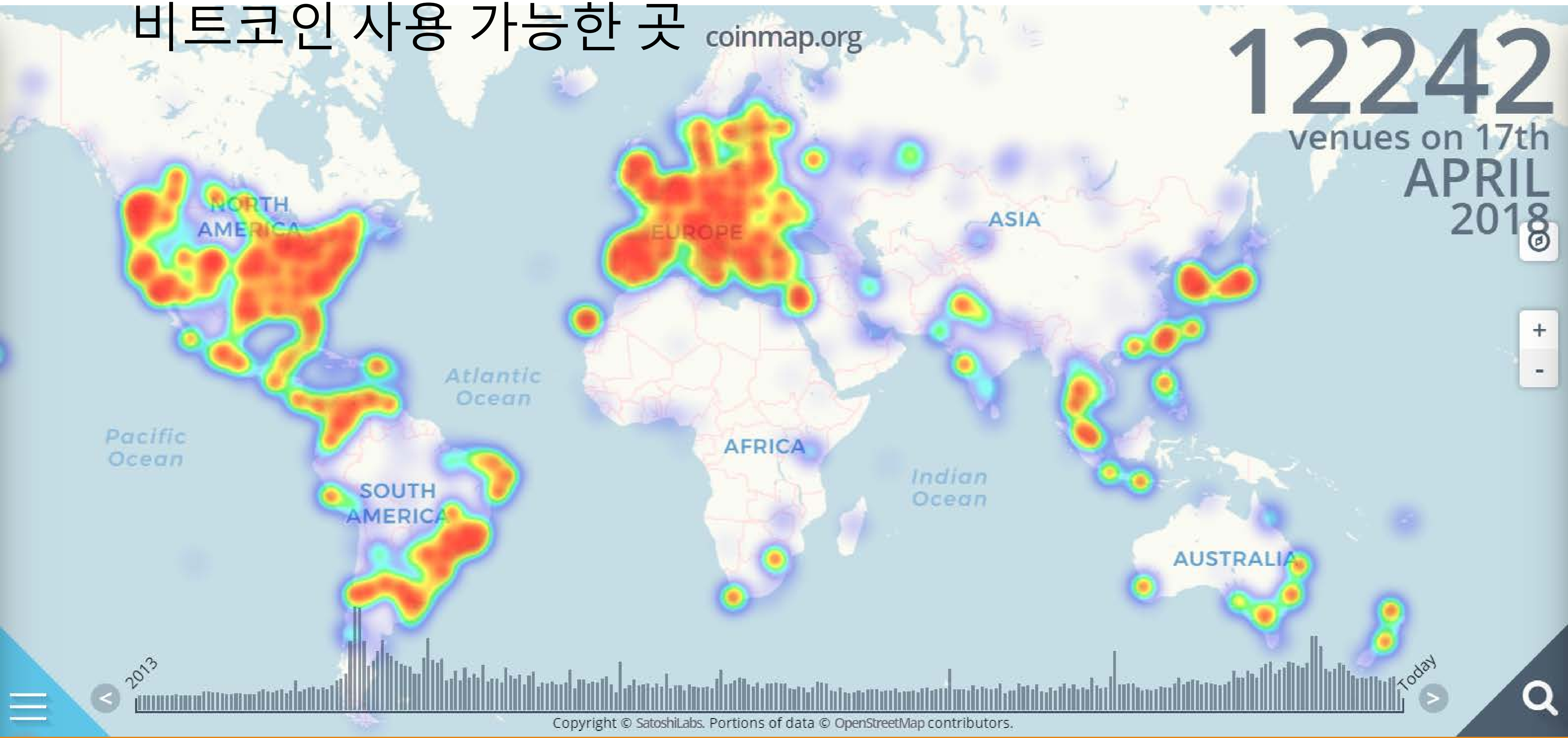
JAPAN[13]
Japan eliminated the consumption tax on bitcoin trading on April 1, 2017, when it officially declared bitcoin as legal tender. Japan also eliminated the possibility of double taxation on trading of bitcoins.

NEW ZEALAND[14]
The Reserve Bank regards cryptocurrencies as a "vulnerability" and considers cryptocurrency as a payment system rather than a currency.

AUSTRALIA[15]
Removing bitcoins from double taxation policies, the government also legalized bitcoin and said it can be used just like money.

Cryptocurrencies by Country, Thompson Reuters, 25 Oct. 2017

비트코인 사용 가능한 곳



Cryptocurrencies by Country, Thompson Reuters, 25 Oct. 2017

한국의 규제

- 2017년 9월 1일: 금융위, ‘지분증권·채무증권 등 증권발행 형식의 ICO는 자본시장법 위반으로 처벌할 것’
- 2017년 9월 29일: 금융위, ‘모든 형태의 ICO 금지’
- 2017년 12월 11일: 금융위원장, 기자 간담회에서 '비트코인 거래 전면금지를 포함한 규제안을 검토 중' 발표
- 2017년 12월 28일: 주요 거래소 가상계좌 발급 중지
- 2018년 1월 12일: 법무부장관, ‘모든 거래소를 폐쇄하고 개인간 거래만 허용하는 법률을 준비 중’
- 2018년 1월 30일: 거래소 거래 실명제 시행. 은행으로부터 가상계좌를 발급받은 가상화폐 거래소 4곳 (업비트, 빗썸, 코인원, 코빗)
    - 나머지 거래소는 가상계좌 사용이 중지돼 원화 입금이 안 되거나 법인계좌를 이용해 투자자들로부터 자금을 받음

규제의 기준

- 불법자금 차단 (KYC, AML 등)
- 투자자/소비자보호 (유사수신 금지, 정확한 정보제공, 개인정보보호, 시스템 보안 등)

- 산업진흥

규제의 대상

- 암호화폐 (과세 등)
- ICO (자본시장법 준수 여부 등)
- 암호화폐 자산운용
- 거래소 (거래소 보안, 전자지갑 보안, 뱅크런 방지 등)
- 국가재정정책 (암호화폐를 통한 자금의 해외 유출에 따른 금융리스크 등)
- 국가 통계
- 정보공개 (프라이버시 침해, 영업비밀 유출 등)
- 가상계좌

현금 없는 사회로

- 스웨덴에서는 현금사용 비율이 2% 미만 (현금도 카드로 결제)
- 2009년 스웨덴에서 마이너스 금리 제도 시행으로 현금 없는 사회 가속화
- 1661년 스웨덴에서 최초로 지폐 발행
- 현금 없는 사회에서 정보의 비대칭 문제 사라짐 (고객의 수입, 지출과 그 패턴을 은행이 더 잘 파악할 수 있음)
- 탈세 예방 등에 현금 없는 사회가 도움이 됨

현금을 받지 않는다는 안내문

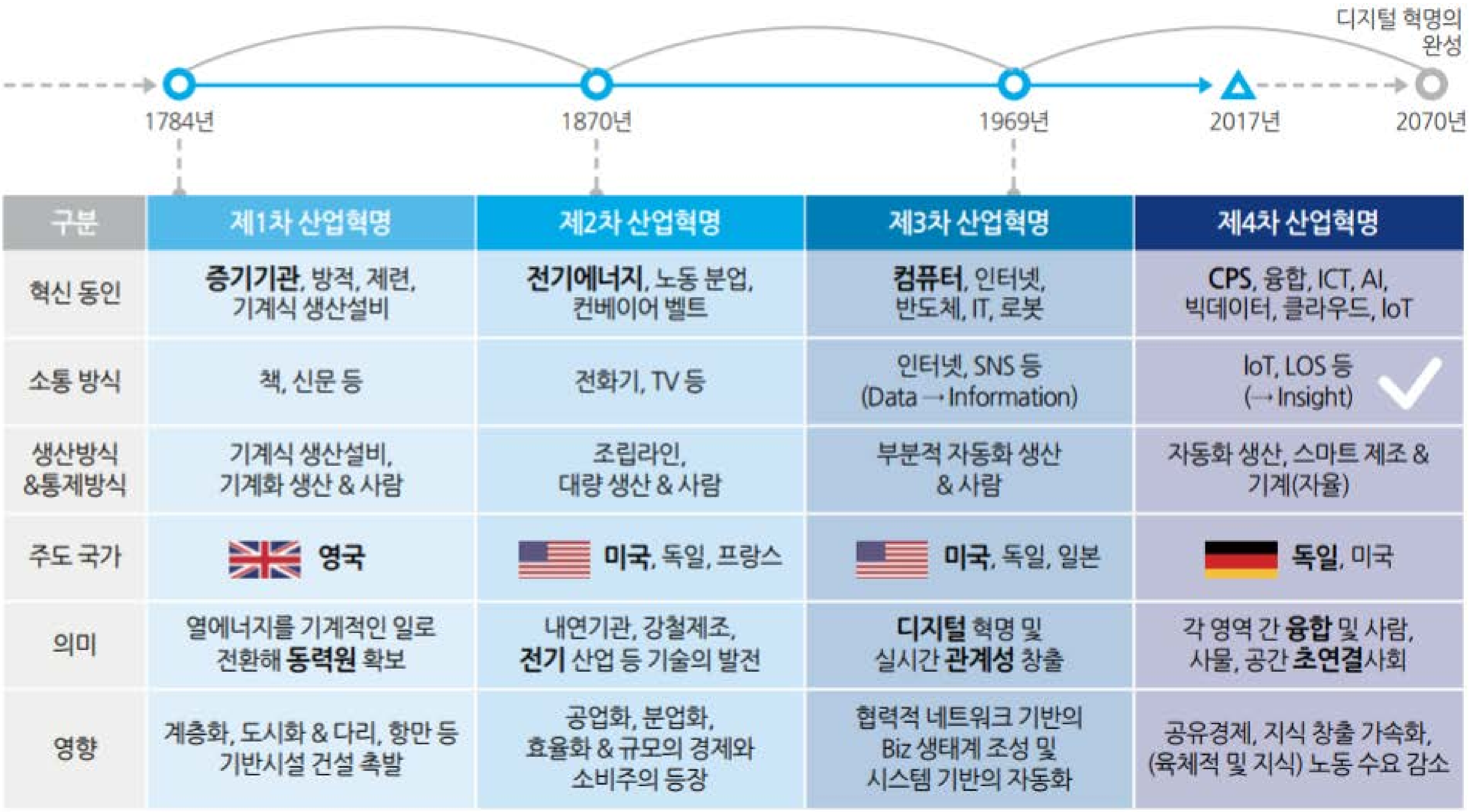
지폐의 미래

- 전자기술의 급속한 발전으로 화폐위조기술 역시 발전 → 지폐 발행비용 및 감별비용 증가
- 2005년부터 77246 번호가 찍힌 5천원권 4만 5838장의 위조범 잡지 못함 (워터마크도 삽입)
- 2015년 영화 '기술자'를 모방해서 고교생이 5만원권 150장을 복사해 사용하다 검거됨 (복사 안되는 띠 모양의 홀로그램, 은색 매니큐어를 덧칠)
- 지폐는 기술적 요인으로 인해 언젠가는 사라질 것
- 반드시 이중지불 (double spending) 불가해야

7년째
잡히지 않은
77246 위조지폐의 비밀

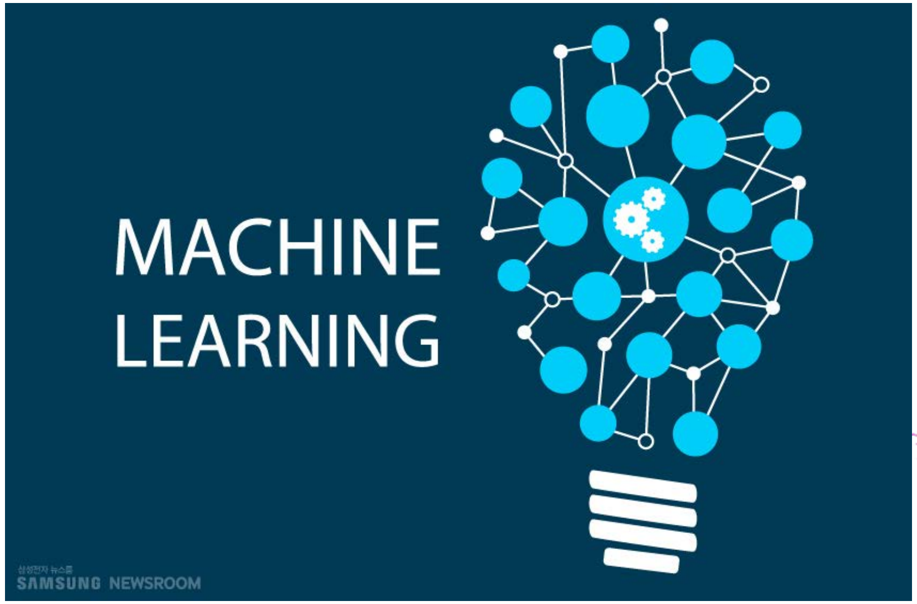
모호한 4차산업혁명

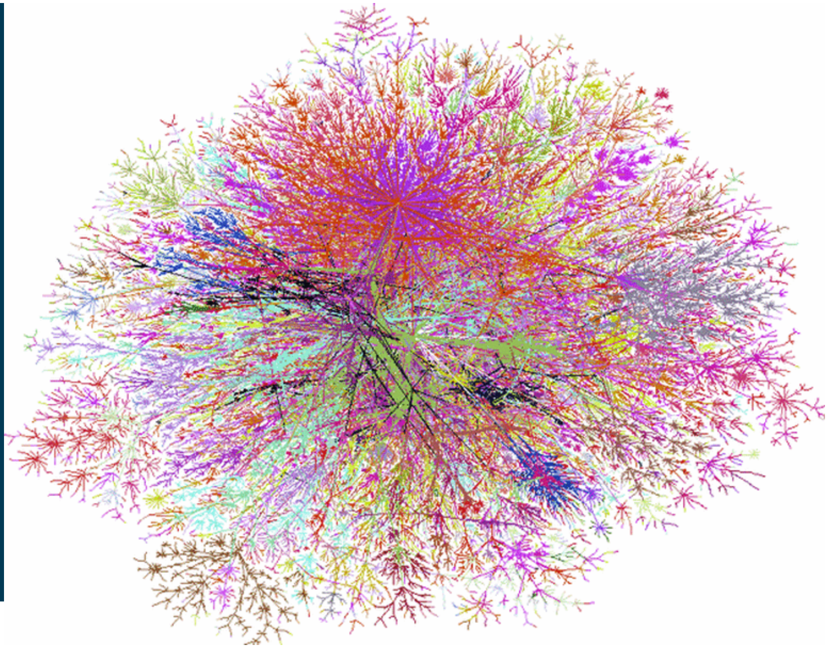
출처: 딜로이트 애널리시스


디지털 혁명의
완성
1784년
1870년
1969년
2017년
2070년

구분	제1차 산업혁명	제2차 산업혁명	제3차 산업혁명	제4차 산업혁명
혁신 동인	**증기기관**, 방적, 제련, 기계식 생산설비	**전기에너지**, 노동 분업, 컨베이어 벨트	**컴퓨터**, 인터넷, 반도체, IT, 로봇	**CPS**, 융합, ICT, AI, 빅데이터, 클라우드, IoT
소통 방식	책, 신문 등	전화기, TV 등	인터넷, SNS 등 (Data → Information)	IoT, LOS 등 (→ Insight) ✓
생산방식 &통제방식	기계식 생산설비, 기계화 생산 & 사람	조립라인, 대량 생산 & 사람	부분적 자동화 생산 & 사람	자동화 생산, 스마트 제조 & 기계(자율)
주도 국가	**영국**	**미국**, 독일, 프랑스	**미국**, 독일, 일본	**독일**, 미국
의미	열에너지를 기계적인 일로 전환해 **동력원** 확보	내연기관, 강철제조, **전기** 산업 등 기술의 발전	**디지털** 혁명 및 실시간 **관계성** 창출	각 영역 간 **융합** 및 사람, 사물, 공간 **초연결**사회
영향	계층화, 도시화 & 다리, 항만 등 기반시설 건설 촉발	공업화, 분업화, 효율화 & 규모의 경제와 소비주의 등장	협력적 네트워크 기반의 Biz 생태계 조성 및 시스템 기반의 자동화	공유경제, 지식 창출 가속화, (육체적 및 지식) 노동 수요 감소

불길한 기술





- 인공지능, 빅데이터, 클라우드 기술은 일자리를 축소하는 기술
- 소수의 혁신적인 기업과 인재들이 독점적 지위를 누림

새로운 미래유망 10대 서비스

개인 맞춤형 헬스케어 서비스

현금없는 금융 서비스

무인 네트워크 운송 서비스

사물 인터넷 재난 대응서비스

건강수명 증진 서비스

전력 충전 서비스

그린 에너지 플랫폼 서비스

인공지능 만능 전문가 서비스

웨어러블 에너지 공급 서비스

소셜 러닝 서비스

① 학습자 ② 동료 ③ 행동과 관련된 보상

적기조례의 교훈

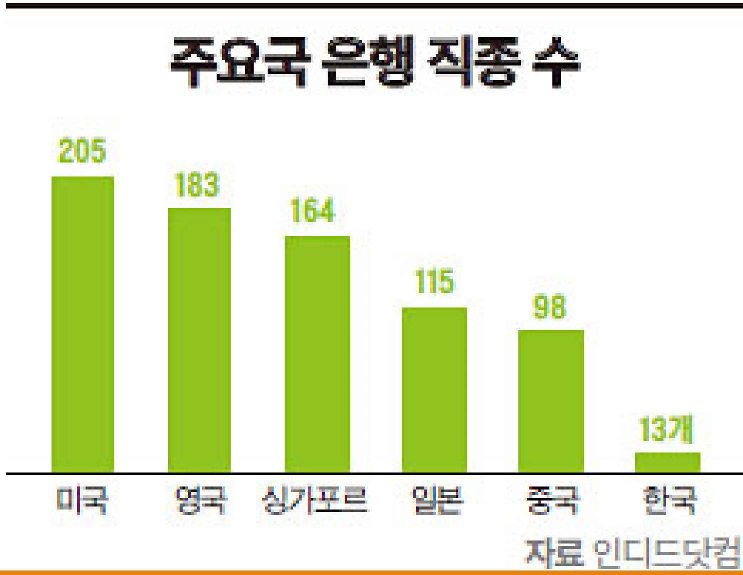
- 1861년 The Locomotives on Highways Act
  - 속도(10/5 mph) 및 중량(14 ton) 제한
- 1865년 The Locomotive Act (적기조례)
  - 속도(4/2 mph) 제한
  - 운전자, 기관원, 전방주행요원 (55m 앞 → 18m 앞)
- 1878년 Highways and Locomotives Act
- 1896년 폐지

- 신기술이 등장할 때마다 적기조례 등장
- 한국 정부의 암호화폐 규제가 일종의 적기조례

한국 금융의 수준

- 2015년 WEF 조사: 140개 국가 중 87위
- 2016년 IMF 금융발전지수: 183개국 중 6위
- 2018년 WEF 금융시장 성숙도: 137개국 중 74위

- 그런데 한국이 금융산업에서 1등을 하려 한다면?



한국의 암호화폐 위상

순위	거래소	24시간 거래규모
1	Upbit	45억 달러
2	Bithumb	41억 달러
3	Binance	27억 달러
4	OKEx	18억 달러
5	Bitfinex	16억 달러
6	Huobi	9억 달러

순위	암호화폐	24시간 거래규모
1	Bitcoin	1938억 달러
2	Ethereum	1013억 달러
3	Ripple	534억 달러
4	Bitcoin Cash	297억 달러
5	Cardano	158억 달러
15	ICON	33억 달러

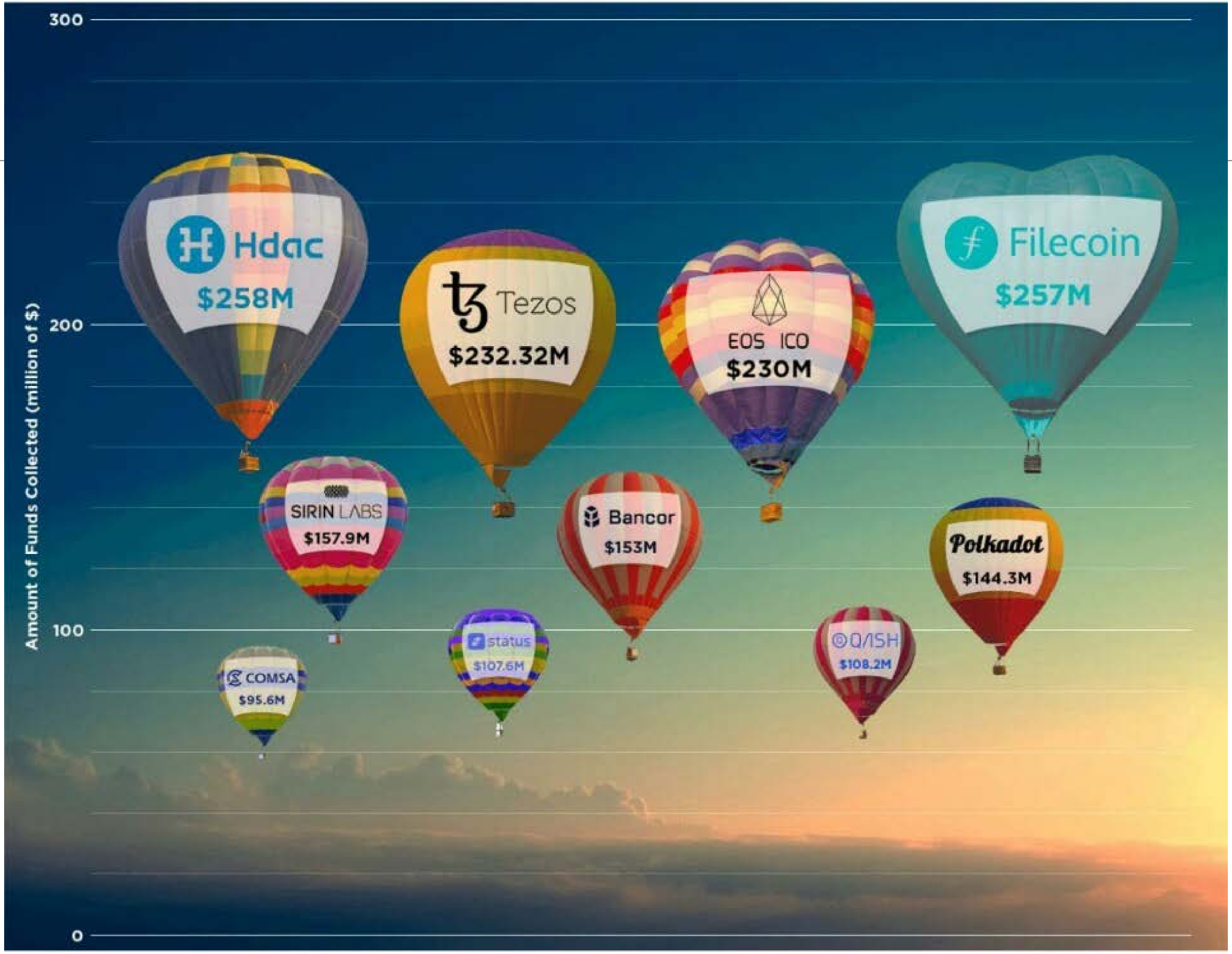
- 암호화폐가 블로체인 최고의 응용사례
- 암호화폐는 블록체인 위에서 합의 도출, 무결성 확보, 익명성 보호 등 다양한 기술을 구현한 제품
- 암호화폐와 불록체인이 불가분의 관계인지 논의하는 것은 무의미한 시도
- 암호화폐 시장에서 한국이 주도권을 잡을 여건 조상됨

국가별 암호화폐 거래규모

국가	거래소 (점유율)	비율
중국	Binance (14.74), OKEx (10.83), Bitfinex (9.81), Huobi (9.58), Bit-Z (1.22)	46.18%
한국	Upbit (11.26), Bithumb (9.43)	20.69%
일본	Bitflyer (11.96), Quoine (1.29)	13.25%
미국	GDAX (2.49), Bittrex (2.42), Kraken (2.24)	7.15%
기타		12.73%

2018년 4월 13일 https://www.coinhills.com/market/exchange/ 자료에서 1% 이상 점유하는 거래규모가 큰 거래소만 뽑아 정리한 자료

Top 10 Initial Coin Offerings (ICOs) in 2017



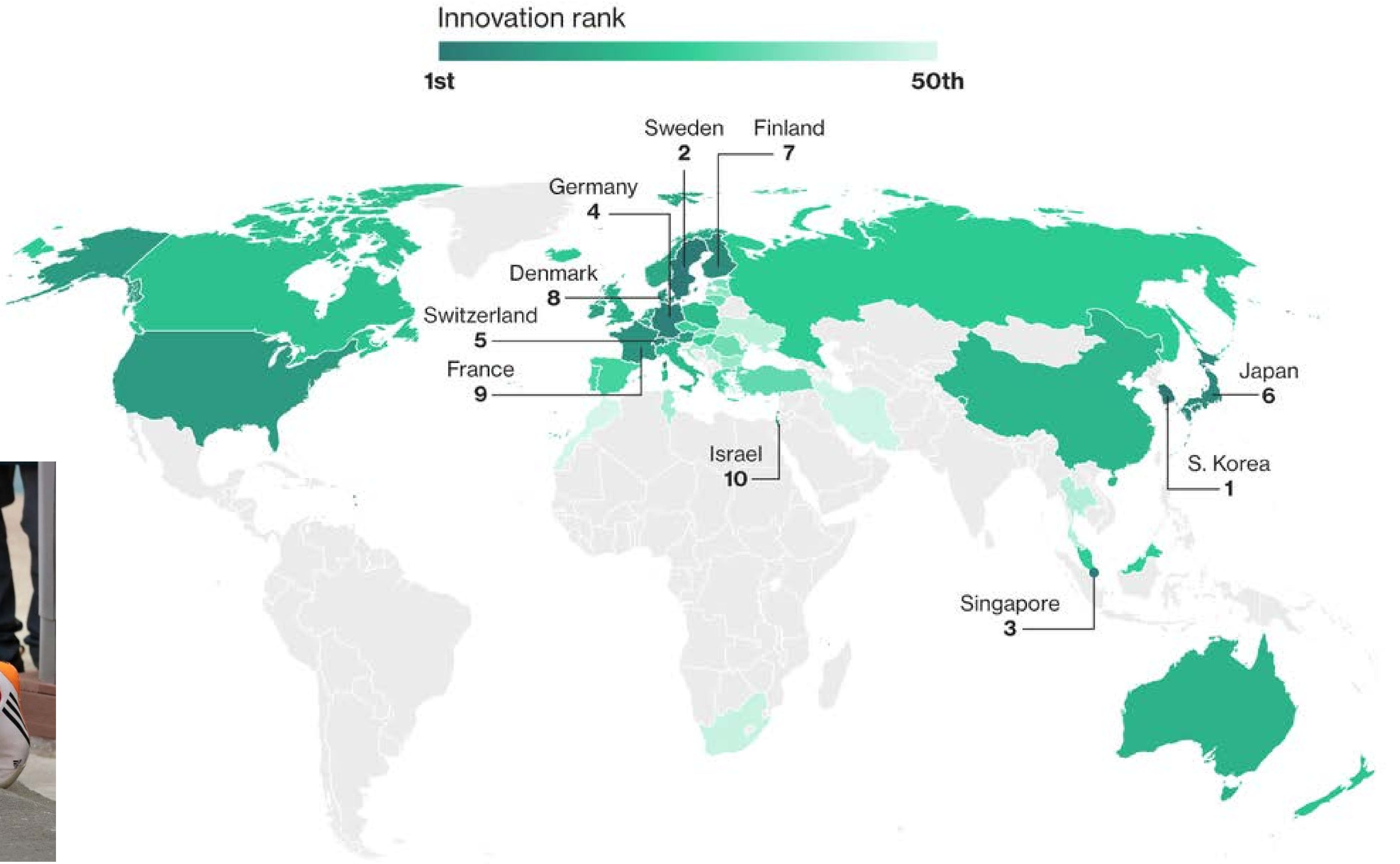
Articles and Sources:
https://howmuch.net/articles/top-10-icos-2017
tokendata.io, icodrops.com, coinschedule.com

howmuch.net

한국의 위상

Fifty Most Innovative Economies

South Korea, Sweden and Singapore top the list; U.S. drops out of top 10.



Sources: Bloomberg, International Labour Organization, International Monetary Fund, World Bank, Organization for Economic Co-operation and Development, World Intellectual Property Organization

Bloomberg

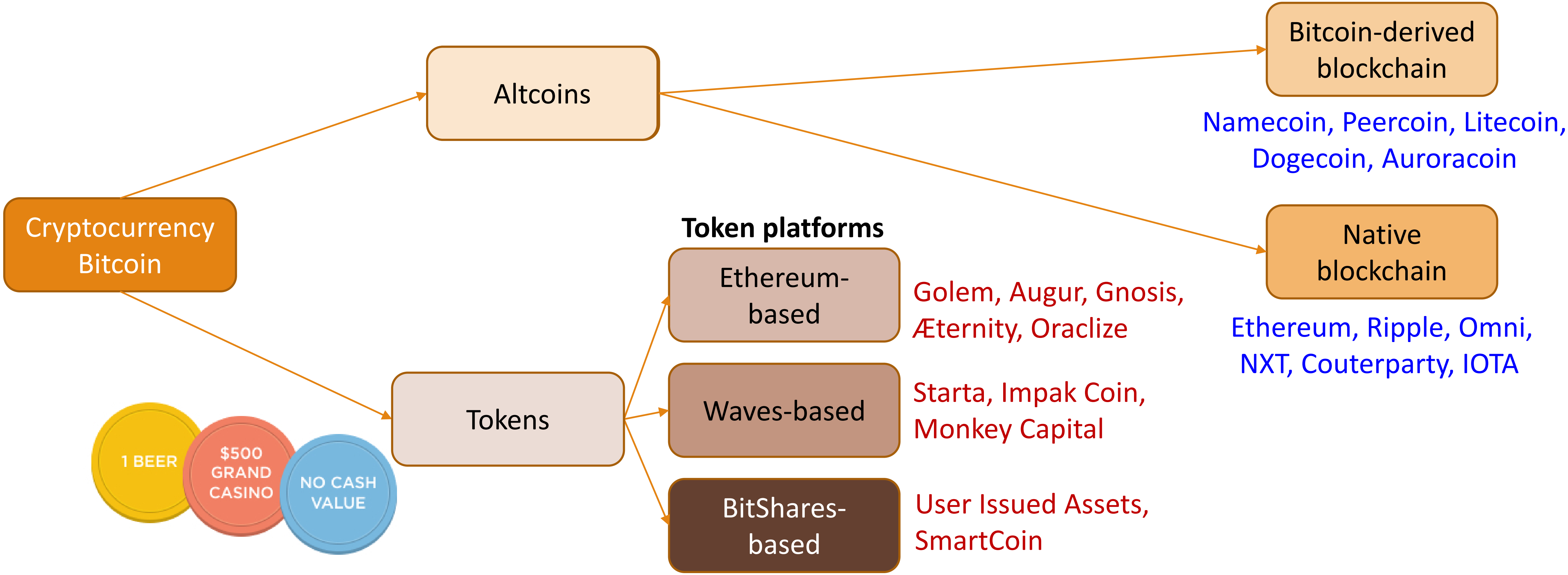
위험하지 않은 종목이 없고,
위험하지 않은 삶이 없다.

https://www.bloomberg.com/

한국은?

- 세계인들에게 한국은 IT강국으로 인식되고 있음
  - 한국인들은 한국이 IT강국이며 선도자임을 인정하기 싫어함
  - 한국인들은 겸손하며 추종자로서 헝그리 정신 DNA를 지니고 있음
- 한국에서 제품이 뜨면 세계에서 뜬다는 믿음이 확산되고 있음
  - 벤치마크 강국
- 한국에서 주요한 암호화폐가 성공하자 암호화폐의 메카처럼 인식
  - 리플의 70%, 카르다노의 80%가 한국에서 거래됨
- 암호화폐 시장을 선도하는 국가로 인식됨
  - 국제적인 영향력 확보

Token vs. Coin



Cryptocurrency Bitcoin

Altcoins

Bitcoin-derived blockchain

Namecoin, Peercoin, Litecoin, Dogecoin, Auroracoin

Native blockchain

Ethereum, Ripple, Omni, NXT, Couterparty, IOTA

Tokens

Token platforms

Ethereum-based

Golem, Augur, Gnosis, Æternity, Oraclize

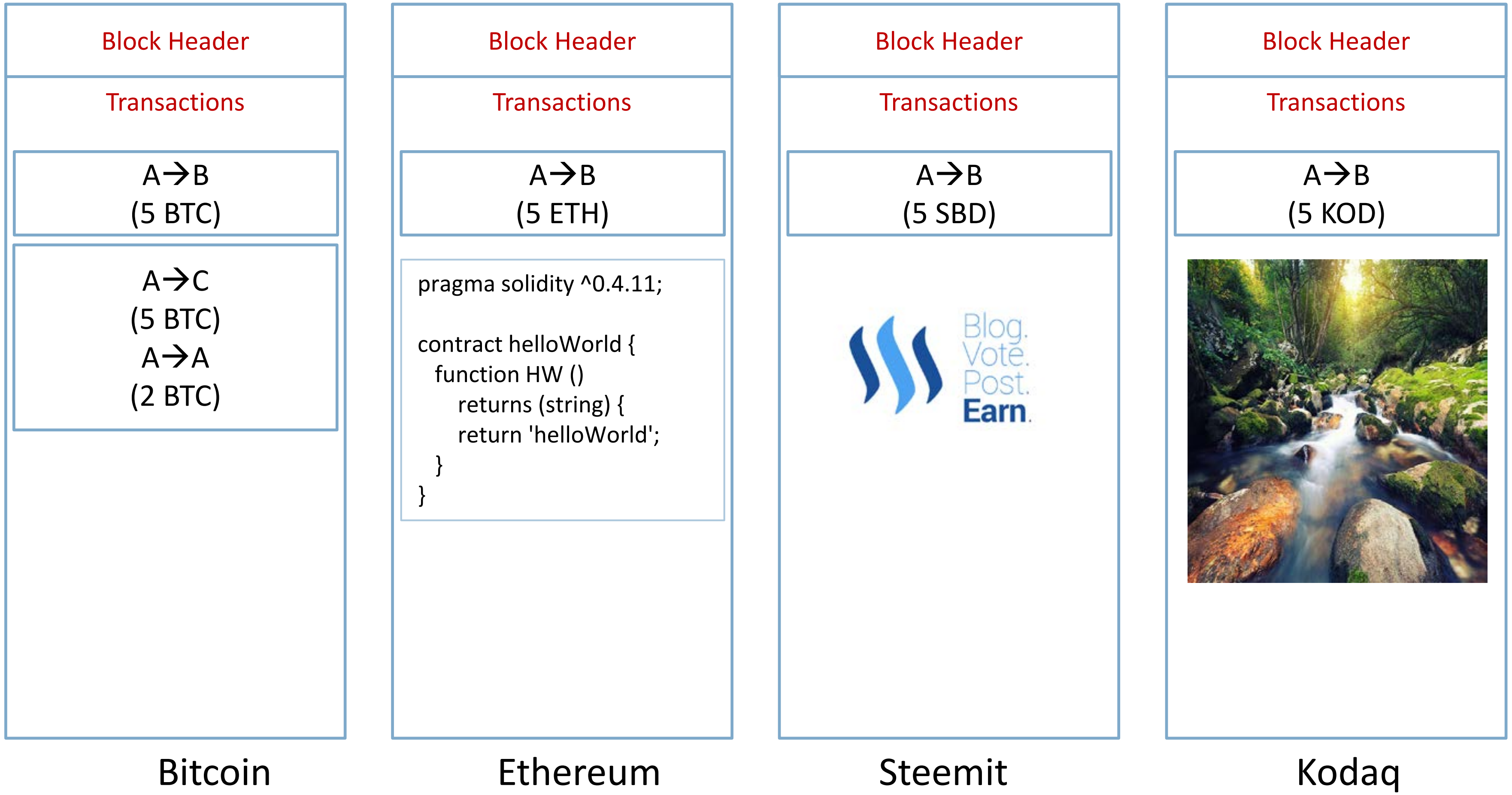
Waves-based

Starta, Impak Coin, Monkey Capital

BitShares-based

User Issued Assets, SmartCoin

Blockchains



Block Header

Transactions

A→B
(5 BTC)

A→C
(5 BTC)
A→A
(2 BTC)

Bitcoin

Block Header

Transactions

A→B
(5 ETH)

```
pragma solidity ^0.4.11;

contract helloWorld {
   function HW ()
       returns (string) {
       return 'helloWorld';
   }
}
```

Ethereum

Block Header

Transactions

A→B
(5 SBD)

Steemit

Block Header

Transactions

A→B
(5 KOD)

Kodaq

Private Blockchain의 한계

- 투명성 (Transparency) 한계
  - 영업비밀, 개인정보 등 공개 가능?
  - 물류, 금융, 의료정보 공유 불가
- 분산 (Distributed) 한계
  - 비효율적
  - 책임지는 주체 없음
  - The DAO (distributed autonomous organization) 교훈
- 물리적 (Physical) 한계
  - 블록체인 데이터는 변조 불가
  - 물리적 실체(돼지고기, 다이아몬드)는 블록체인에 담을 수 없음
- 블록체인만으로 할 수 있는 사례 희귀

베네수엘라 사례

- 2017년 3월 22일: 세계 최초로 정부가 자원을 담보로 가치를 보장하는 암호화폐 페트로(Petro)의 ICO 시작
- 2018년 2월20일부터 3월19일까지 기관을 대상으로 비공개로 진행한 사전판매에서 20만927건의 페트로 구매 이뤄짐 (약 50억2000만 달러 상당의 판매고 달성)
  - 베네수엘라, 미국, 터키, 러시아, 중국 등 133개 국가가 달러(52.7%), 위안(22.59%), 유로(15.9%), 이더리움(7.9%) 등으로 구매
- 사전 판매를 통해 1억 개의 초기 발행 페트로 중 3840만개 판매했고, ICO 기간 동안 4400만개 판매 예정
- 페트로의 판매가격은 전일 베네수엘라 유가 1배럴에 연동

국제동향

- FRB (Federal Reserve Board), BIS (Bank for International Settlements), ECB (European Central Bank), IMF (International Monetary Fund): 중앙은행을 중심으로 가상통화 관련 기술 현황과 통화제도에 미칠 영향에 대해 논의
- 기존의 명목화폐를 보완하는 중앙은행 가상통화(CBCC: Central Bank Cryptocurrency) 혹은 중앙은행 디지 털통화(CBDC: Central Bank Digital Currency)의 발행에 대한 연구 및 실험 진행 (FedCoin vs CADCoin)
- 2018년 6월 15일 서울에서 G20 회원국들을 대상으로 G20 국제금융체제 2차 실무회의 열어 회원국들간 공조를 모색할 예정

일본의 거래소 등록 현황 (2017년 10월)

Exchange operator	Cryptocurrencies handled
Bitbank (중국)	BCH, BTC, ETH, LTC, MONA, XRP
BitFlyer	BCH, BTC, ETC, ETH, LTC
BitPoint	BCH, BTC, ETH, LTC, XRP
BitTrade	BCH, BTC, ETH, LTC, MONA, XRP
BTCBox	BCH, BTC
Fisco Virtual Currency Exchange	BCH, BTC, CICC, FSCC, MONA, NCXC
GMO Coin	BTC
Money Partners	BTC
Quoin	BCH, BTC, ETH
SBI Virtual Currencies	BTC
Tech Bureau	BCH, BCY, BTC, CICC, FSCC, MONA, NCXC, PEPECASH, SCJX, XCP, XEM, ZAIF, ZEN

일본의 거래소 등록 현황 (2017년 12월 이후)

- 2017년 12월 Tokyo Bitcoin Exchange, Bit Arg Exchange Tokyo, FTT Corporation, Xtheta Corporation, Bitocean 등 추가 등록 허용으로 16개 거래소 등록
- Minnano Bitcoin, Payward Japan, Lemuria Bitcoin Exchange (Bitcrements), Campfire Corporation, Tokyo Gateway, Lastroots Corporation, Debit, Eternal Link, FSHO Corporation, Raimu, Bit Station, Blue Dream Japan, Mr. Exchange, Bmex Corporation, Bitexpress Corporation, Coincheck 등 16개 업체 등록 대기
- 2018년 1월 Coincheck 해킹 이후 4월 Eternal Link, FSHO Corporation에게 2개월 영업정지 명령

Smart Contracts

- 프로그래밍(smart) 기능 + 계약(contract) 기능
- 제3자 없이 신뢰할 수 있는 계약 수행
- 계약 수행은 추적 가능하고 비가역적
- Turing completeness가 장점이자 약점
- smart contract secure coding 등 보완책 시급

스마트 컨트랙트

- The DAO 해킹: 2016년 6월 243만 ETH 탈취 (Contract Bug)
- Parity Wallet Hacking: 2017년 9월 15만 ETH 도난 (initWallet function call)
  - 모든 함수들을 callable로 변경
- Parity Wallet Bug: 2017월 11월 50만 ETH 잠김

- 얼마나 많은 bug가 존재할 지 몰라

병아리 감별사?

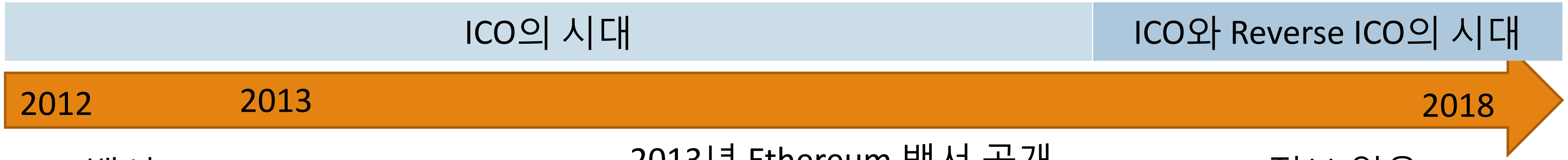
- 암호화폐/토큰 감별사
  - 2,000종이 넘는 암호화폐와 토큰
  - 매년 수천 종, 새로 출현
  - 쓰레기와 순금을 가려내는 전문직업
- 고도의 암호이론, 컴퓨터공학, 소프트웨어공학 등 진문지식 필요
- 경제학, 사회학, 경영학 등 경제상품에 대한 전문지식 필요

- 글로벌코인평가 Global Coin Ratings (공정한 코인평가 시급)

ICO란

	IPO	ICO
참여자	투자자(investors) 주로 법정화폐와 주식 교환	지지자(supporters) 주로 (비트코인, 이더)와 (코인, 토큰) 교환
공모시점	민간기업이 상당 기간 기업을 운영한 후 IPO 실시	개념증명이 되지 않은 백서를 가지고 신생 기업이 종자자본을 마련하려고 ICO 실시
배당	영업이익에서 배당금 지급	배당금 없음 (상승 예상되는 암호화폐 가격이 배당금에 해당)
규제	주식을 발행하기 전 해당 국가의 규제 기관에 공모신청	국경 없는 분산플랫폼에서 스타트업이 ICO 실시 (KYC, AML 등 규제 적용 추세)
통제와 관리	중앙집중식 조직에서 잘 작동	중앙집중식 조직 없는 오픈 소스 프로젝트에서 잘 작동
이익 배분	주주끼리 이익 공유	개발자, 투자자, 참여자가 고루 이익을 공유하는 **이익공유경제 모델**

ICO 이정표



Mastercoin 백서 공개 (1월)

ICO 개시 (7월부터 1개월)
500여명이 5000 BTC 제공

2013년 Ethereum 백서 공개
2014년 ICO 실시
2015년 Ether 발행

ICO 정보 없음
8억5천만달러 모금 소문

J.R. Willett, Mastercoin (지금의 Omni), ICO의 창안자

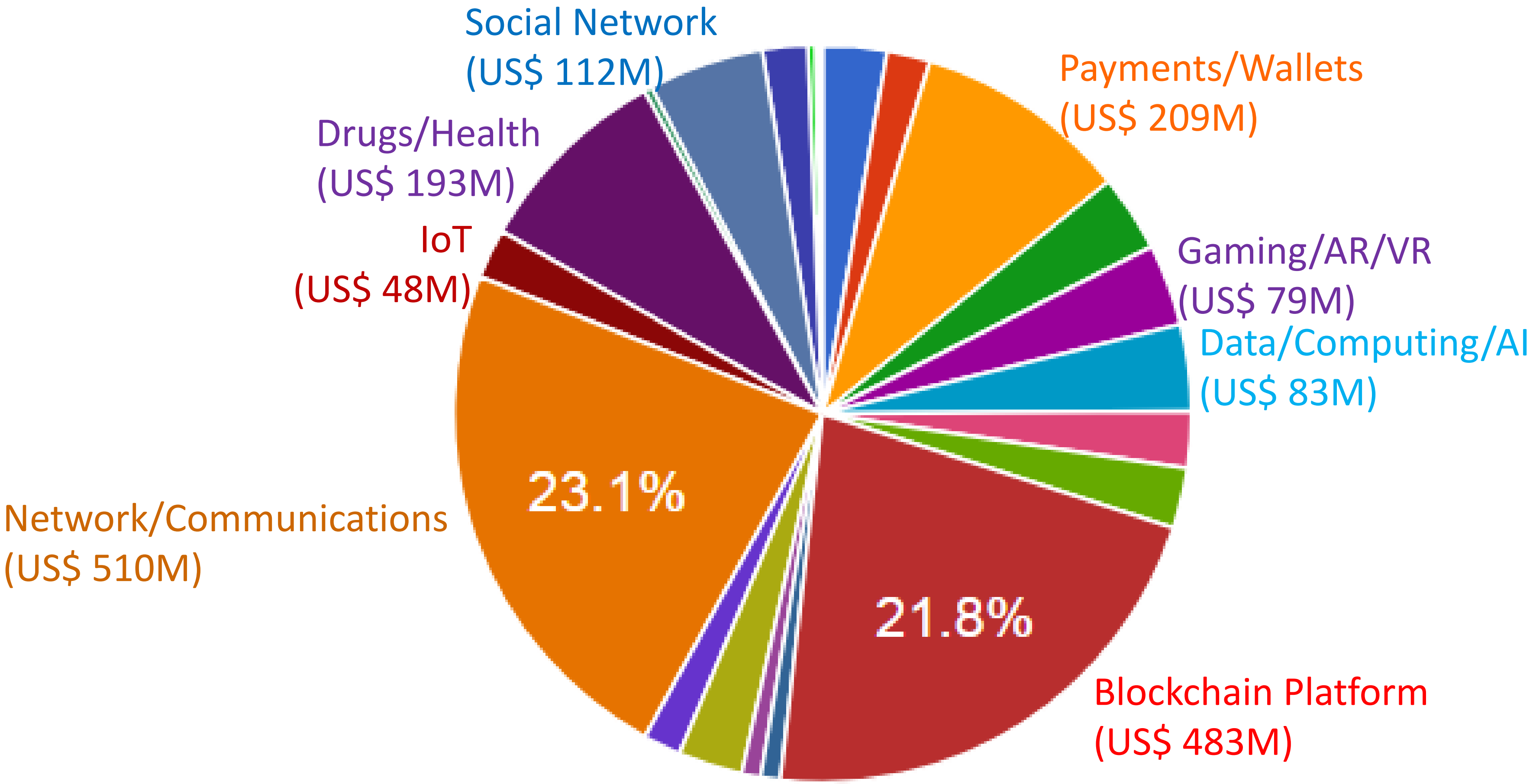
Vitalik Buterin

Pavel Durov, Telegram 창업자, GRAM ICO

ICO 동향

- 2013년 Mastercoin이 최초의 ICO
- 2014년 Ethereum이 12시간 만에 3,700 BTC를 모음 (당시 시가 $2.3M)
- 2017년 8월까지 최소 400여 개의 ICO 진행
- SEC, ICO 토큰의 증권 여부 판별법 제시 (Howey 테스트)
  1. 자본의 투자(investment of money)
  2. 공동의 사업체(common enterprise)
  3. 타인의 노력에 의한 수익의 기대(expectation of profit, primarily from the efforts of others)
- 암호화폐 공모에서 일반 상품 공모로 확산
  - 2017년 5월, 인터넷 브라우저 Brave (30초만에 $35M 공모)
  - 2017년 9월, 메신저 앱 Kik (168,732 ETH 공모)

산업별 ICO 현황



https://icowatchlist.com/statistics/categories

ICO의 변신

- IPO와 ICO의 경계 허물다 (**Reverse ICO**)

- Omise (2013년 창업, 2017년 ICO **OmiseGo**) Payment gateway
- Kik Interactive (2009년 창업, 2017년 ICO **Kin**) Messenger
- PlayKey (2103년 창업, 2017년 ICO **PlayKey Token**) Cloud gaming
- OPSkins (2015년 창업, 2017년 ICO **Wax**) Online marketplace
- Telegram (2013년 출범, 2018년 ICO **GRAM**) Social networking
  - Kik, YouNow, Telegram의 비교 (https://hackernoon.com/considering-the-telegram-ico-proceed-with-caution-92c178e2a178)
- reverse ICO에 대해 어떤 태도를 취해야 하나?
  - 신선한 아이디어의 산실이 될 수 있을까?

승자독식 공유경제

- 구매자와 판매자를 이어주는 marketplace
- 자산의 부분 사용으로 전세계 사람들이 재정적 이익을 위해 잉여재고, 시간 및 기술을 교환
- Death Star 플랫폼 (플랫폼 자체의 힘 또는 부에 집중하는 기업으로 참여자들에게 힘과 부를 재분배하지 않는 기업)

ICO 성공 요인

Team

Qualified, well rounded and capable team

자격을 갖춘 원숙하고 유능한 팀

Use Case

Solves a problem, has a clear purpose and real application

문제를 풀고, 분명한 목적과 실제 응용사례를 보유

Business Model

Sustainable and scalable business model

지속 가능하고 확장 가능한 비즈니스 모델

Institutional Mindset

Looking at building a long term institutional grade business

장기적인 기관 수준의 사업을 추구

자료: PWC

ICO에서 주목할 점

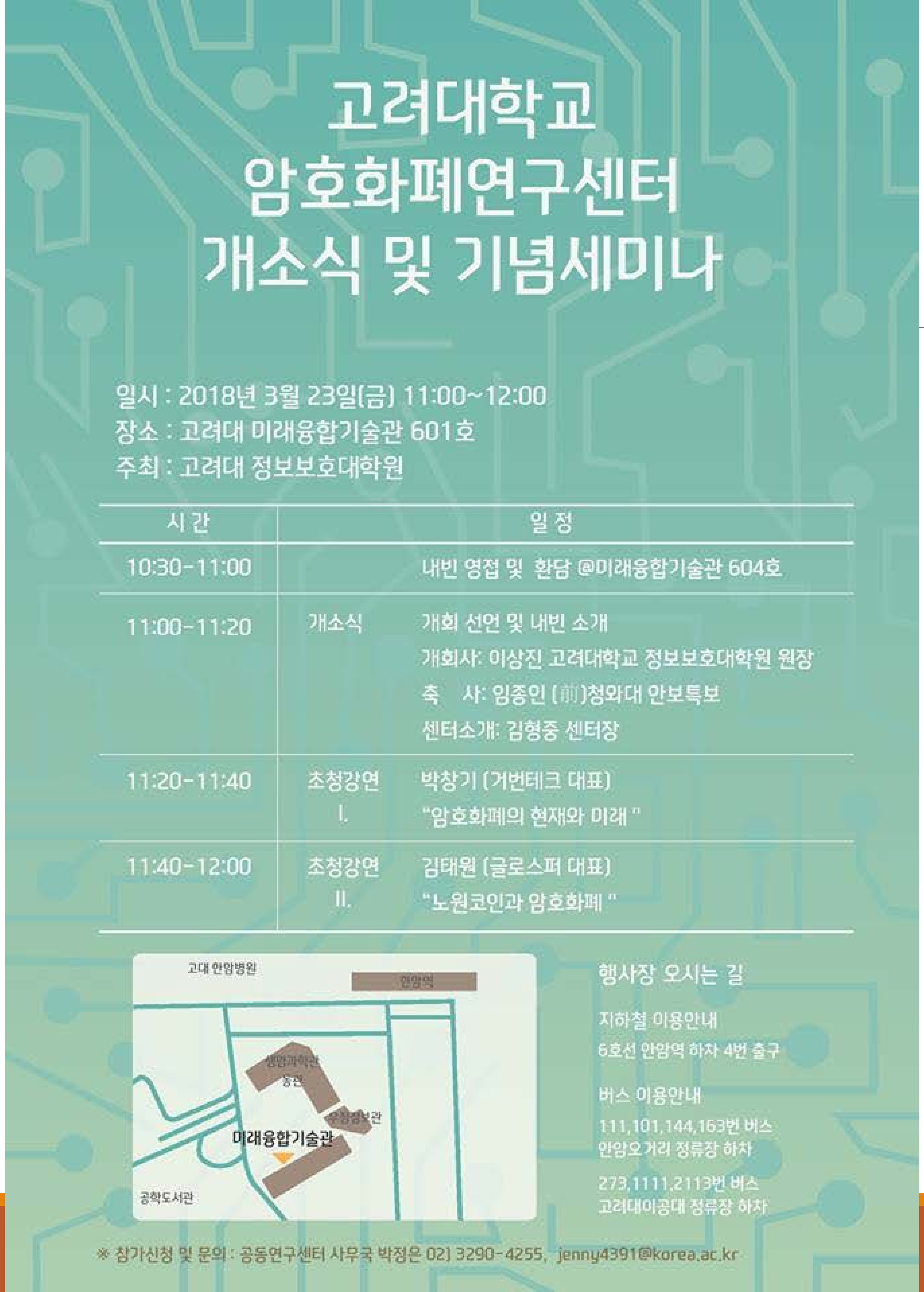
- ICO는 공공재로서의 블록체인을 구현하고 있는가?
- ICO가 산업발전에 기여하고 있는가?
- 백서는 적정한 비즈니스 모델과 구현 가능한 기술을 담고 있는가?
- 코인/토큰판매 절차는 적법한가?
- 백서의 계획대로 기술이 구현되고 코인/토큰이 안정된 가격을 유지하는가?

거래소에서 주목할 점

- 거래소와 증권거래소의 차이점에 대한 명확한 이해 필요
- 거래소의 보안수준이 적절히 유지되고 있는가?
- 거래소 파산에 대한 준비가 되어 있는가?
- 거래소 상장 또는 상장폐지가 적절한 절차에 따라 이루어지고 있는가?
- 거래서 내부에서 장부거래, 차익거래 등 도덕적 해이 현상이 벌어지고 있지 않은가?

결어

- 암호화폐에 대한 정확한 정의 필요
- 암호화폐 관련 입법 시기에 대한 논의 필요
- 암호화폐 개발과 운용에 필요한 인력과 기술 점검



고려대학교 암호화폐연구센터 개소식 및 기념세미나

일시 : 2018년 3월 23일(금) 11:00~12:00
장소 : 고려대 미래융합기술관 601호
주최 : 고려대 정보보호대학원

시 간	일 정	
10:30-11:00		내빈 영접 및 환담 @미래융합기술관 604호
11:00-11:20	개소식	개회 선언 및 내빈 소개 개회사: 이상진 고려대학교 정보보호대학원 원장 축 사: 임종인 (前)청와대 안보특보 센터소개: 김형중 센터장
11:20-11:40	초청강연 I.	박창기 (거번테크 대표) "암호화폐의 현재와 미래 "
11:40-12:00	초청강연 II.	김태원 (글로스퍼 대표) "노원코인과 암호화폐 "

행사장 오시는 길

지하철 이용안내
6호선 안암역 하차 4번 출구

버스 이용안내
111,101,144,163번 버스
안암오거리 정류장 하차

273,1111,2113번 버스
고려대이공대 정류장 하차

※ 참가신청 및 문의 : 공동연구센터 사무국 박정은 02) 3290-4255, jenny4391@korea.ac.kr

고려대 블록체인공학과

- 석사/박사과정
- 금요일 오후, 토요일 오전-오후 강의
- 기업이 등록금의 50% 이상 지원
- 기술, 기획, 정책

대한전자공학회 통신소사이어티 워크샵 : 블록체인으로 여는 미래

블록체인 기반 IoT 플랫폼 개발 동향

이 두 원 / CEO, Ph.D
doowon.lee@gmail.com

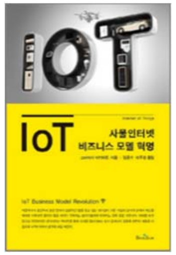
버전 1.0, 2018. 4

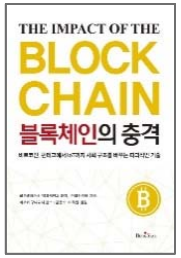
이 두 원

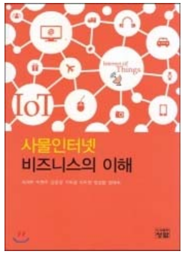
- ㈜아니스트 대표이사 / 공학박사, 신지식인
- 전, 국립 부산대학교 교수
- 전, LG히다찌㈜ 상무
- 주요분야 : IoT, SCM, 핀테크, 블록체인

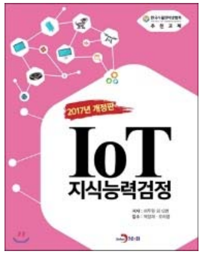
▨ 블록체인 기술 기획 및 자문

- 대통령준비위원회 집단지성센터 블록체인기술위원회 위원
- 4차산업혁명 대응 추진위원 (한국정보통신공사협회)
- 한국블록체인학회 운영위원
- 블록체인미래과제 전문자문위원 (국가보안기술연구소, 2017 ~ 현재)
- ICT R&D 중장기 계획 수립 블록체인 담당 기획위원 (2016 ~ 현재)
- 2017. 블록체인의 충격(북스타)









대한전자공학회 통신소사이어티 워크샵
: 블록체인으로 여는 미래

블록체인 기반
IoT 플랫폼 개발 동향

Ⅰ. 블록체인 개념 정리

- 4차 산업혁명의 특징
- 블록체인 개념 이해
- 블록체인 기술 개요 및 특징
- 표준화 및 대응 기구

Ⅱ. IoT 블록체인

- IoT 블록체인 개요
- 블록체인 융합 기대효과와 한계점
- 블록체인의 IoT 적용

Ⅲ. IoT 블록체인 플랫폼 동향

- 주요 IoT 블록체인 플랫폼 동향
- 신규 IoT 블록체인 플랫폼 개발동향

Ⅳ. IoT 블록체인 USE CASE

Ⅴ. IoT 블록체인 플랫폼 전망

Warming-up

블록체인 개념 정리

4차 산업혁명의 특징

첫째, 초 연결성

- 4차 산업혁명은 정보의 공유 방식과 대상에 경계가 사라짐

둘째, 기기의 지능화

- 기기들이 서로 네트워크로 정보를 공유, 상황에 맞게 좀 더 지능적인 결정을 내릴 수 있게 됨
- 기기들의 정보공유로 인해서 장치가 가지고 있는 정보들만을 활용 하는 게 아니라 주위의 여러 기기들과 정보공유로 얻어서 더 합리적인 결정을 내리게 됨

셋째, 인공지능

- 사고가 필요로 하는 고도의 업무에 인공지능 적용 (예, 자율주행 자동차)

넷째, 맞춤형 서비스

- 자동화가 가능해지면서 서비스의 개인 맞춤화가 가능하게 됨
- 사물이 개인들의 사용 패턴 정보를 수집하고 스스로 분석해 서비스 제공 가능

다섯째, 효율성

- 사용자에게 능동형 정보를 제공함으로서, 사용자는 좀 더 합리적인 의사결정을 할 수 있게 됨
- 사물이 스스로 학습하고 판단하는 자동화 과정 또한 효율성을 향상시키는 역할을 함

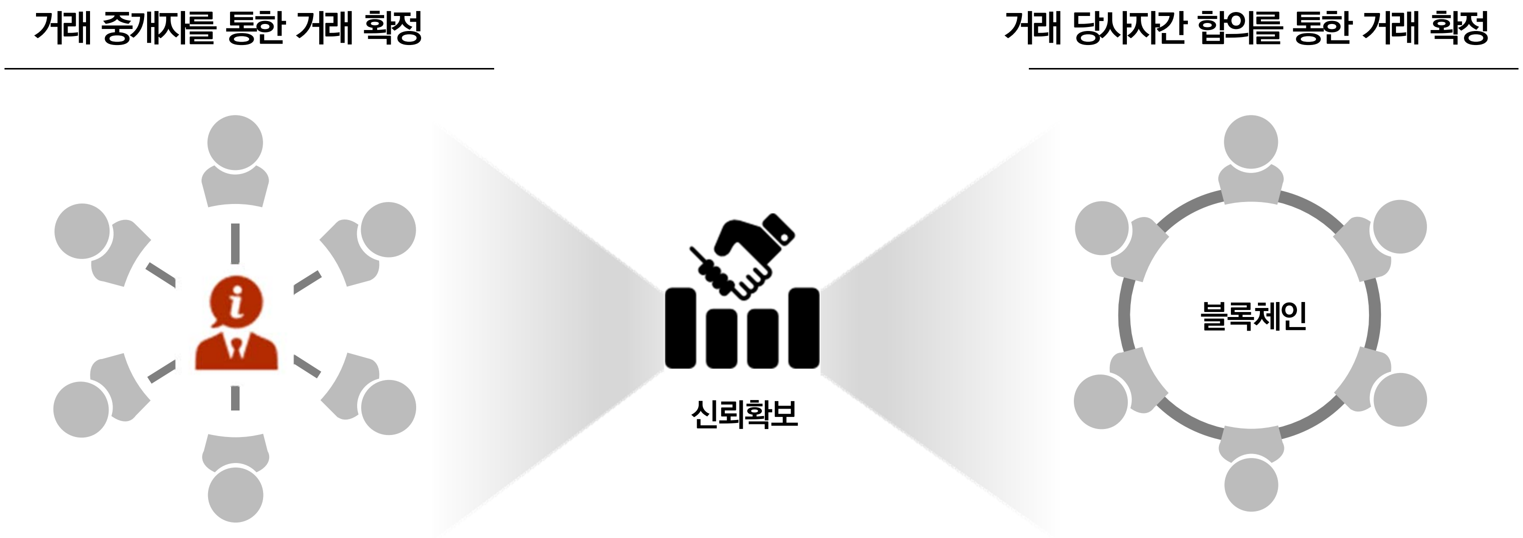
기존의 문제점과 블록체인을 통한 해결방안

기존 문제점 (ICBM)	해결방안 (블록체인)
낮은 보안성	- 분산형 원장 기술로, 해킹에 대해서 참여자끼리 서로 보안 - (비트코인) 공개키 암호화로 중간자 공격 방지
사생활 침해	- 공개키와 개인키로 본인으로만 증명하기 때문에 사생활 침해 이슈 없음
정보 독점	- 모든 정보는 중간 관리자 없이 익명으로 공유되어, 정보 독점 현상이 나타나기 어려움
높은 운영비용	- 중앙센터가 없어 센터에서 부담해야 할 운영 비용이 발생하지 않음

블록체인이란?

분산원장(Distributed Ledger) 기술은 거래정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P(Peer-to-Peer)네트워크에 분산하여 네트워크 참여자가 생산하는 정보 및 가치를 **공동으로 기록하고 관리하는 분산화된 공개 장부 관리 기술**을 의미함 (한국은행, 2016)

"중개자 없이 당사자 간 거래를 안전하게 처리하는 기술"


거래 중개자를 통한 거래 확정
거래 당사자간 합의를 통한 거래 확정
신뢰확보
블록체인

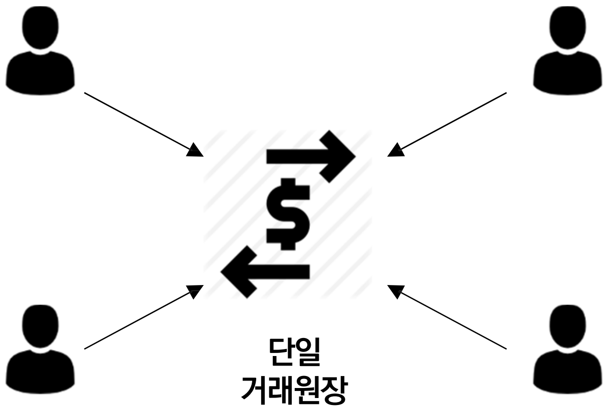
- 신뢰 보장의 대가로 고비용 발생
- 거래의 완료까지 시간 소요
- 거래 중개자의 신뢰성 중요

- 상대적 저비용으로 신뢰 확보
- 거래 완료까지 시간 단축

블록체인의 원리 (1/3) - 거래 내역의 보관

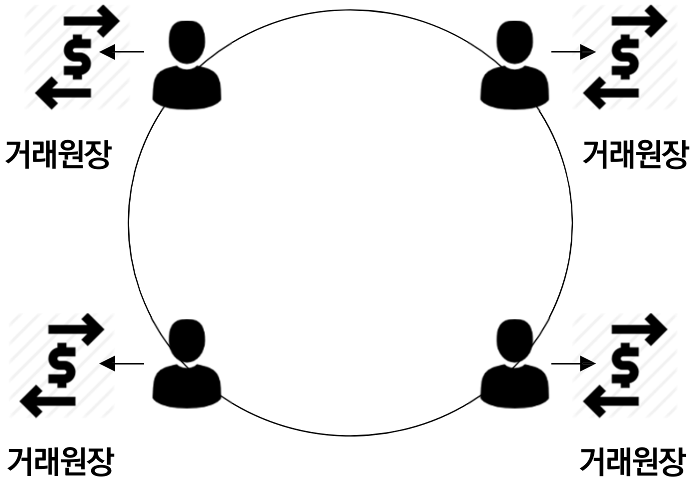
“거래 내역을 공개하여 거래 참여자가 공동으로 저장 ”

한곳에서 폐쇄적으로 보관



- 거래 내역을 기관 내부에서 안전하게 보관
- 이전 거래 기록에 기반하여 신규 거래 수행

거래 당사자 간 공동 보관

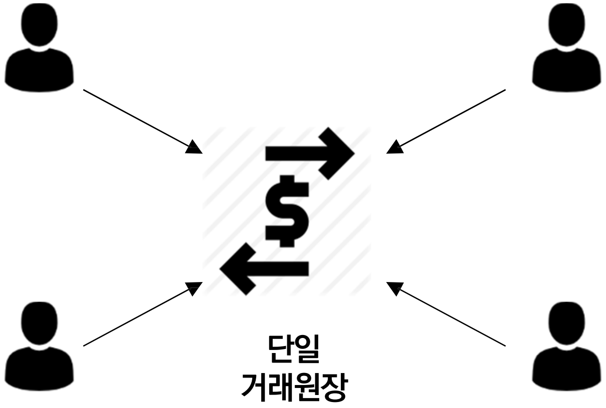


- 거래내역을 참여자가 공동으로 공개하여 보관
- 이전 거래 기록에 기반하여 신규 거래 검증

블록체인의 원리 (2/3) - 거래 내역에 대한 합의

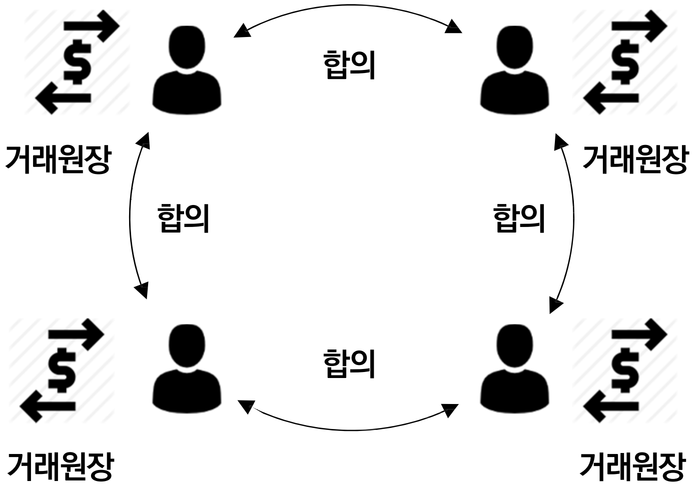
"합의를 통해 공동 보관하는 거래내역을 동일하게 유지 "

단일 거래 원장 유지



- 하나의 거래원장을 유지
- 별도의 합의 절차 필요 없음

합의를 통해 동일한 원장 유지

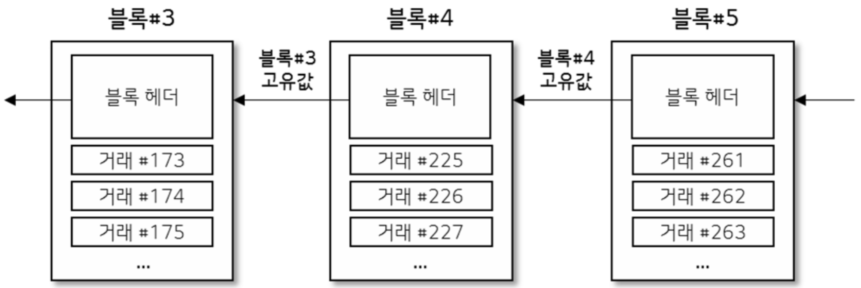


- 다수의 기록을 동일하게 유지하기 위해 합의 필요
- 더 많은 수의 참여자가 인정하는 결과를 선택 (다양한 알고리즘 존재)

블록체인의 원리 (3/3) - 거래 기록의 위변조 방지

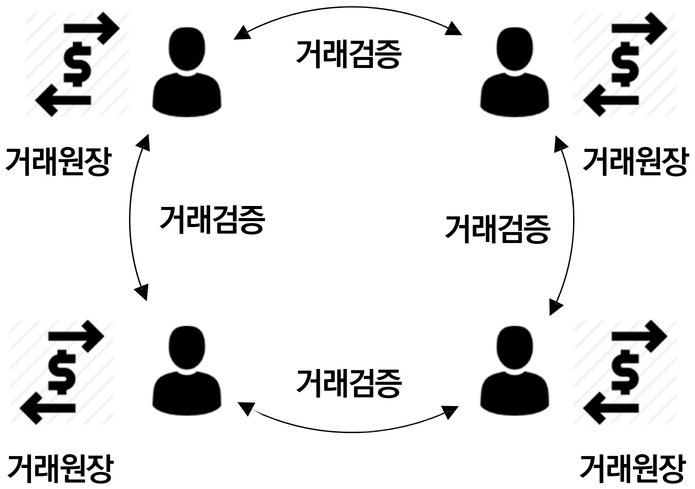
"합의된 거래결과의 임의적 변경 방지 "

개별 참여자에서의 위변조



- 블록이 체인으로 연결, 거래 전체에 대한 무결성 검증 수행
- 단일 블록만의 변경으로는 손쉽게 위변조 탐지 가능

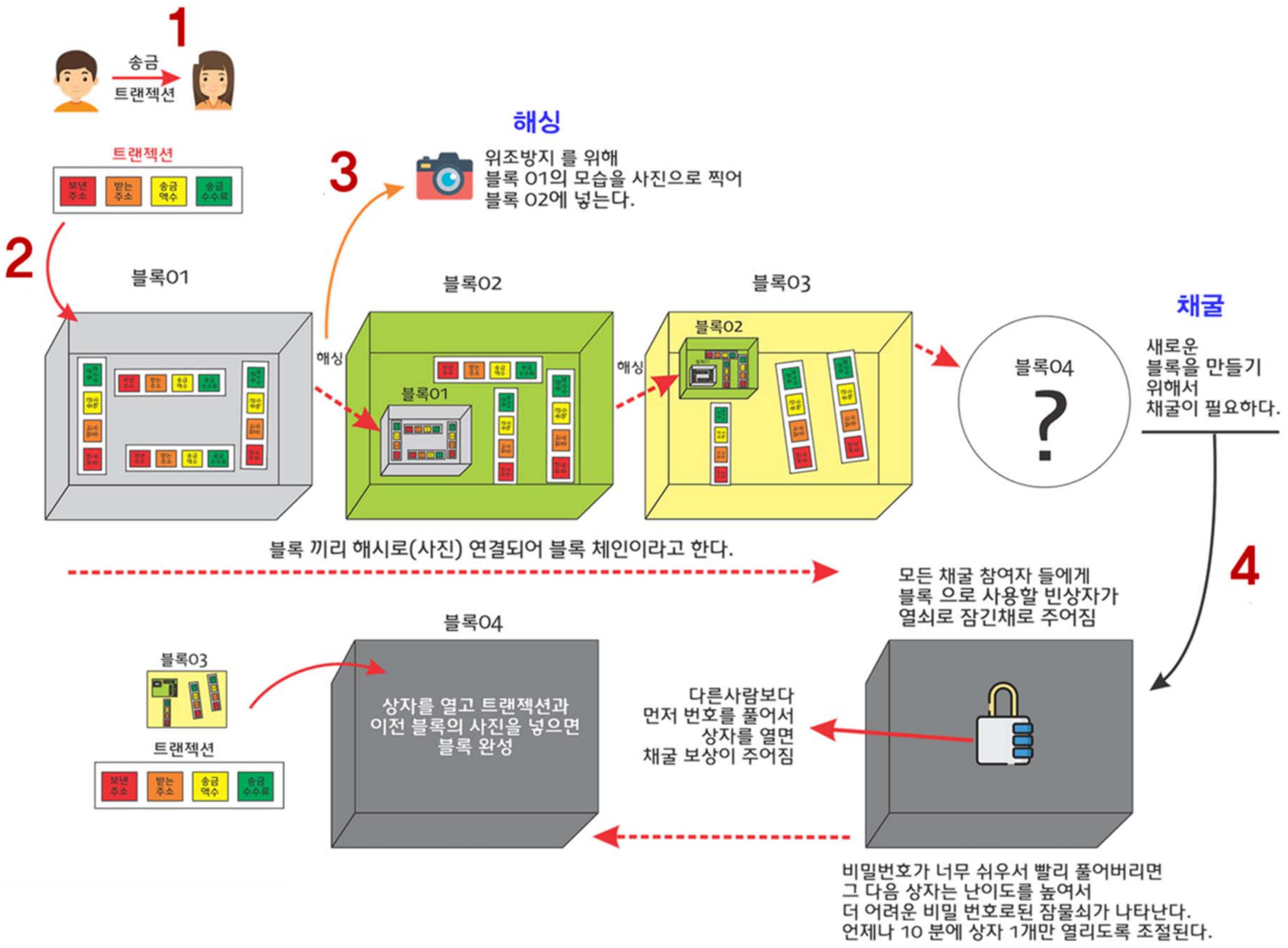
전체 네트워크에서의 위변조



- 전체 참여자에 대한 위변조 필요
- 현실적으로 불가능

블록체인은 …

- An append-only system of record or log of transactions.
  - 블록체인은 계약(promises), 거래(trades), 트랜잭션 등의 영구데이터를 기록하기 위해서 사용될 수 있음
  - 특정 네트워크 상에서 미러링되고, 누구나 해당 네트워크에 참여할 수 있도록 함
  - 분산원장은 중앙 신뢰 인증자가 없는 다자간 데이터베이스
  - 블록체인의 순서 보장을 통해서 트랜잭션이 처리되는 분산원장을 의미함



위조방지 를 위해
블록 01의 모습을 사진으로 찍어
블록 02에 넣는다.

새로운
블록을 만들기
위해서
채굴이 필요하다.

블록 끼리 해시로(사진) 연결되어 블록 체인이라고 한다.

모든 채굴 참여자 들에게
블록 으로 사용할 빈상자가
열쇠로 잠긴채로 주어짐

상자를 열고 트랜젝션과
이전 블록의 사진을 넣으면
블록 완성

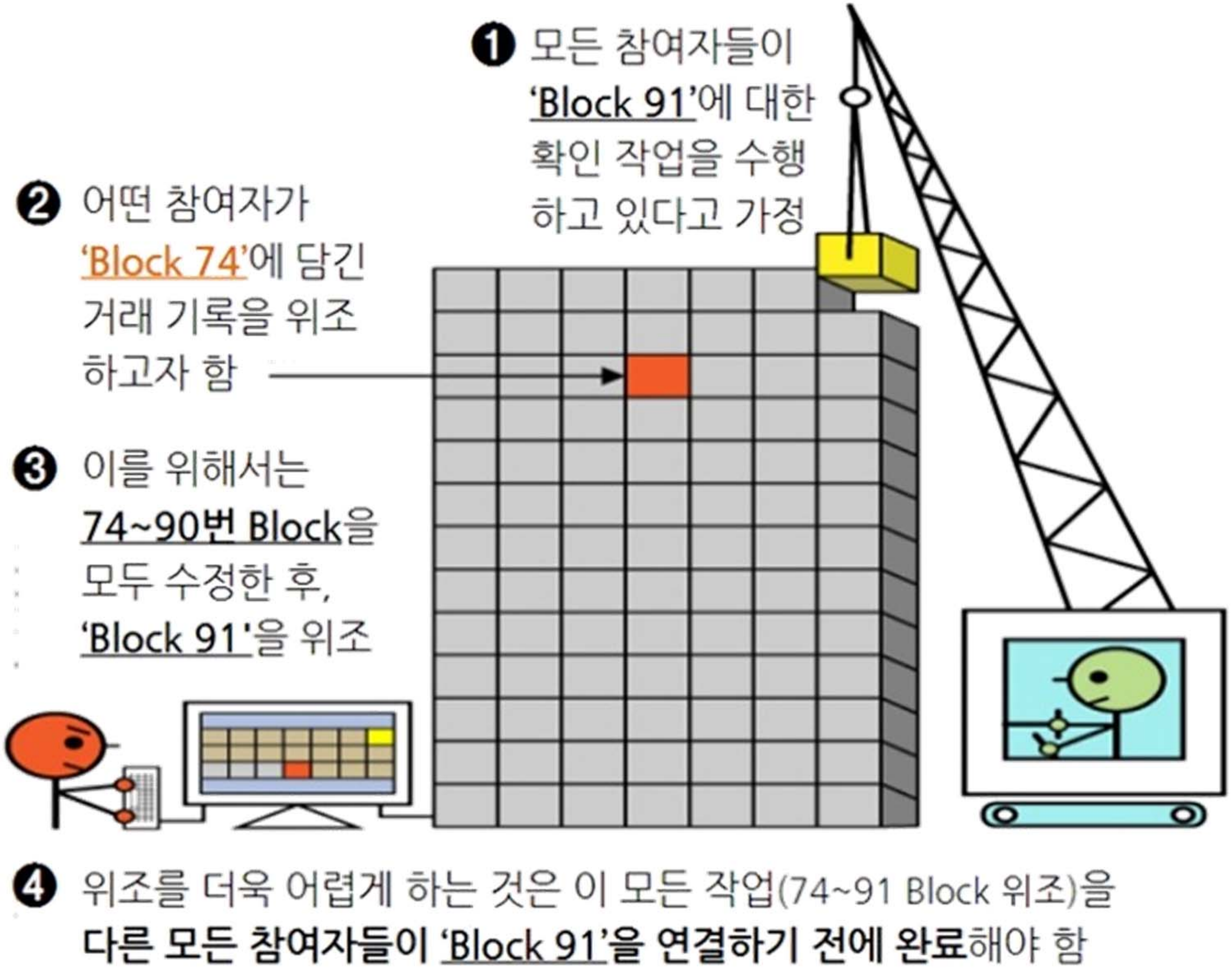
다른사람보다
먼저 번호를 풀어서
상자를 열면
채굴 보상이 주어짐

비밀번호가 너무 쉬워서 빨리 풀어버리면
그 다음 상자는 난이도를 높여서
더 어려운 비밀 번호로된 잠물쇠가 나타난다.
언제나 10 분에 상자 1개만 열리도록 조절된다.

※ 채굴이라는 것은 새로운 상자속에 트랜잭션 데이터를 기록하고 해시데이터를 기록하는 것

https://steemkr.com/kr/@tintom/2fgvq8

블록체인의 해킹이 어려운 이유



❶ 모든 참여자들이 'Block 91'에 대한 확인 작업을 수행하고 있다고 가정

❷ 어떤 참여자가 'Block 74'에 담긴 거래 기록을 위조하고자 함

❸ 이를 위해서는 74~90번 Block을 모두 수정한 후, 'Block 91'을 위조

❹ 위조를 더욱 어렵게 하는 것은 이 모든 작업(74~91 Block 위조)을 **다른 모든 참여자들이 'Block 91'을 연결하기 전에 완료**해야 함

[자료] IEEE Spectrum (2015.7)

비트코인 채굴

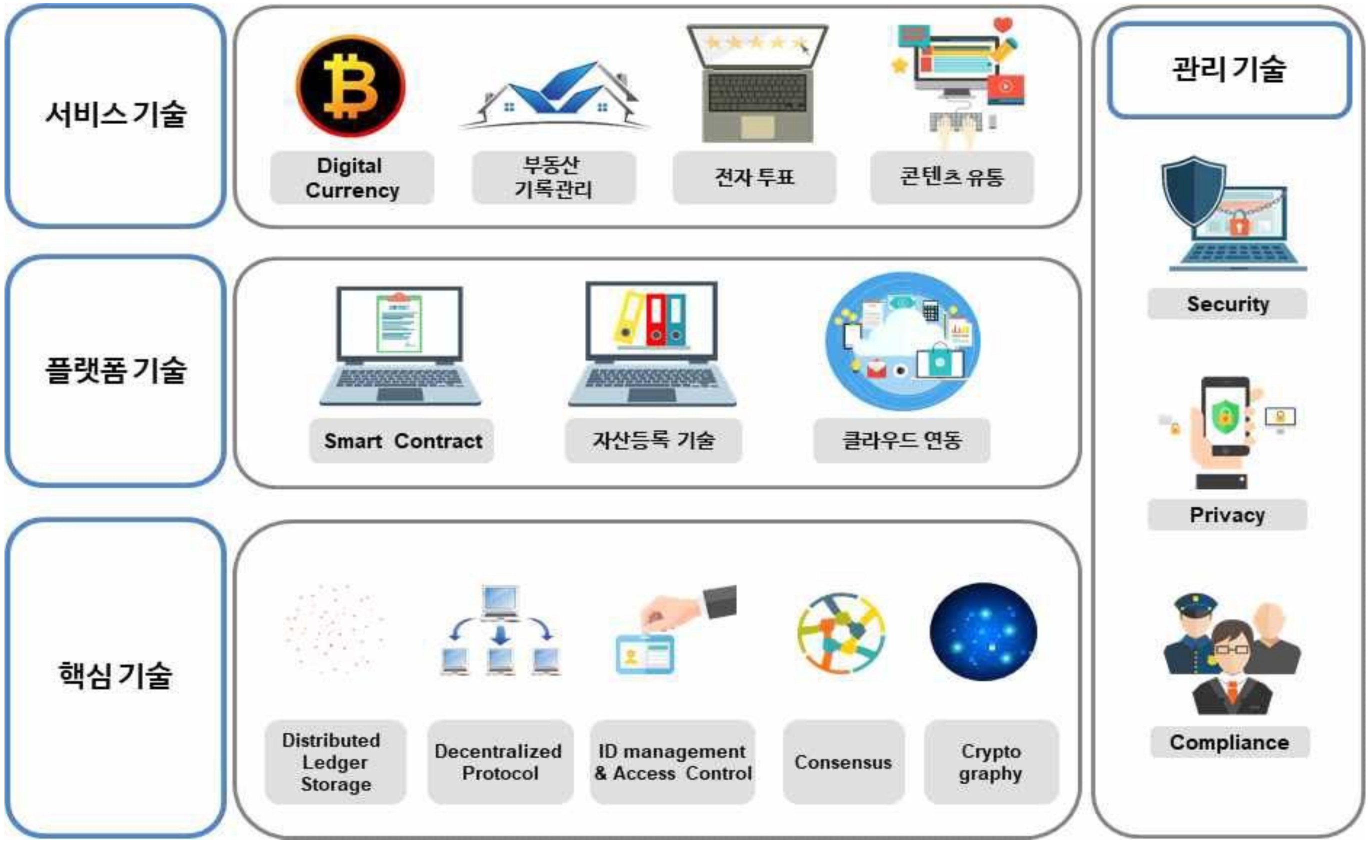
- 채굴(Mining)은 블록헤더 Hash값이 난이도 목표에 제시된 값보다 작은 값이 나오게 하는 Nonce값 찾는 과정
- 채굴 노드가 다음 블록을 찾는 데 1초당 **50경 회 이상의** Hash 계산이 평균적으로 필요함 ⇒ 채굴의 기업화

중국 채굴 공장 : 월 16억원을 버는 중국인 초기에 빨리 시작해서 현재 자산 수백억 수준 한 달에 전기세로만 9,000만원이 나간다고 함

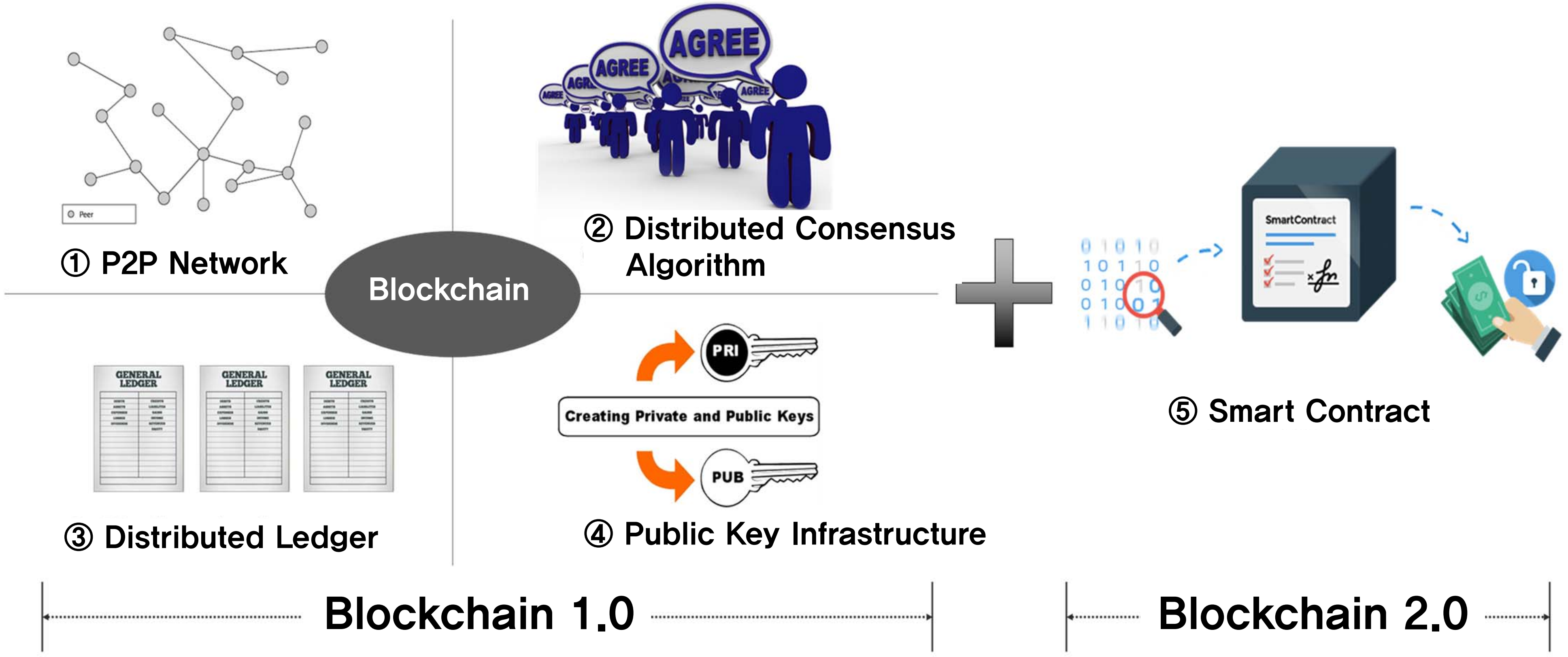
블록체인 기술 개요

블록체인 기술은 크게 핵심기술, 플랫폼 기술, 서비스 기술 및 관리기술로 분류됨

- 핵심 기술은 Distributed Ledger Storage, Decentralized Protocol, ID Management and access control, Consensus, Cryptography, 등의 요소기술로 구성된 블록체인 핵심 기술
- 플랫폼 기술은 Smart Contract, 자산 등록기술, 클라우드 연동 등의 기술
- 서비스기술은 Digital Currency, 부동산 기록관리, 전자투표 및 콘텐츠 유통 등 서비스 기술
- 관리기술은 Security, Privacy, Compliance 기술



블록체인의 4가지 핵심 기술



① P2P Network

Blockchain

② Distributed Consensus Algorithm

③ Distributed Ledger

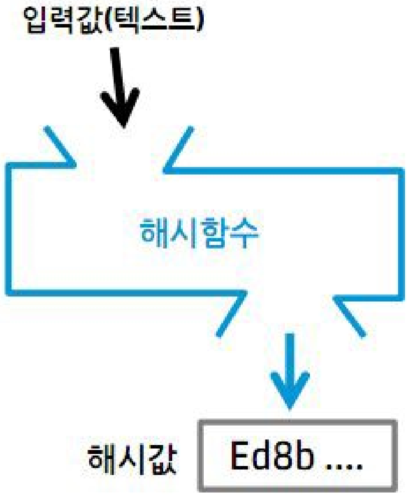
④ Public Key Infrastructure

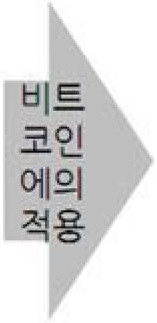
⑤ Smart Contract

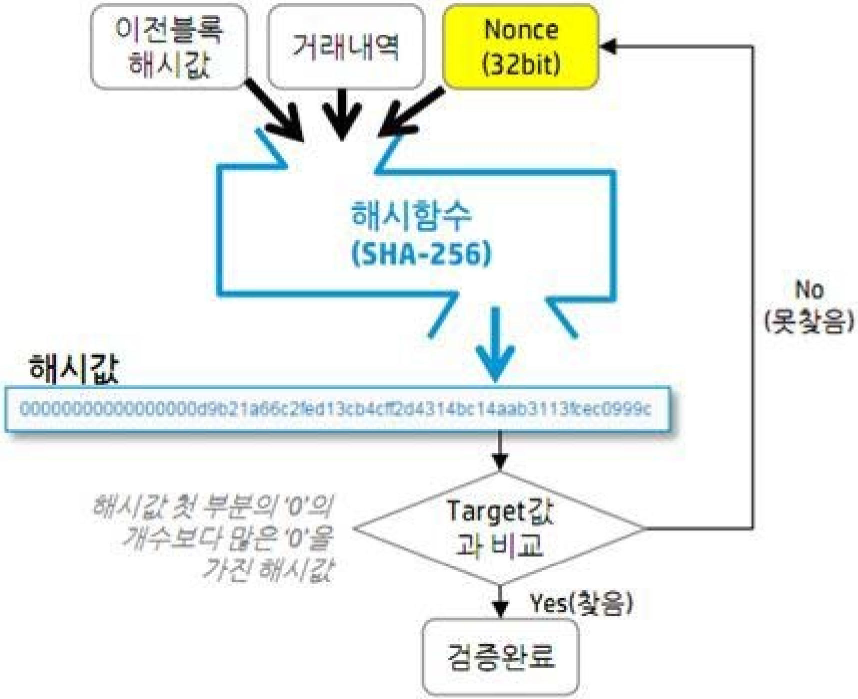
Blockchain 1.0

Blockchain 2.0

해시함수의 역할

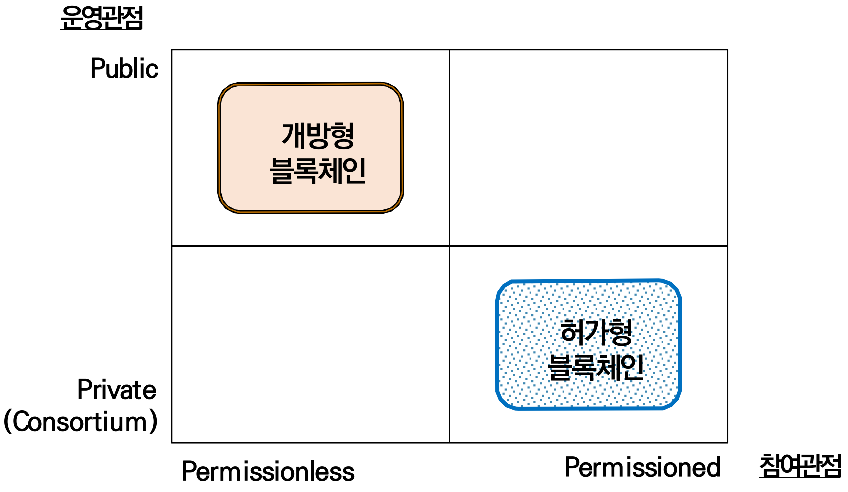






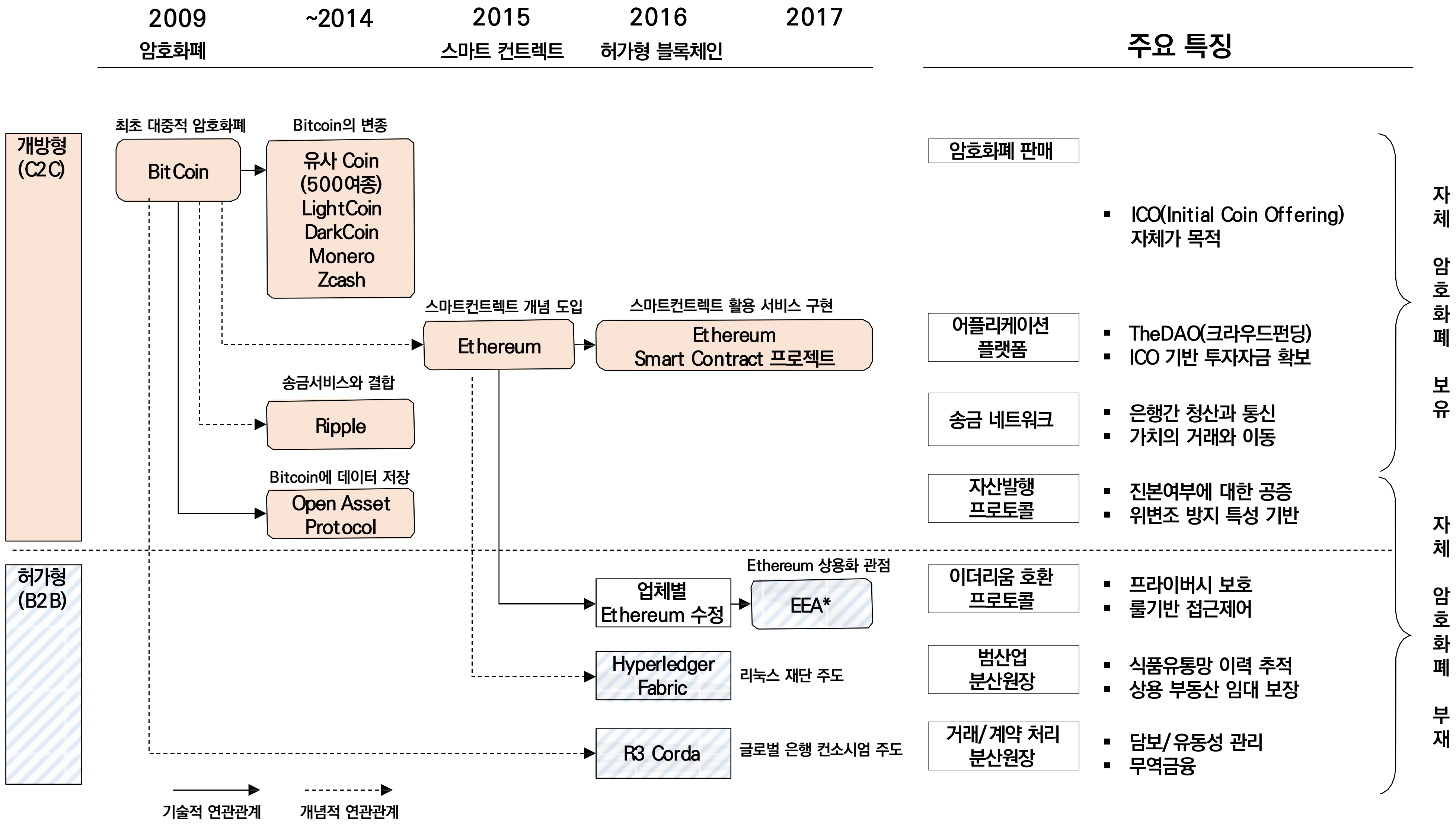
- 같은 입력값 → 같은 해시값 출력
- 해시값에서 입력값 역추적은 불가능

블록체인 유형별 특징



	개방형 블록체인	허가형 블록체인
특징	· 네트워크에 자유로운 참여 가능 · 암호화폐에 기반한 네트워크 규모 유지 · 모든 거래를 공유, 안정적인 거래 처리에 집중	· 네트워크에 참여하기 위해서는 승인 필요 · 암호화폐 부재, 필요시 스마트컨트렉트로 구현 · 신속한 거래 처리, 확장성, 프라이버시 중심
적용 영역	· 중개자가 배제된 순수한 탈중항형 거래 처리 · 일반대중, IoT디바이스 등 불특정 참여자간 서비스 · 암호화폐와 결합된 혁신적 서비스 지형	· 중재자의 역할 최소화 및 효율화된 거래 처리 · 기업/기관 등 참여자를 사전에 특정할 수 있는 서비스 · B2B 거래 처리의 인프라 관점에서 접근

블록체인 기술 변화



2009 암호화폐

~2014

2015 스마트 컨트렉트

2016 허가형 블록체인

2017

개방형 (C2C)

최초 대중적 암호화폐: BitCoin

Bitcoin의 변종: 유사 Coin (500여종) LightCoin DarkCoin Monero Zcash

스마트컨트렉트 개념 도입: Ethereum

스마트컨트렉트 활용 서비스 구현: Ethereum Smart Contract 프로젝트

송금서비스와 결합: Ripple

Bitcoin에 데이터 저장: Open Asset Protocol

허가형 (B2B)

업체별 Ethereum 수정

Ethereum 상용화 관점: EEA*

Hyperledger Fabric: 리눅스 재단 주도

R3 Corda: 글로벌 은행 컨소시엄 주도

기술적 연관관계

개념적 연관관계

주요 특징

암호화폐 판매	▪ ICO(Initial Coin Offering) 자체가 목적	자체 암호화폐 보유
어플리케이션 플랫폼	▪ TheDAO(크라우드펀딩) ▪ ICO 기반 투자자금 확보	
송금 네트워크	▪ 은행간 청산과 통신 ▪ 가치의 거래와 이동	
자산발행 프로토콜	▪ 진본여부에 대한 공증 ▪ 위변조 방지 특성 기반	자체 암호화폐 부재
이더리움 호환 프로토콜	▪ 프라이버시 보호 ▪ 룰기반 접근제어	
범산업 분산원장	▪ 식품유통망 이력 추적 ▪ 상용 부동산 임대 보장	
거래/계약 처리 분산원장	▪ 담보/유동성 관리 ▪ 무역금융	

✓ EEA: Enterprise Ethereum Alliance: Ethereum 기반 솔루션간 호환성 추구

중점 표준화 항목 및 대응 기구

핵심 기술

- 블록체인 용어 : ISO TC 307
- 블록체인 기반 투명한 트랜잭션과 응용을 위한 보안 요구사항 : ISO TC307, ITU-T SG17
- 블록체인 ID 관리 : ISO TC 307

플랫폼 기술

- 클라우드 기반 블록체인 : ITU-T SG13

서비스 기술

- 블록체인 기반 전자문서 유통 : ISO TC 307
- 콘텐츠 저작권 정보의 블록체인 관리 : ITU-T SG13
- 블록체인 기반 전자투표 : ISO TC 307
- IoT 블록체인의 Trust 구조 및 가이드라인 : oneM2M, ITU-T SG20

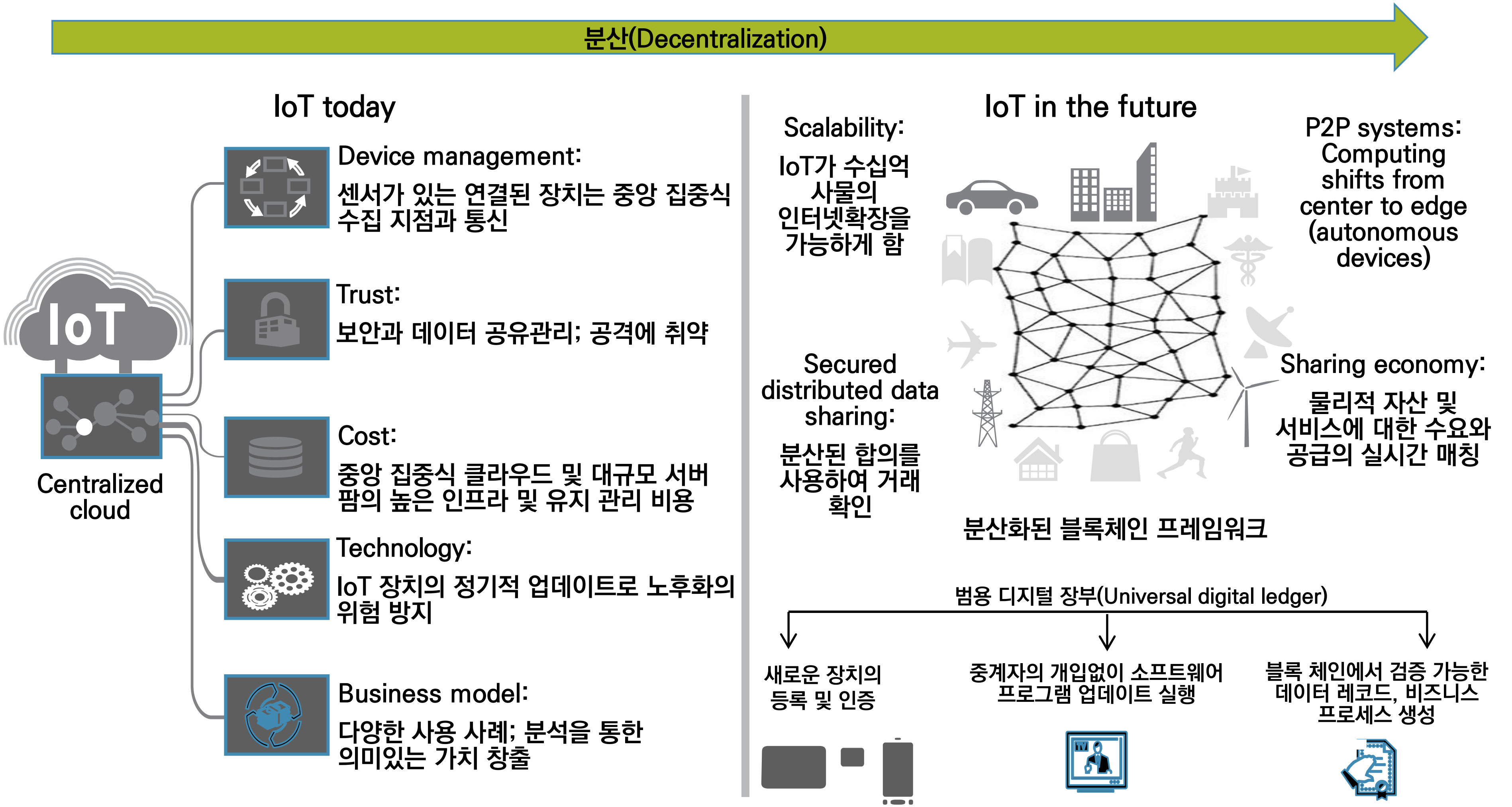
관리 기술

- 블록체인 기반 시스템에 대한 신뢰성 평가 기준 : ISO TC 307, ITU-T SG17
- 분산원장 기반의 금융서비스에 대한 보안 위협 및 보안 요구사항 : ISO TC 307, ITU-T SG17
- 분산원장 기술을 활용한 온라인 투표에 대한 보안 위협 : ITU-T SG17
- 개인정보보호지침 : ITU-T SG17 / FG DLT, ISO TC 307

IoT 블록체인

IoT 블록체인 개요

블록체인 프레임워크는 중앙 집중식 제어를 필요로 하지 않고 장치 간 P2P (peer-to-peer) 통신을 가능하게 함으로써 확장 가능하고 안전하며 효율적인 IoT를 용이하게 함



분산(Decentralization)

IoT today

Centralized cloud

Device management:

센서가 있는 연결된 장치는 중앙 집중식 수집 지점과 통신

Trust:

보안과 데이터 공유관리; 공격에 취약

Cost:

중앙 집중식 클라우드 및 대규모 서버 팜의 높은 인프라 및 유지 관리 비용

Technology:

IoT 장치의 정기적 업데이트로 노후화의 위험 방지

Business model:

다양한 사용 사례; 분석을 통한 의미있는 가치 창출

IoT in the future

Scalability:

IoT가 수십억 사물의 인터넷확장을 가능하게 함

P2P systems: Computing shifts from center to edge (autonomous devices)

Secured distributed data sharing:

분산된 합의를 사용하여 거래 확인

Sharing economy:

물리적 자산 및 서비스에 대한 수요와 공급의 실시간 매칭

분산화된 블록체인 프레임워크

범용 디지털 장부(Universal digital ledger)

새로운 장치의 등록 및 인증

중계자의 개입없이 소프트웨어 프로그램 업데이트 실행

블록 체인에서 검증 가능한 데이터 레코드, 비즈니스 프로세스 생성

IoT와 블록체인 융합 배경

- 사물인터넷(IoT, Internet of Things)의 도입이 활성화되고 있으나 확장성과 보안 등이 사물인터넷 도입의 저해 요소로 인식

- 사물인터넷의 이러한 단점을 보완하고 보안성을 강화하기 위해 사물인터넷에 블록체인(Blockchain)을 활용하는 시도 증가

IoT와 블록체인 융합시 기대효과

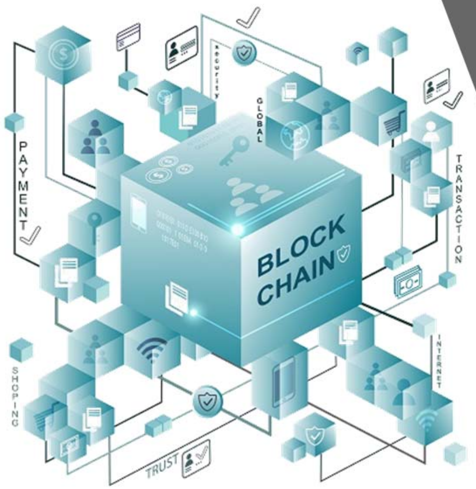
첫째, 보안강화

- 확장성 좋고 분권화된 보안을 사물 인터넷 디바이스와 애플리케이션, 플랫폼에 가져다 줄 것으로 기대

➔사물 인터넷 역시 분산되어 있고 분권화되어 있기 때문

- 개별 IoT Device 보안 취약점의 근본적 해결 방안

- 비인가 디바이스 및 데이터 위·변조 문제의 부분 해결



① 개발 아이템과 패키지의 이력을 안전하게 등록하고 추적

② 감사 기록을 생성하고 새로운 종류의 스마트 계약을 가능하게 만듦

③ 블록체인 기술은 안전하고 신뢰할 만한 응답 확인 방식으로 디바이스 간에 돈이나 데이터 같은 자산의 일부를 직접 전송할 수 있는 단순 인프라

IoT와 블록체인 융합시 기대효과

둘째, 비용절감 – IoT 기능이나 비용 효율성도 개선

블록체인 : "트랜잭션이나 인터랙션과 관련된 애플리케이션"

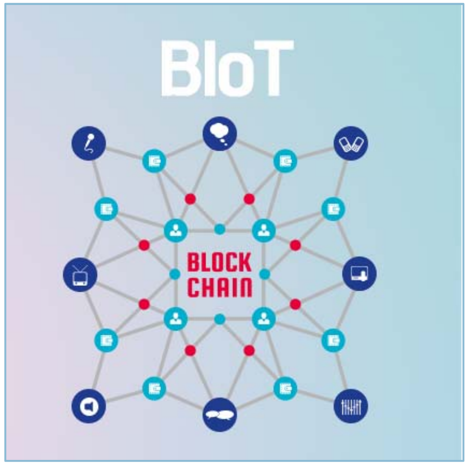
① IoT 프로세스 감시 적합

② 특정 조건을 만족하면 자동으로 특정 작업 수행 가능

③ IoT의 ID와 Discovery 지원 가능

④ Micro-transaction을 촉진하고 IoT 디바이스 간 지급 증명 구축 가능

셋째, Risk Hedging – C/S 기반 서비스의 잠재적 위험 (중앙 서버 장애 시, 전체 서비스 불가)



IoT와 블록체인 융합시 예상 한계점

첫째, 기존 블록체인 동작원리는 IoT 환경에 부적합

- 합의 알고리즘, 트랜잭션 구조 등이 거래에 최적화
- 경량화된 노드는 정식 노드로서 참여가 불가능하기 때문에 다양한 사물이 존재하는 IoT환경에서 부적합

사물인터넷 생태계의 구조는 단말기(사물)와 네트워크 인프라, 클라우드 인프라, 게이트웨이 등 네 가지 요소로 구성

:: 다양한 사물끼리 소통하면서 인간에게 편리하고 쾌적한 생태계를 조성해 주려면 이 요소 모두가 통일성 있는 시스템에서 서로 잘 소통되어야 함

But, 아직까진 다양한 디바이스가 다양한 프로토콜과 기술을 사용하기 때문에 구성이 복잡해지고 때로 충돌도 발생

둘째, 블록체인 내에서 사물인터넷 기기 인식 및 식별자 검증 기술 및 IoT 플랫폼을 위한 외부 API호출 기술 개발 필요

블록체인의 IoT 적용

**블록체인 기술이 사물인터넷의 다양한 분야에서 적용될 것으로 예상되며,
주로 데이터 관리, 거래 또는 인증을 위한 목적으로 블록체인 도입 가능**

**(데이터 관리)
사물인터넷이 수집한 데이터의 저장·관리**

- (감사) 수집데이터 해시값을 블록체인에 저장할 경우 비인가자에 의한 수집데이터 변조, 삭제 등의 오남용 추적 감사 가능

  ※ 수집데이터는 별도의 저장소(데이터베이스, 클라우드 스토리지 등)에 저장하고, 블록체인에는 수집데이터 관리에 필요한 해시값 등 메타데이터를 저장

- (접근통제) 수집데이터에 대한 접근권한 정책(policy 또는 rule)을 블록체인에 저장하여 소유권이 있는 사용자만 접근하도록 통제

**(거래)
사물인터넷 센서로부터 수집된 데이터의 안전 거래 환경 제공 ➔ 제3의 기관 없이 거래 가능**

- (응용) 운동 관련 앱 제공자(Nike 등)가 미세먼지 정보를 수집하는 기관으로부터 데이터를 구매하여 이용자에게 운동 최적 시기 제공

**(인증)
사물인터넷 기기들의 인증키(public key)를 블록체인에 저장하여 등록, 갱신, 폐기 등의 키관리를 수행하고, 사물인터넷 기기 간 인증 필요 시 블록체인을 통해 검증**

블록체인 플랫폼 동향

블록체인 플랫폼 경쟁(1)

블록체인 플랫폼을 둘러싼 치열한 경쟁은 다양한 방식으로 진행 중

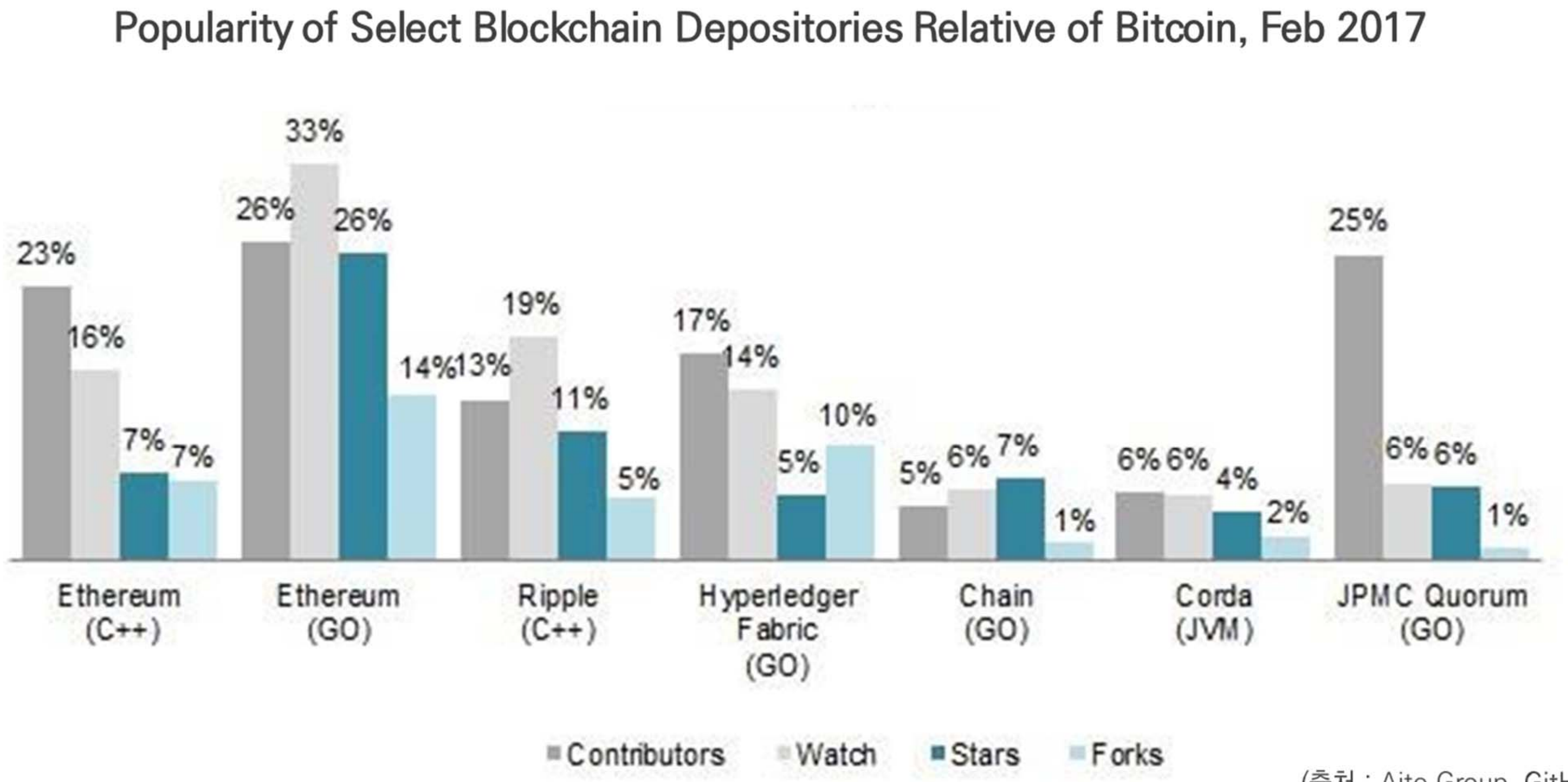
Top 10 Capital Markets Chaintech Platforms: Securities Settlement in Focus

- Hyperledger's Fabric
- Chain Core
- R3's Corda
- Nasdaq Linq
- Enterprise Ethereum
- Axoni AxCore
- Digital Asset platform
- Symbiont's Assembly
- SETL's OpenCSD
- Overstock.com's t0

(출처 : Aite Group)

블록체인 플랫폼 경쟁(2)

블록체인 플랫폼을 둘러싼 치열한 경쟁은 다양한 방식으로 진행 중



(출처 : Aite Group, GitHub)

IT서비스사 블록체인 주도권 경쟁

핀테크 업체 중심으로 블록체인 플랫폼이 개발되었고, 올해부터 IT서비스사도 블록체인 플랫폼을 발표, 주도권 경쟁 시작

coinplug
Fidoledger

theloop
loopCHAIN

blocko
coinstack

ScaleChain

BOScoin

SAMSUNG SDS
Nexledger™

LG CNS

SK 주식회사 C&C

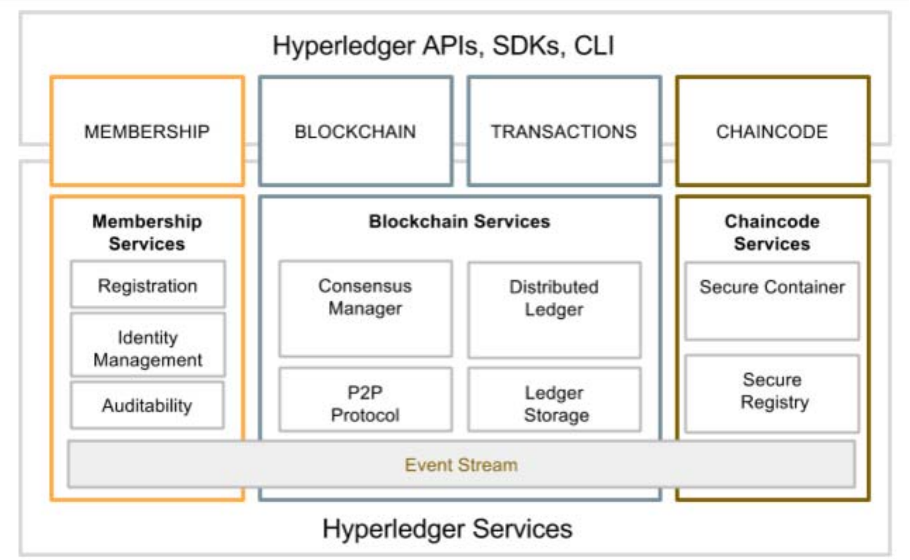
현대BS&C

주요 IoT 블록체인 플랫폼 동향

Linux Foundation's Hyperledger Project

- 리눅스 재단의 Hyperleder 프로젝트는 2015년 12월 17일에 17개 회원사로 시작됨
- 현재 210여개 회원사가 참여하고 있음
- Hyperledger 프로젝트는 전세계적으로 비즈니스 거래가 수행되는 방식을 변혁할 수 있는 분산 원장에 대한 산업 표준에 중요한 기능들을 확인하고 적용하여 블록체인을 발전시키기 위한 협력 프로젝트 임
- 오픈 소스 및 오픈 표준 기반으로 주로 기업결제, 상품추적 및 관리 등을 위한 산업용 공동 플랫폼으로의 역할
- 대표적인 참가기업으로는 액센츄어, 시스코, IBM, intel, J.P.Morgan 등
- 블록체인 유관기업으로는 R3, DA(Digital Asset), ConsenSys, Blockstream, 코인플러그(Coinplug) 등

HYPERLEDGER



Hyperledger APIs, SDKs, CLI

MEMBERSHIP

BLOCKCHAIN

TRANSACTIONS

CHAINCODE

Membership Services

Registration

Identity Management

Auditability

Blockchain Services

Consensus Manager

Distributed Ledger

P2P Protocol

Ledger Storage

Chaincode Services

Secure Container

Secure Registry

Event Stream

Hyperledger Services

Hyperledger Reference Architecture

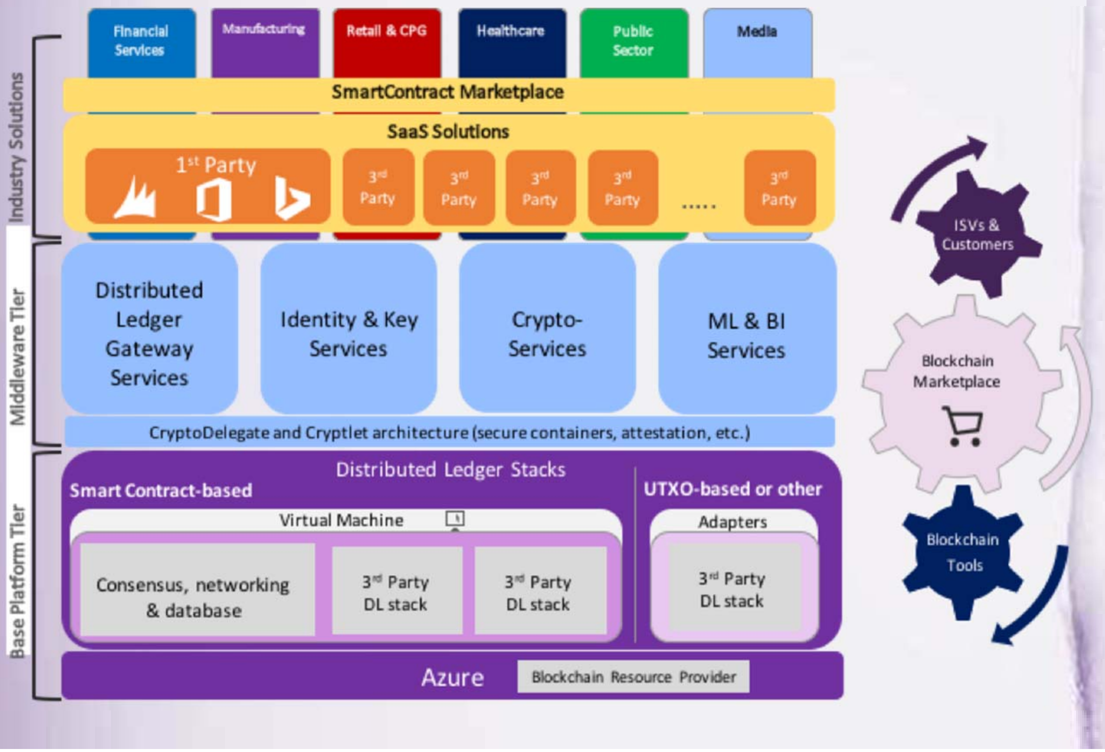
https://jira.hyperledger.org/secure/Dashboard.jspa?selectPageId=10104

Microsoft's BaaS

:: ETH BaaS

Microsoft
Bletchley

- 2016. 11월 블록체인 플랫폼 개발업체인 '컨센시스'와 손잡고 애저(Azure) 위에 블록체인 서비스(BaaS)를 구현
- **MS 클라우드 서비스인 애저 위에서 애플리케이션을 개발하고 배포할 수 있으며, 크게 블록체인 미들웨어와 블록체인 기술의 새로운 빌딩 블록을 일컫는 '크립틀렛'으로 이루어 짐**



Industry Solutions

Financial Services | Manufacturing | Retail & CPG | Healthcare | Public Sector | Media

SmartContract Marketplace

SaaS Solutions

1st Party | 3rd Party | 3rd Party | 3rd Party | 3rd Party | ..... | 3rd Party

Middleware Tier

Distributed Ledger Gateway Services | Identity & Key Services | Crypto-Services | ML & BI Services

CryptoDelegate and Cryptlet architecture (secure containers, attestation, etc.)

Base Platform Tier

Distributed Ledger Stacks

Smart Contract-based

Virtual Machine

Consensus, networking & database | 3rd Party DL stack | 3rd Party DL stack

UTXO-based or other

Adapters

3rd Party DL stack

Azure | Blockchain Resource Provider

ISVs & Customers

Blockchain Marketplace

Blockchain Tools

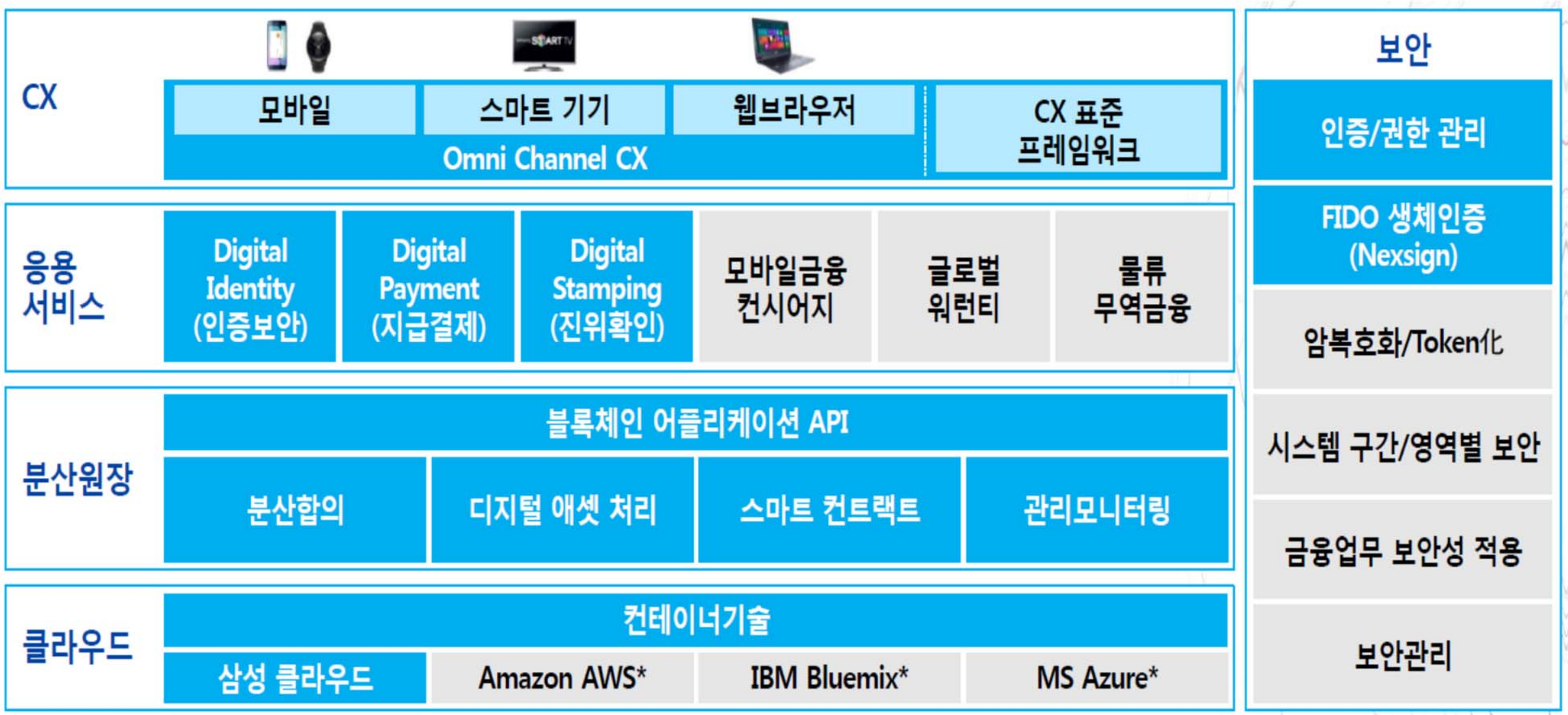
Microsoft's BaaS

:: ETH BaaS

- 블록체인 미들웨어는 클라우드 서비스 운영 관리, 블록체인 게이트웨이, 암호화·인증 서비스, 데이터 분석 서비스, 머신러닝 등과 같은 기능을 제공한다. 이 모든 기술은 애저의 여러 서비스 요소와 결합해 활용할 수 있으며, 써드파티 개발사도 자사 솔루션을 연동해서 활용
- 크립틀렛은 블록체인3.0에서 등장한 새로운 빌딩 블록. 애저 클라우드와 다른 퍼블릿 혹은 프라이빗 클라우드 사이 암호화된 통신 환경을 제공하며, 애플리케이션과 정보를 주고 받을 때 보안된 정보를 주고 받을 수 있게 도움
- 다양한 블록체인 프로토콜을 지원하며, 아직 소비되지 않고 지갑에 남아 있는 비트코인 화폐를 일컫는 UTXO(Unspent Transaction Output-based protocols)와 블록체인에 모든 노드에 접근할 수 있는 코드를 업로드하면 이를 실행하는 규칙을 따르는 스마트 계약(Smart Contract) 프로토콜 준수

삼성 SDS,「Nexledger™」

- 표준화된 확장성 및 실시간처리 기반 스마트계약, 관리모니터링, 내·외부연계, 생체인증, CX 등을 결합한 기업용 블록체인 플랫폼
- 다양한 서비스를 단일 블록체인 플랫폼에서 신속히 론칭하고 표준 컨테이너 단위 구성으로 제약 없이 규모 확장이 가능함



CX

모바일

스마트 기기

웹브라우저

Omni Channel CX

CX 표준 프레임워크

응용 서비스

Digital Identity (인증보안)

Digital Payment (지급결제)

Digital Stamping (진위확인)

모바일금융 컨시어지

글로벌 워런티

물류 무역금융

분산원장

블록체인 어플리케이션 API

분산합의

디지털 애셋 처리

스마트 컨트랙트

관리모니터링

클라우드

컨테이너기술

삼성 클라우드

Amazon AWS*

IBM Bluemix*

MS Azure*

보안

인증/권한 관리

FIDO 생체인증 (Nexsign)

암복호화/Token化

시스템 구간/영역별 보안

금융업무 보안성 적용

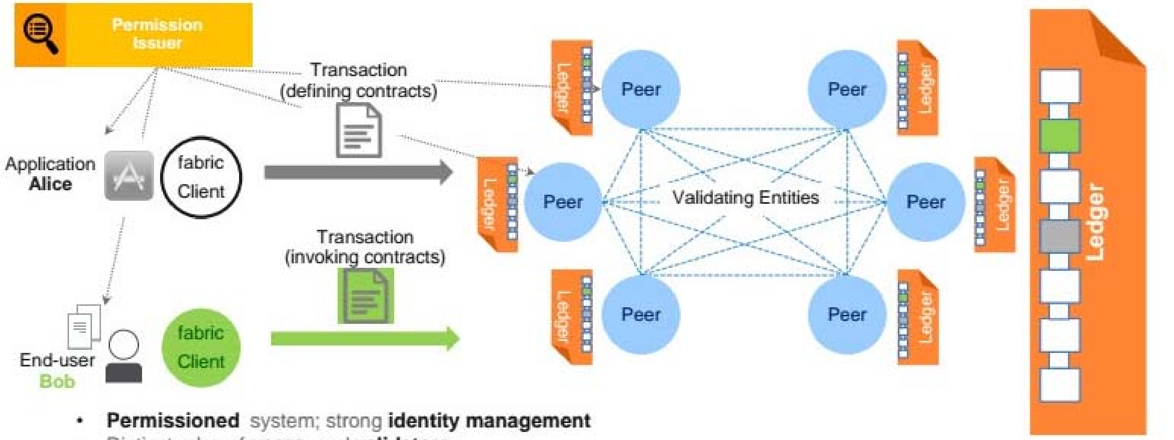
보안관리

* 삼성 클라우드에 기본적으로 구성되나 AWS/Bluemix/Azure 등 적용 가능

IBM's Hyperledger Fabric

리눅스 재단(Linux Foundation)과 IBM의 주도로 2015년 12월부터 '하이퍼레저(Hyperledger)' 프로젝트가 시작됨

- 시스코(Cisco), JP모건(JP Morgan), 인텔(Intel), 웰스 파고(Wells Fargo) 등 글로벌 기업들이 공동으로 참여
- 기업결제, 상품 추적 및 관리 등을 위한 오픈소스 분산원장 프레임을 개발하고 글로벌 블록체인 기술 표준화 작업을 진행
- 최근 IBM과 하이퍼레저 컨소시엄은 기업용 블록체인 네트워크 프레임워크인 '패브릭(Fabric)'을 공개
- 블록체인이 인터넷 상의 트랜잭션 처리를 위한 공통 프로토콜이 될 것으로 전망



- **Permissioned** system; strong **identity management**
- Distinct roles of **users**, and **validators**
- Users **deploy** new pieces of code (chaincodes) and **invoke** them through **deploy** & **invoke** transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the **ledger**
- **Ledger** = total order of transactions + hash (global state)
- **Pluggable consensus** protocol, currently PBFT & Sieve

블록체인 플랫폼 비교

구분	Bitcoin	Ethereum	Hyperledger Fabric	R3CEV Corda
가상화폐	Yes	Yes	No	No
적용 영역	가상화폐	가상화폐/범용	범용	계약의 기록/자동화
네트워크 참여	Anyone	Anyone	Permissioned Network (membership Service)	Permissioned Network (doorman Service)
거래공유	전체 참여자에 전체 거래 공유	전체 참여자에 전체 거래 공유	전체 참여자에 전체 거래 공유 (멀티채널개념 :사용자 Grouping)	거래 당사자에게 해당 거래 공유
Smart Contract	not Turing complete only scripts, no loop	Turing complete object Solidity, Python	Turing complete chaincode Go-based or java	Turing complete Java, Kotlin
Virtual Machine	None	Ethereum Virtual Machine	Depends on language (Java, Go)	Java Virtual Machine
법적문구	N/A	법률문서를 해시값으로 저장	법률문서를 첨부할 수 있음	내재적 기능 (법률문구 실행)
거래 타당성 검토 (합의 알고리즘)	Mining (PoW)	Mining (PoW, PoS?)	Pluggable Consensus (PBFT, Solo, Kafka 등)	Consensus by Notary service (RAFT, PBFT 등)
State (상태값 표현)	UTXO	Account Base	Key, value pair	UTXO (Unspent TXn Output)
거래 처리량	합의에 따른 거래 처리 한계	합의에 따른 거래 처리 한계	Scalable by design	Scalable by design
원장의 확장성	글로벌 단일 원장	글로벌 단일 원장	채널별 단일 원장	글로벌 단일 원장
감독기관 지원	N/A	N/A	N/A	모니터링 노드 제공
DB	LevelDB	LevelDB	CouchDB, LevelDB	H2, MySQL
Player	Bitcoin 재단	Ethereum 재단	Linux 재단, IBM	R3, 100 여개 금융기관

신규 IoT 블록체인 플랫폼 개발 동향

Horizon : Edge Insights

깃허브(github.com)를 통해 오픈 소스로 개발된 블록체인 기반 IoT 솔루션으로 블록체인을 이용하여 Edge(사물인터넷 기기)를 서로 연결하고 Edge에서 수집한 데이터를 분석하여 항공기 추적, 라디오 전파 분석 등 다양한 분야에 활용

- Edge로부터 데이터를 생성하여 전송하는 생산자(Producer)와 데이터를 받아 이용하는 소비자(Consumer)로 구분되며 생산자와 소비자 간의 계약 (Agreement), 거래 내용 등을 블록체인에 등록
- Horizon은 블록체인을 이용하여 자동으로 시스템을 구성하고 스마트 컨트랙트를 통해 기기 간 거래를 자동화하였으며 추후 오픈 소스로 공개될 예정

Horizon의 IoT 기기 간 연결 절차

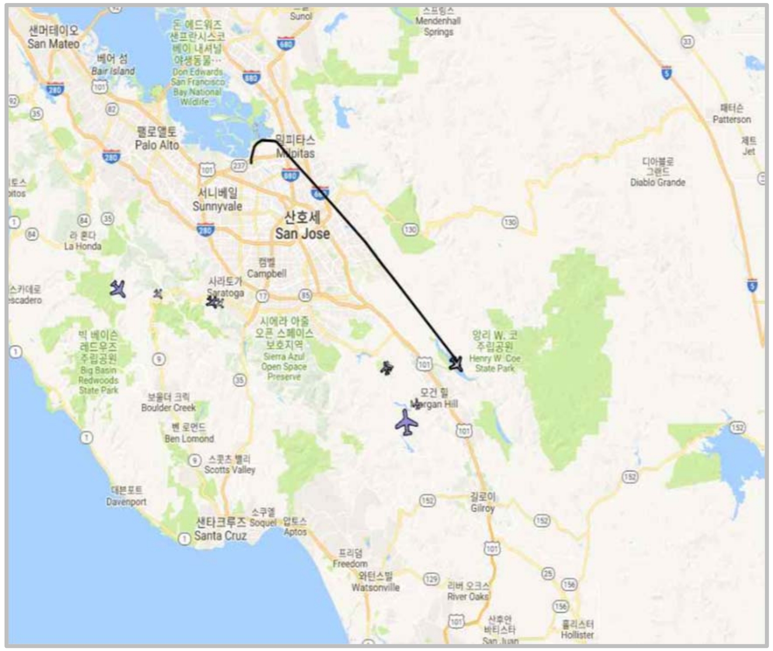
① Horizon에 등록된 소비자와 생산자는 요구 사항(데이터 종류, 비용 등)을 블록체인 노드에 등록하여 블록체인 참가자에 공유

② 소비자의 요구 사항에 부합하는 생산자와의 계약을 승인할 경우 계약 내용을 노드에 저장하여 블록체인에 등록

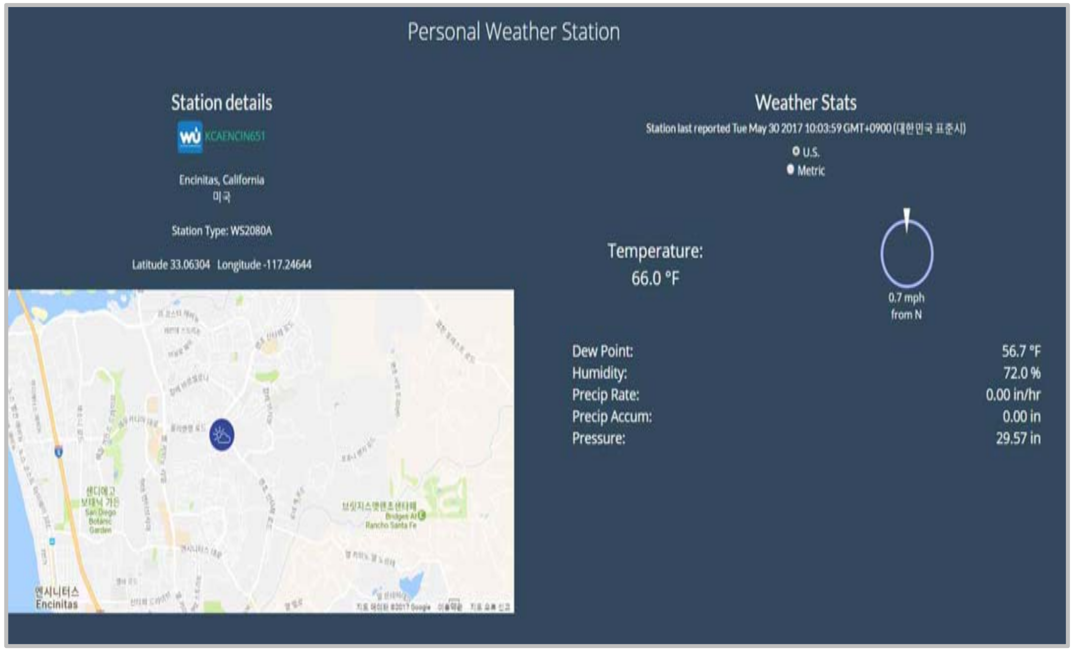
③ 등록된 블록체인 노드는 다른 소비자/생산자에게 전달되어 계약의 신뢰성 확보

Horizon : Edge Insights

- **현재 7개의 데이터 공유·분석을 위한 분야*가 운영 중이며 지속적으로 응용 분야를 개발 중**
  - 수집·분석된 내용은 Google맵을 통해 시각화 하여 기기 위치 정보가 제공되며 해당 기기의 링크를 통해 상세 정보를 웹 UI를 통해 확인 가능



Horizon의 Google맵을 이용한 IoT 기기 위치 시각화



Personal Weather Station

Station details

KCAENCIN651

Encinitas, California
미국

Station Type: WS2080A

Latitude 33.06304 Longitude -117.24644

Weather Stats

Station last reported Tue May 30 2017 10:03:59 GMT+0900 (대한민국 표준시)

○ U.S.
● Metric

Temperature:
66.0 °F

0.7 mph
from N

Dew Point: 56.7 °F
Humidity: 72.0 %
Precip Rate: 0.00 in/hr
Precip Accum: 0.00 in
Pressure: 29.57 in

Horizon의 Personal Weather Station 웹 UI

IOTA's Tangle

- Tangle 이라고 불리는 **새로운 형태의 분산 원장** 사용
  - 기존 블록체인의 사용자 및 채굴자 구분 구조 탈피
    - 신규 Transaction 1개 발생을 위해 기존 Transaction 2개 검증 필수
    - 기존 Transaction(=Tip) 선택하는 알고리즘 : MCMC(Markov Chain Monte Carlo)
  - 블록 형성을 위한 별도 과정이 존재하지 않아 거래 수수료 및 고성능 하드웨어 자원 불필요
- IoT 환경에서 micro-payment를 활성화할 목적으로 전송 수수료 면제(No Fee) 개념 도입
- 방향성 비-사이클 그래프(Directed Acydic Graph, DAQ) 알고리즘을 이용한 검증 기법 적용
- 근본적으로 블록체인과 동일한 분산 데이터베이스 및 P2P 네트워크를 이루고 합의와 확인(Consensus & Validation) 메커니즘 보유

Tangle에서 Transaction이 진행/검증되는 4단계

① 서명하기 : 개인 소유의 키로 거래 인풋을 서명

② 팁 선발 : 한 거래를 통해 다른 두 개의 팁(미 확인된 거래들)을 선택하기 위해 MCMC 알고리즘 사용

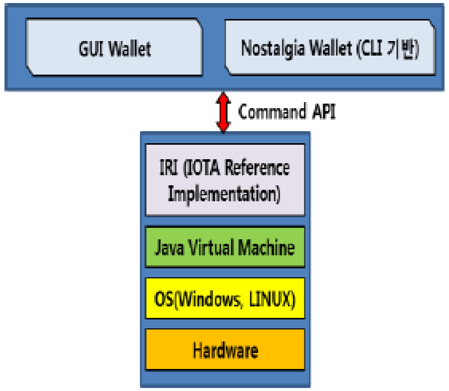
③ 작업증명 : Hashcash

④ 신규 Transaction(거래)가 네트워크에 브로드캐스트 됨 ➔ "팁"

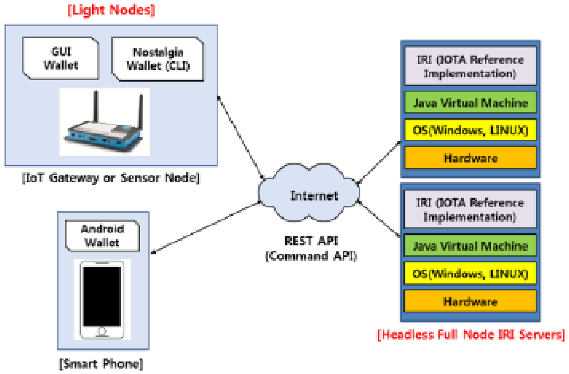
IOTA's Tangle

IoT용 블록체인 플랫폼인 Tangle 기술 분석(IRI Release 1.4.1.1, Beta Version)

- 데스크탑 PC 기반에서 환경 구축 /트랜잭션 처리 실험
- 저전력 Raspberry Pi-3 기반에서 Full node 구성 불가(ARM64 계열 지원불가), Light node는 시험 완료(2017.11)



<전용 Wallet을 가지고 있는 Full Node 구성도>



<Headless Full Node IRI와 Light Node(Wallet 만 탑재) 구성도>

Full Node

- Local에 IOTA 코어(IRI) 설치
- GUI Wallet or Nostalgia Wallet(CLI방식) 통해 IRI 연동

Light Node

- Wallet을 이용한 원격 구축
- Local에 Wallet(GUI/Nostalgia/Android) 설치
- 원격으로 IOTA 코어가 설치된 외부 IRI Server(Headless Full Node) 연동

IOTA's Tangle 플랫폼 현황 분석

- Neighbor 검색 및 추가가 어려움 (수동적 연결)
  - ✓ 다른 Node들과의 Neighbor 연결(UDP or TCP)을 통한 Private 형태로 운영
  - ✓ 신규 노드 가입 승인 및 원장 동기화를 위해 7~9개의 Neighbor 연결 권장 (via Slack Channel)
  - ✓ 8개의 Neighbor 연결에 일주일 소요
- 트랜잭션 성공률이 낮음
  - ✓ 트랜잭션 실패율 : 약 40%
  - ✓ 승인이 될 때까지 계속 reattach 과정 필수(하나 트랜잭션 승인: 평균 20분)
  - ✓ 작업증명과는 달리 이웃 노드에서 트랜잭션을 승인하는 구조로 되어있어, 노드 수가 적은 경우 비례적으로 트랙잭션 성공율이 낮음

➡ **New IoT 블록체인 기술 필요**

IoT 블록체인 USE CASE

비금융사 적용 방향

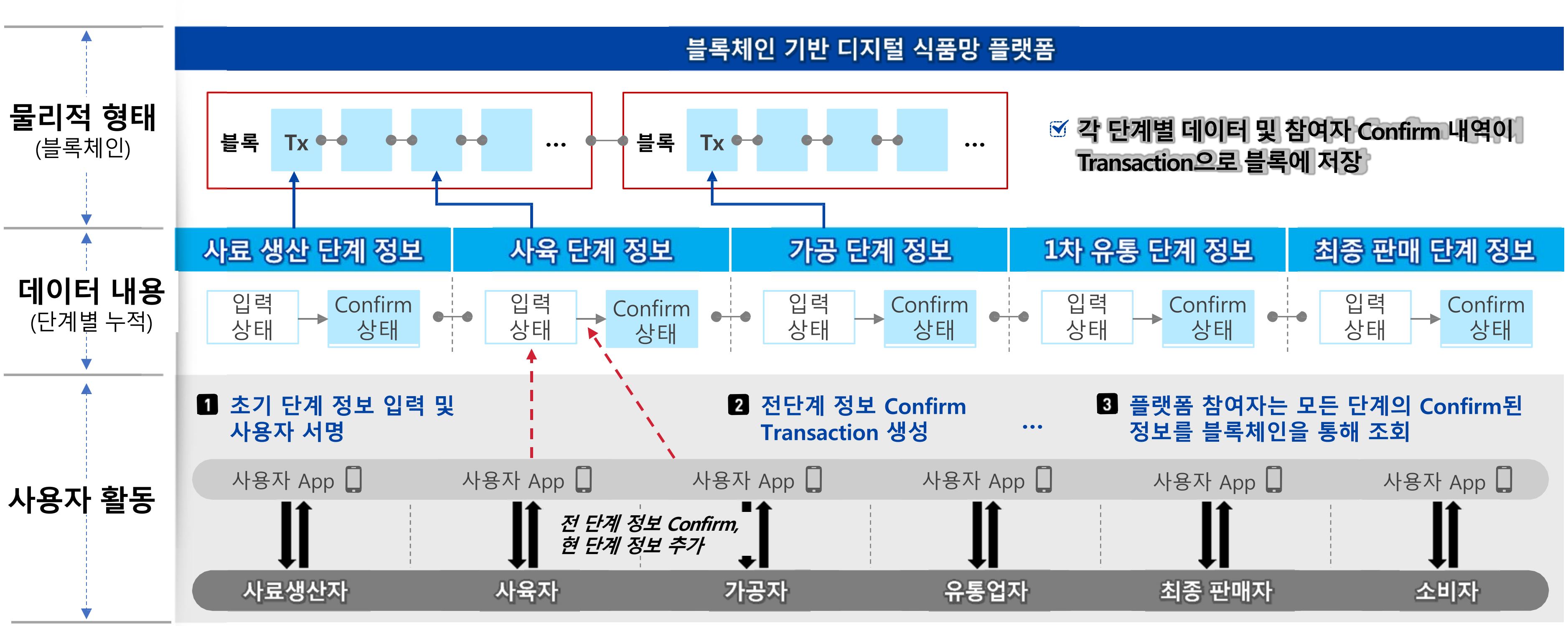
블록체인 및 Smart Contract 기능 적용은 지속적인 Value 창출 및 혁신을 통한 글로벌 경쟁력 강화의 새로운 기회를 제공함

제조업 Value-chain별 주요 시너지 기회

블록체인 특징	공급망	Manufacturing	판매망	고객 채널	新생태계
보안성	●	○	●	●	●
중간자 대체	◑	○	◑	◑	●
투명성	●	●	●	●	●
확장성	●	◑	●	●	●
자동화	●	◑	●	●	●
적용 유형	Process Automation 型	Shared Truth 型	Business Innovation 型		New Value Network 型
적용 기회	• 글로벌 공급망 금융 • Supplier 대상의 Dispute 관리	• 가공품 Provenance • 센서 기반의 장비 이상 계측 및 이력 관리	• 온·오프라인 판매 유통 채널 통합 • Partner Benefit 프로그램	• 글로벌 Warranty Program	• Industrial IoT • 커넥트오토와 UBI 결합

Digital Provenance

식품 생산 全 단계에 걸쳐 전달되는 품질 정보를 디지털 식품망으로 공유하여 식품 원산지정보에 대한 소비자 신뢰를 확보함



물리적 형태
(블록체인)

데이터 내용
(단계별 누적)

사용자 활동

블록체인 기반 디지털 식품망 플랫폼

블록 Tx …

블록 Tx …

☑ 각 단계별 데이터 및 참여자 Confirm 내역이 Transaction으로 블록에 저장

사료 생산 단계 정보

사육 단계 정보

가공 단계 정보

1차 유통 단계 정보

최종 판매 단계 정보

입력 상태 → Confirm 상태

❶ 초기 단계 정보 입력 및 사용자 서명

❷ 전단계 정보 Confirm Transaction 생성

…

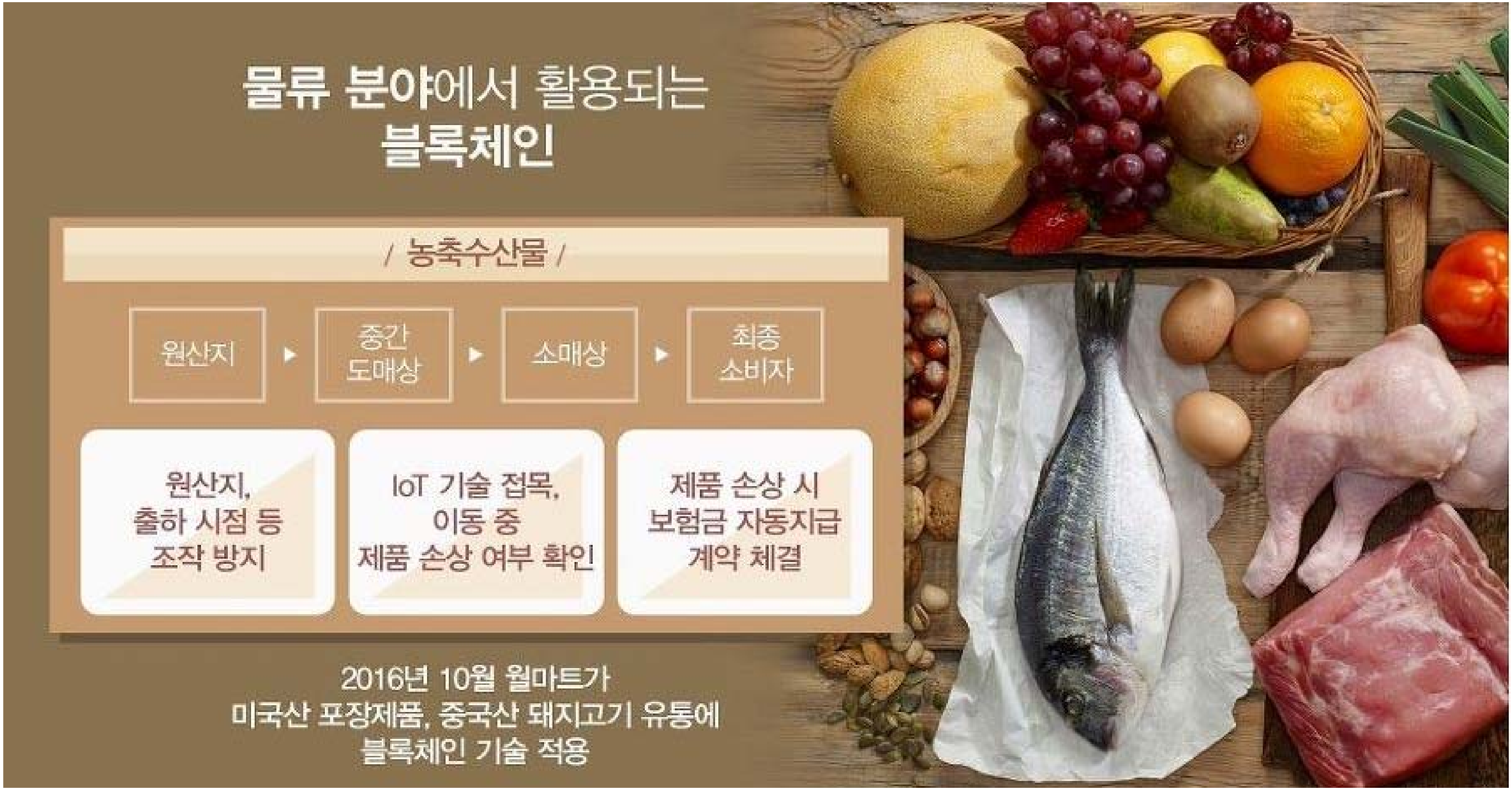
❸ 플랫폼 참여자는 모든 단계의 Confirm된 정보를 블록체인을 통해 조회

사용자 App

전 단계 정보 Confirm, 현 단계 정보 추가

사료생산자 · 사육자 · 가공자 · 유통업자 · 최종 판매자 · 소비자

(Source : 제 5회 Samsung Oracle Insight Forum)



물류 분야에서 활용되는
블록체인

/ 농축수산물 /

원산지 ▸ 중간 도매상 ▸ 소매상 ▸ 최종 소비자

원산지,
출하 시점 등
조작 방지

IoT 기술 접목,
이동 중
제품 손상 여부 확인

제품 손상 시
보험금 자동지급
계약 체결

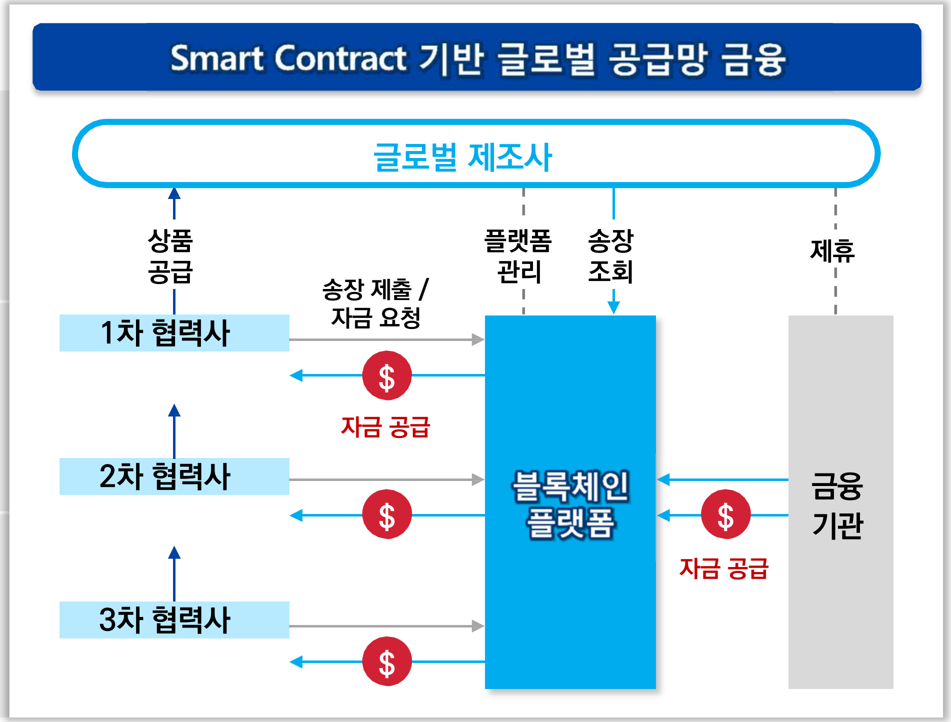
2016년 10월 월마트가
미국산 포장제품, 중국산 돼지고기 유통에
블록체인 기술 적용

- 2016년 10월부터 월마트가 미국산 포장제품, 중국산 돼지고기 유통에 블록체인 기술을 적용하고 있음

Supply Chain Finance

블록체인 및 Smart Contract 적용을 통해 글로벌 공급망의 투명성을 강화하고 협력사들의 자금 지원을 자동화함

특징	온라인 플랫폼을 통해 협력사 송장 기반의 글로벌 공급망 단기 자금 조달 지원 – 금융기관 제휴로 낮은 할인율에 대금 先 지급
블록 체인 적용 기회	글로벌 공급망 거래의 복잡성/불투명성으로 유동성 이슈 금융기관과 협력사를 연결하는 투명하고 안전한 거래
주요 기능	全공급망의 금융거래 정보 관리로 자금 흐름 가시성 확보 참여자間 상호 승인을 통한 자동화된 거래 확정/실행


Smart Contract 기반 글로벌 공급망 금융

블록체인 및 IoT 기술 활용,
미국산 면화의 중국 수출 전 과정을 관리하는
기술 시연

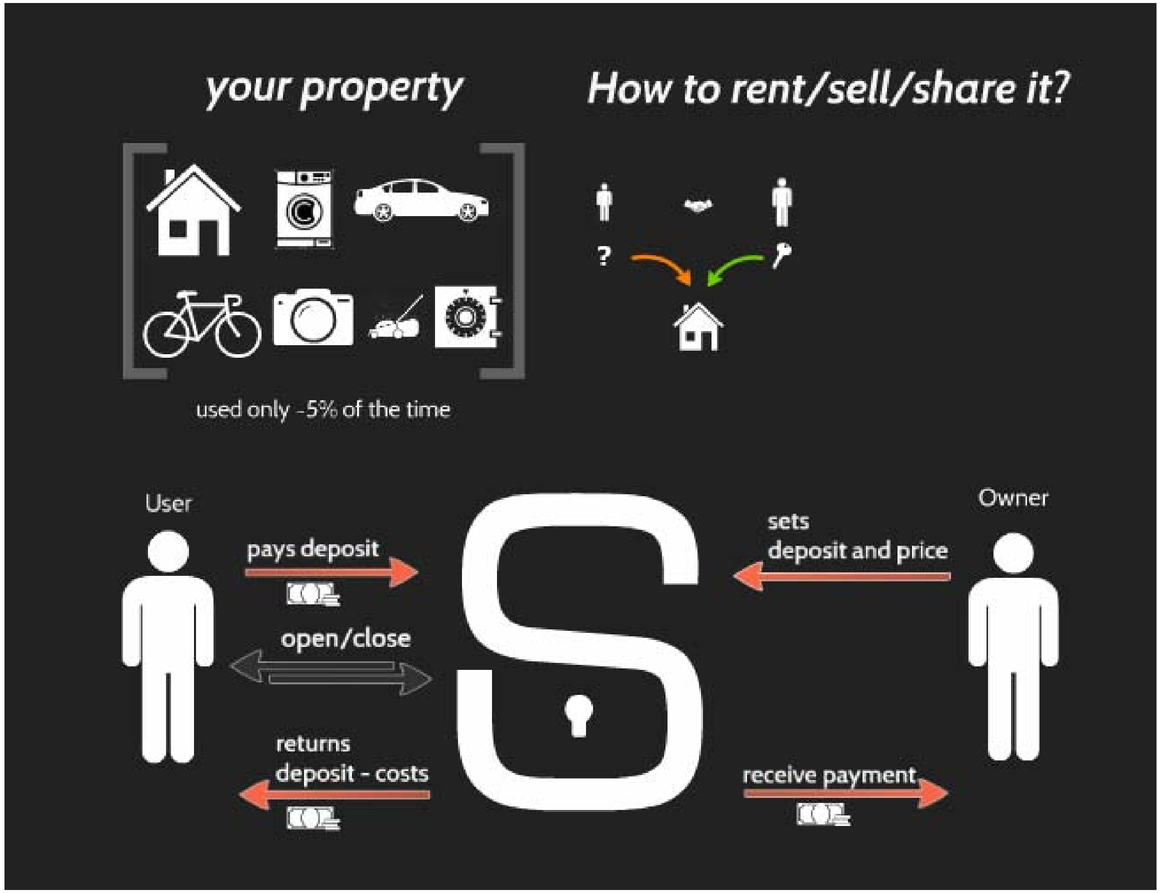
투명성을 제고해 서류 검토 시간을
며칠에서 몇 분으로 단축
▶ 수출 비용 절감

- A에서 Z까지 복잡한 여러 이해 관계자간 정보 전달을 스마트 계약으로 단순화
- 세분화 된 재고 추적 및 공급 보증 달성으로 공급망에서의 금융, 보험의 잠재적 위험 개선
- 사기 및 도난 위험 완화

- 커먼웰스 은행, 웰스파고 은행, 브리건 코튼사 는 블록체인과 IoT기술을 활용하여 미국산 면화의 중국 수출 전 과정을 관리하는 기술 시연
- 투명성을 제고해 서류검토시간을 몇 일에서 몇 분으로 획기적으로 감소시키며, 수출비용의 절감

블록체인 기반 집 임대 서비스 : 슬록잇

- 사용자가 블록체인을 통해 임대료의 2배의 금액을 보증금으로 제출한 다음 스마트폰을 이용해서 현관 문을 열고 집안의 다양한 서비스를 이용
- 이용이 끝나면 블록체인의 계약 내용과 비교하여 남은 금액을 정산해주는 서비스 제공



IoT와 블록체인이 만나면 … 슬록잇(Slock.It)

IoT와 블록체인을 결합해 수수료가 거의 없는 공유경제를 지향하는 스타트업

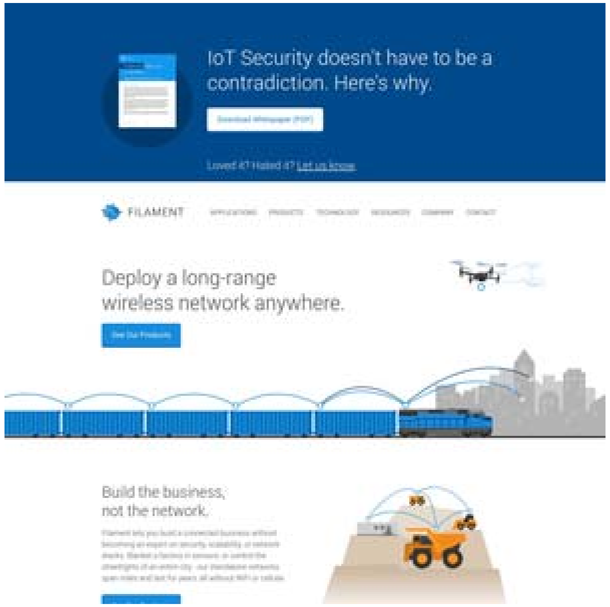
블록체인 기반 IoT 전원 소켓

사용자가 스마트폰을 이용해서 전원 소켓 이용권 신청 → 블록체인으로부터 이용권 전자 토큰 발급 → 이를 이용해서 전원 소켓을 활성화해서 사용할 수 있음

NAYUTA

블록체인과 IoT의 융합 : 필라멘트

- **필라멘트(Filament)**
  - 목표 : 분권화된 인터랙션과 교환을 위한 안전한 기반으로 제공하는 것
  - 블록체인 신생업체로 최근 산업용 IoT 디바이스가 여러 가지 블록체인 기술과 함께 동작하도록 하는 신형 칩 발표
  - 필라멘트의 블로클릿(Blocklet) 칩은 IoT 센터 데이터를 블록체인에 직접 코딩할 수 있도록 해줌



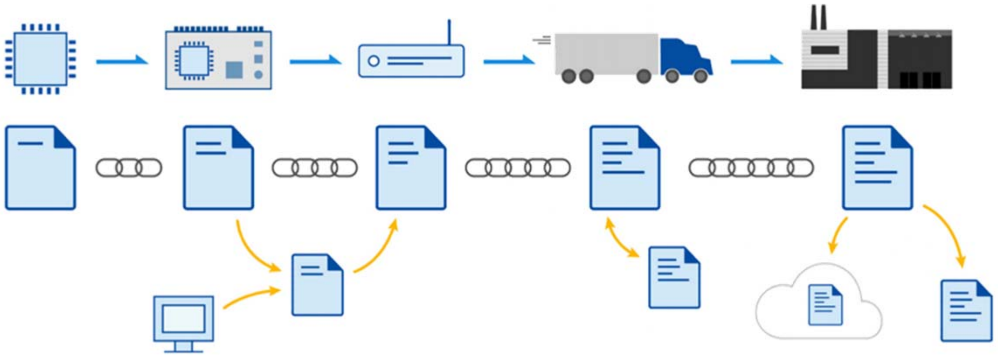
IoT Security doesn't have to be a contradiction. Here's why.

Loved it? Hated it? Let us know.

Deploy a long-range wireless network anywhere.

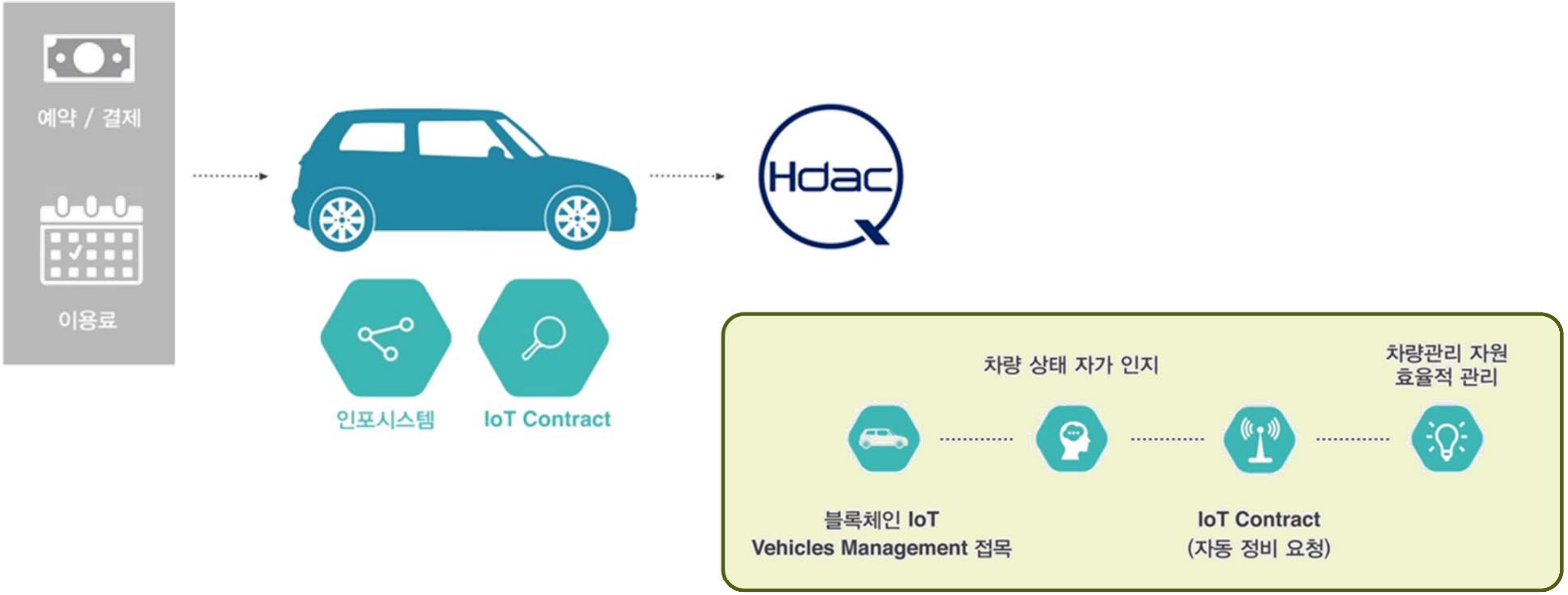
Build the business, not the network.

Filament lets you build a connected business without becoming an expert on security, scalability, or network stacks. Blanket a factory in sensors, or control the streetlights of an entire city - our standalone networks span miles and last for years, all without WiFi or cellular.



블록체인과 IoT의 융합 : HDAC

- HDAC (Hyundai Digital Asset Currency)
  - IoT 블록체인 신생업체
  - IoT용으로 특화된 자체 프라이빗 블록체인 구축



[참고] Intel Realsense 안면인식시스템 + IoT Blockchain Security
출처 : https://www.youtube.com/watch?v=QdIlU75nyAs

전력과 블록체인

"블록체인이 이끄는 새로운 전력시장은 분산된 전력시스템이 토대가 될 것"이며 "여기에는 대규모 원전 뿐만 아니라 태양광 패널, 전기차 배터리까지 모두 포함되며 수십억 명의 사람들이 블록체인 상에서 에너지를 소비하고 동시에 팔 수 있다".

– 미래학자 돈 탭스콧

➔ '미래 에너지의 생산과 분배, 거래 모두 블록체인에서 이뤄질 수 있다'는 의미

소수 대규모 생산자로부터 다수 소비자에게 에너지를 전달하는 **중앙집중형 단방향 전력 계통 구조**

다수의 생산자와 소비자(프로슈머)가 분산형으로 서로 에너지를 주고 받는 **양방향 전력 계통 구조**

전력 발전과 판매를 겸업할 수 없도록 규정하고 있는 전기사업법 개정 필요

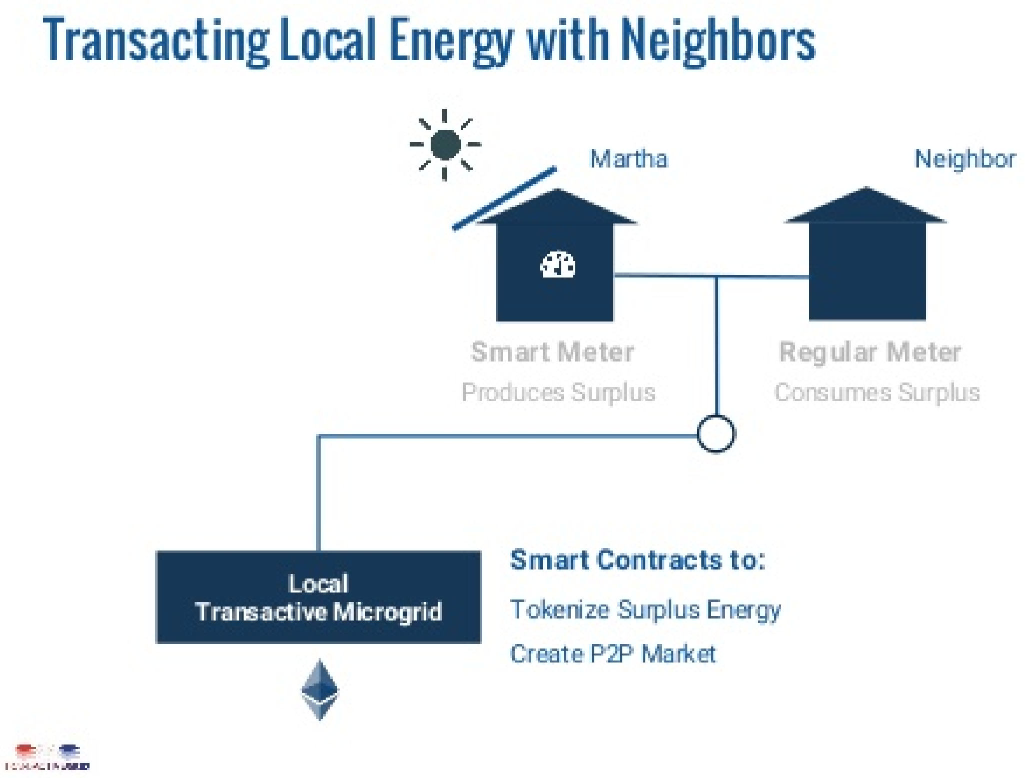
☞ 현재, 생산/소비자 간 직접거래(P2P: peer to peer) 사업이 활성화되지 못하고 있음
➔ 한전이나 전력거래소를 통해 전력을 거래하는 것이 원칙

※ 2017.12 과학기술정보통신부와 한전은 '블록체인 기반 이웃간 전력거래 및 전기차 충전 서비스' 구축

전력시장 : LO3 Energy

https://lo3energy.com/

- 개인이 자가발전 등으로 생산한 전기를 주변 마을 사람들에게 블록체인 기반으로 판매
- 2016년 4월 미국 뉴욕에서 TransActive Grid 프로젝트로 실증 실험 완료



IoT 블록체인 플랫폼 전망

IoT 블록체인 플랫폼 전망

블록체인 기술이라면,

1. 중앙 대형 센터를 거치지 않는 일명 'P2P 메시징' 방식으로 에너지와 비용 소비를 대폭 낮추고,
2. 분산형 파일 공유로 보안을 강화하며,
3. 네트워크 간 자율적 코디네이션을 통해 기기를 연결시켜줄 수 있다는 전망

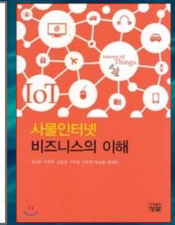
[해결 과제]

- 운영 및 호환성 문제
- IoT와 블록체인의 결합이 불러올 법적 문제와 컴플라이언스 문제

블록체인은
지금까지 확인된 IoT 생태계 구축 과정에서의 문제점을 모두 극복할 수 있을 뿐 아니라 한층 포괄적이고 활성화된 IoT 생태계를 유지하는 데 꼭 필요한 기능을 갖고 있는 기술

THANK YOU

for **attending**



이 두 원

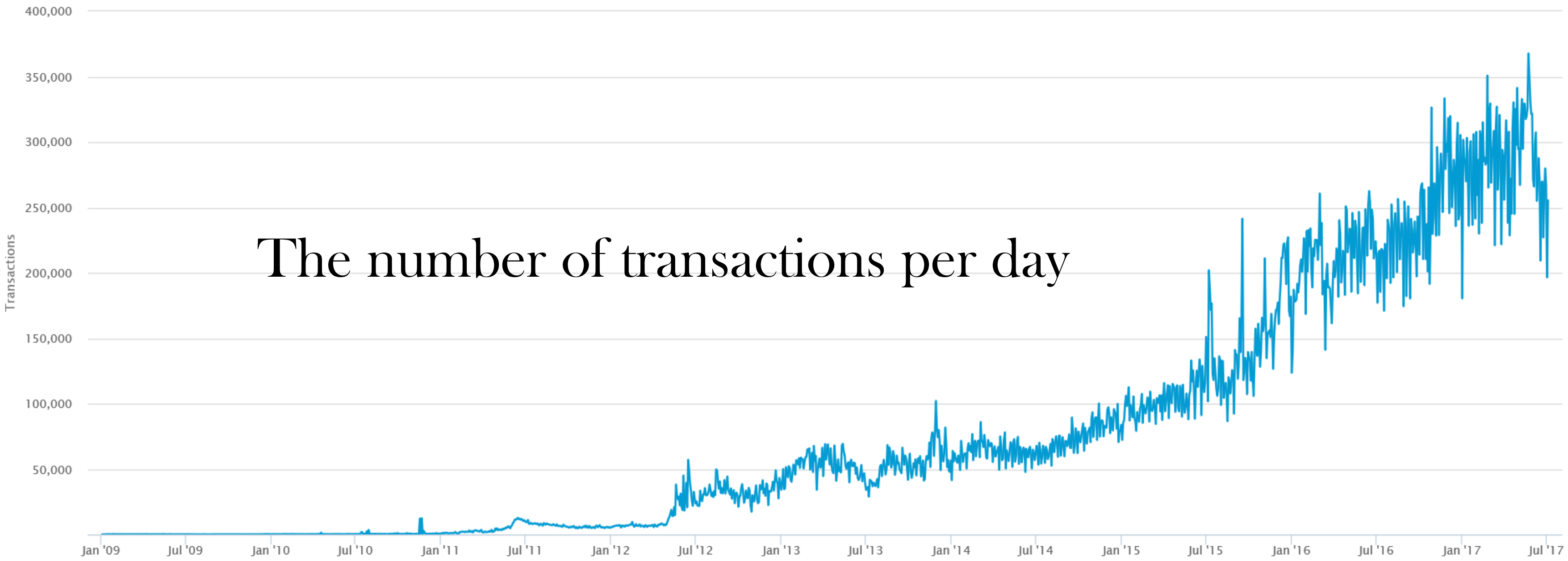
○ ㈜아니스트 대표이사 / 공학박사, 신지식인
○ 전, 국립 부산대학교 교수
○ 전, LG히다찌㈜ 상무이사
○ 주요분야 : IoT, SCM, 핀테크, 블록체인
○ Mail : doowon.lee@gmail.com

블록체인 취약점 연구 동향

Yongdae Kim
Korea Advanced Institute of Science and Technology
School of Electrical Engineering
System Security Lab.

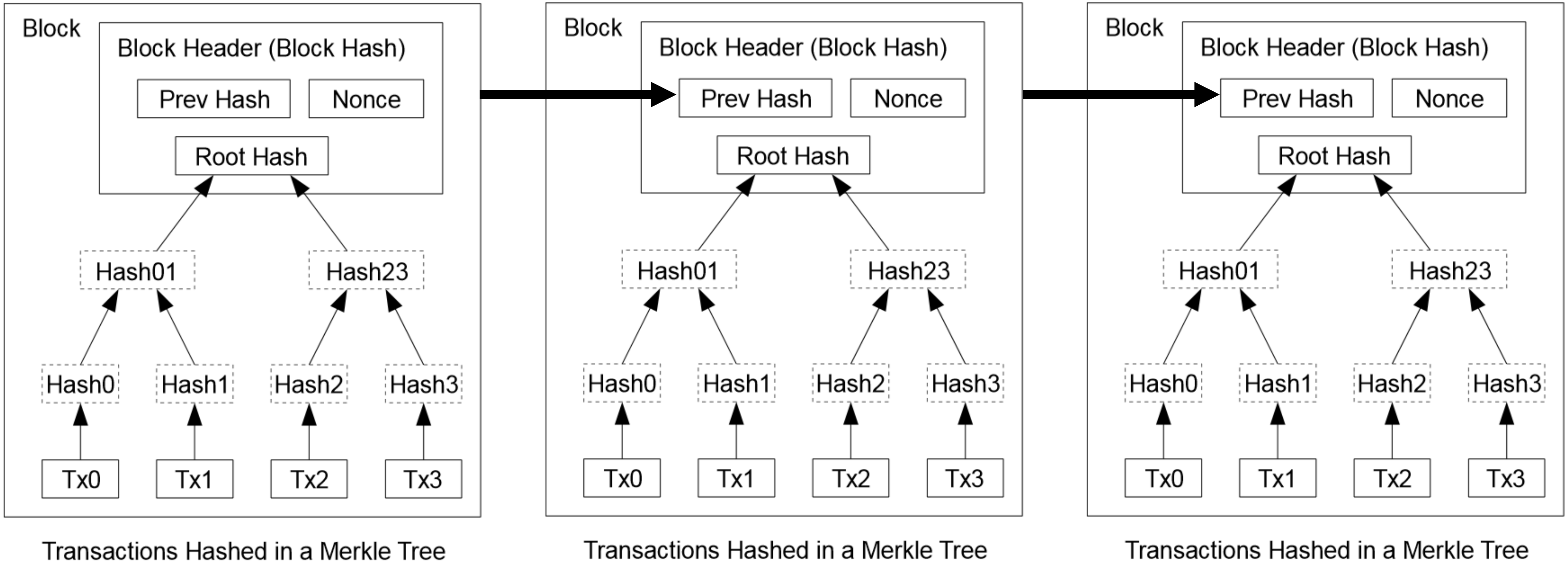
What is Bitcoin?

- Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009.
- Bitcoin is a first cryptocurrency based on a peer-to-peer network.
- Bitcoin as a form of payment for products and services has grown, and users are increasing.



The number of transactions per day

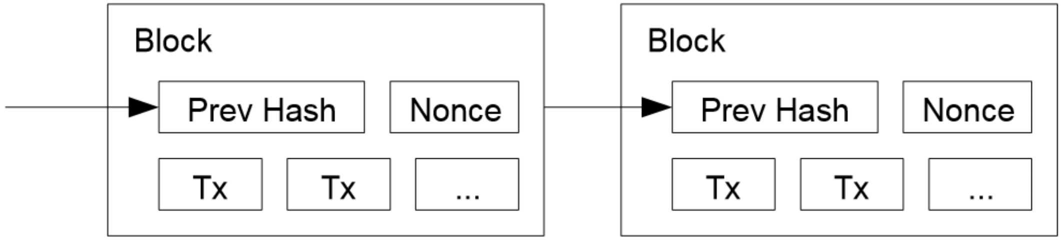
Blockchain



- ❖ Blocks connect as a chain.
- ❖ Each header of blocks includes the previous block’s hash.

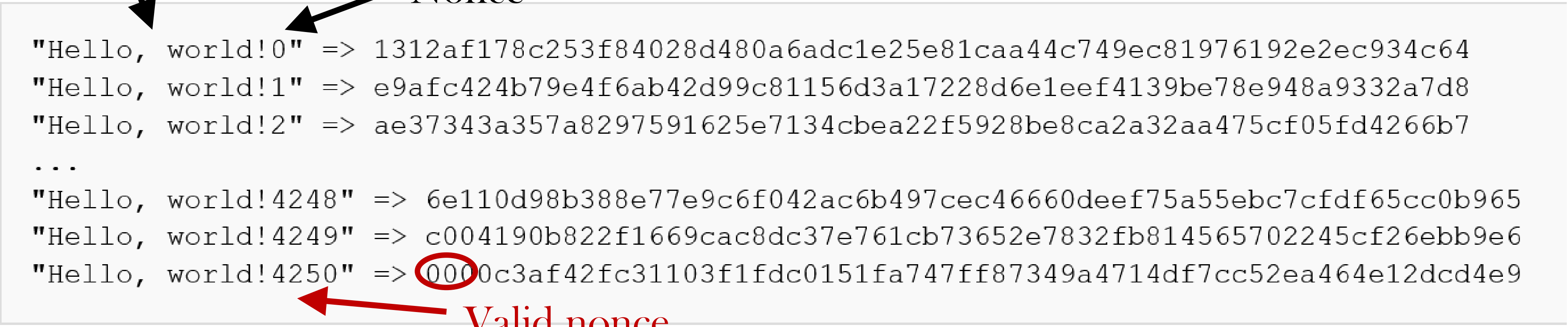
Proof-of-Work

- Proof-of-work scheme is based on SHA-256
- Proof-of-work is to find a valid Nonce by incrementing the Nonce in the block header until the block's hash value has the required prefix zero bits.



Contents

Nonce

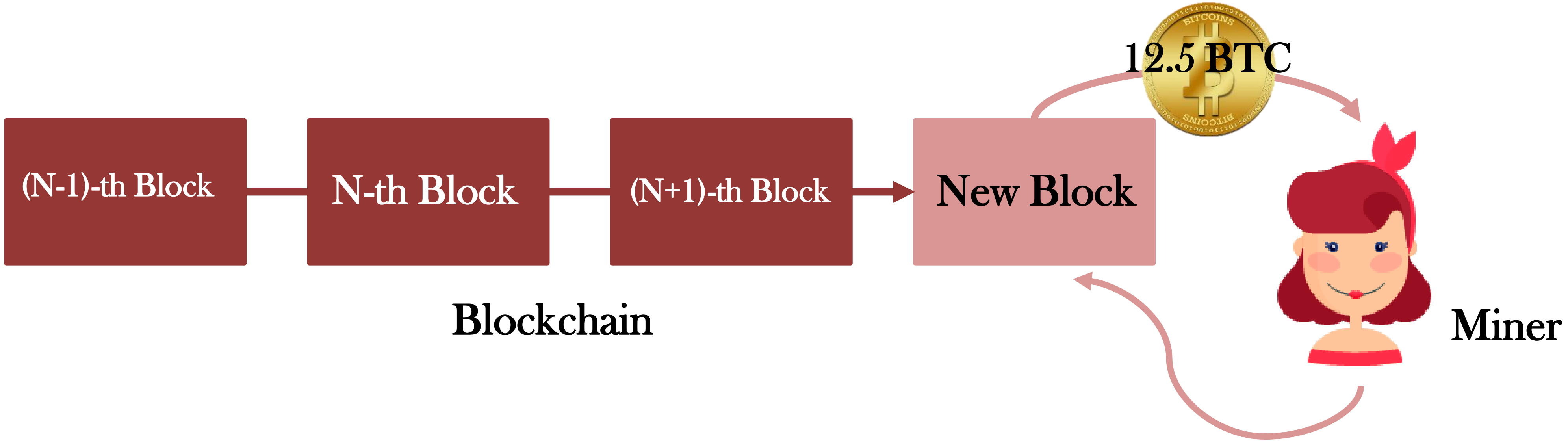


```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Valid nonce

Reward

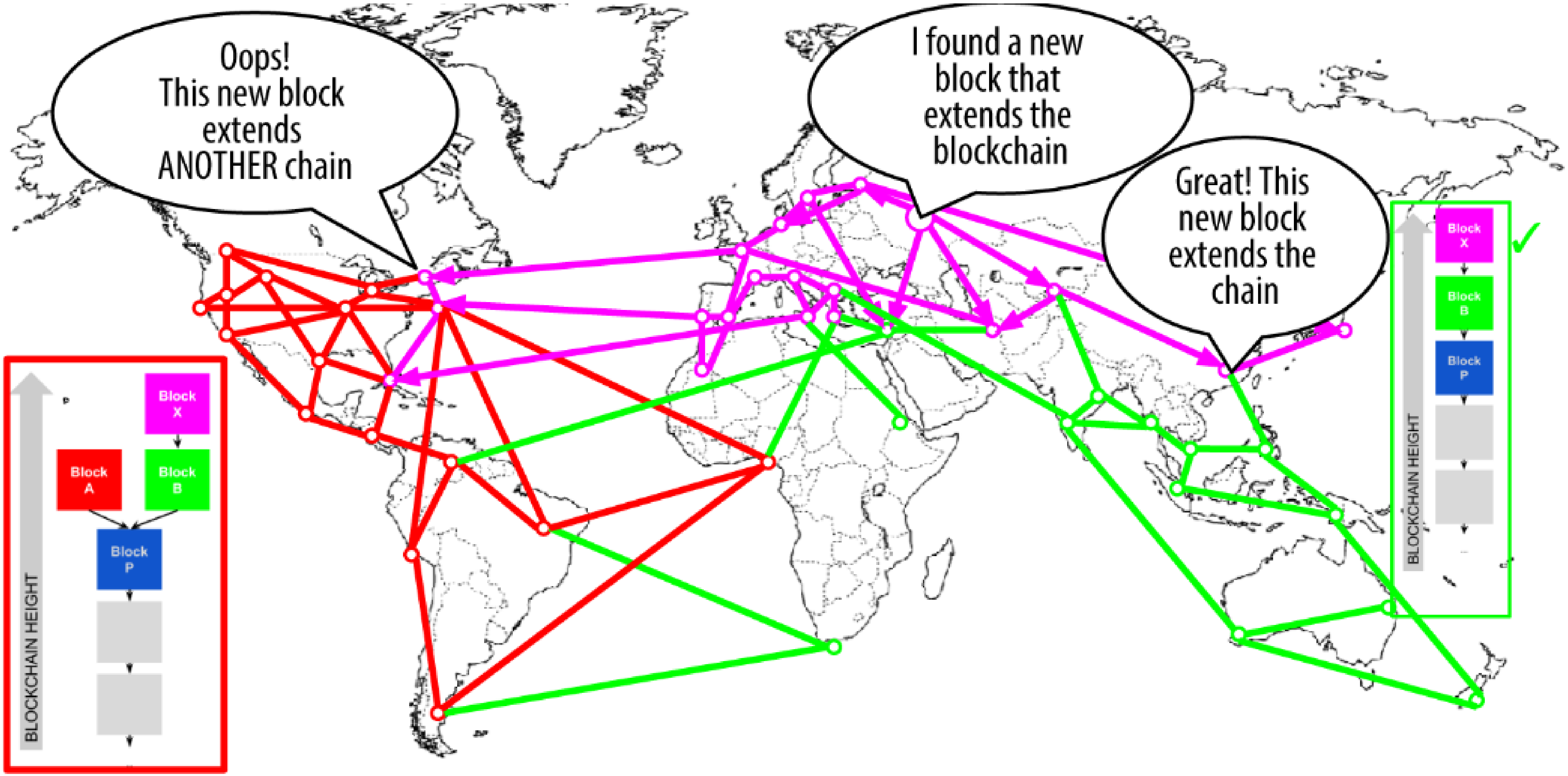
- Performing proof-of-work is called **Mining.**
- A person which do mining is called **Miner.**
- A miner can earn 12.5 BTC (≈ $ 10k) as a reward when she succeeds to find a valid nonce.



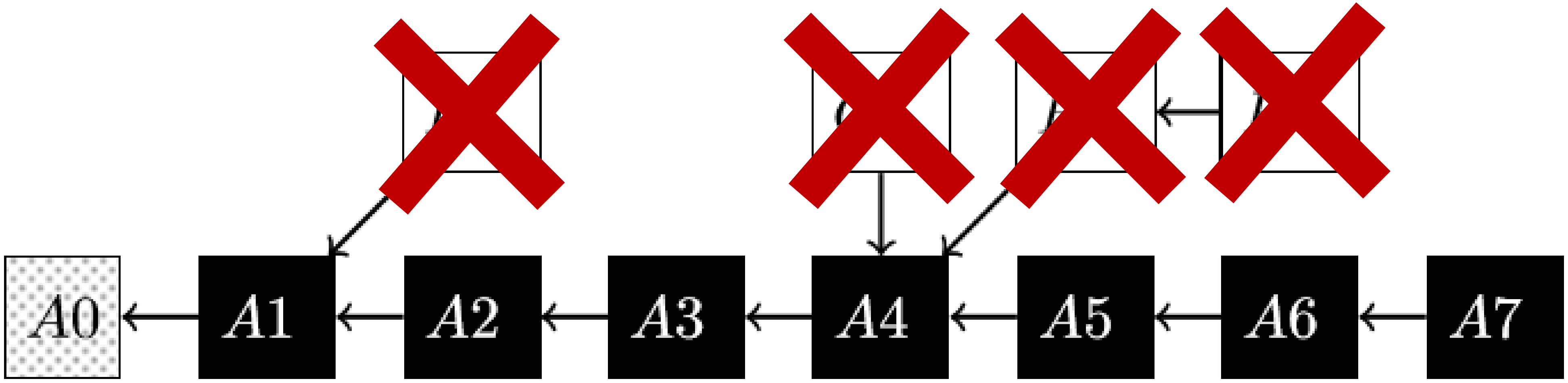
Step (Miner)

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes express their acceptance of the block by working on creating the next chain, using the hash of the accepted block as the previous hash.

Forks

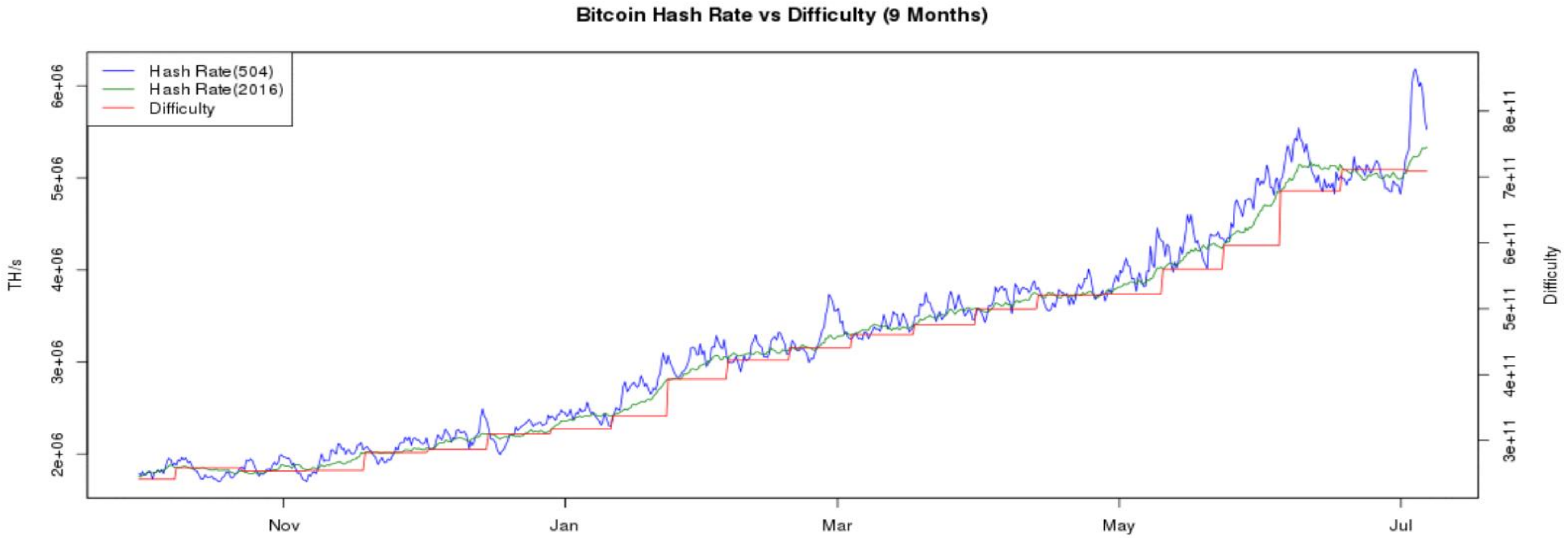

Oops!
This new block
extends
ANOTHER chain
I found a new
block that
extends the
blockchain
Great! This
new block
extends the
chain
BLOCKCHAIN HEIGHT
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block X
Block B
Block P
✓

Forks



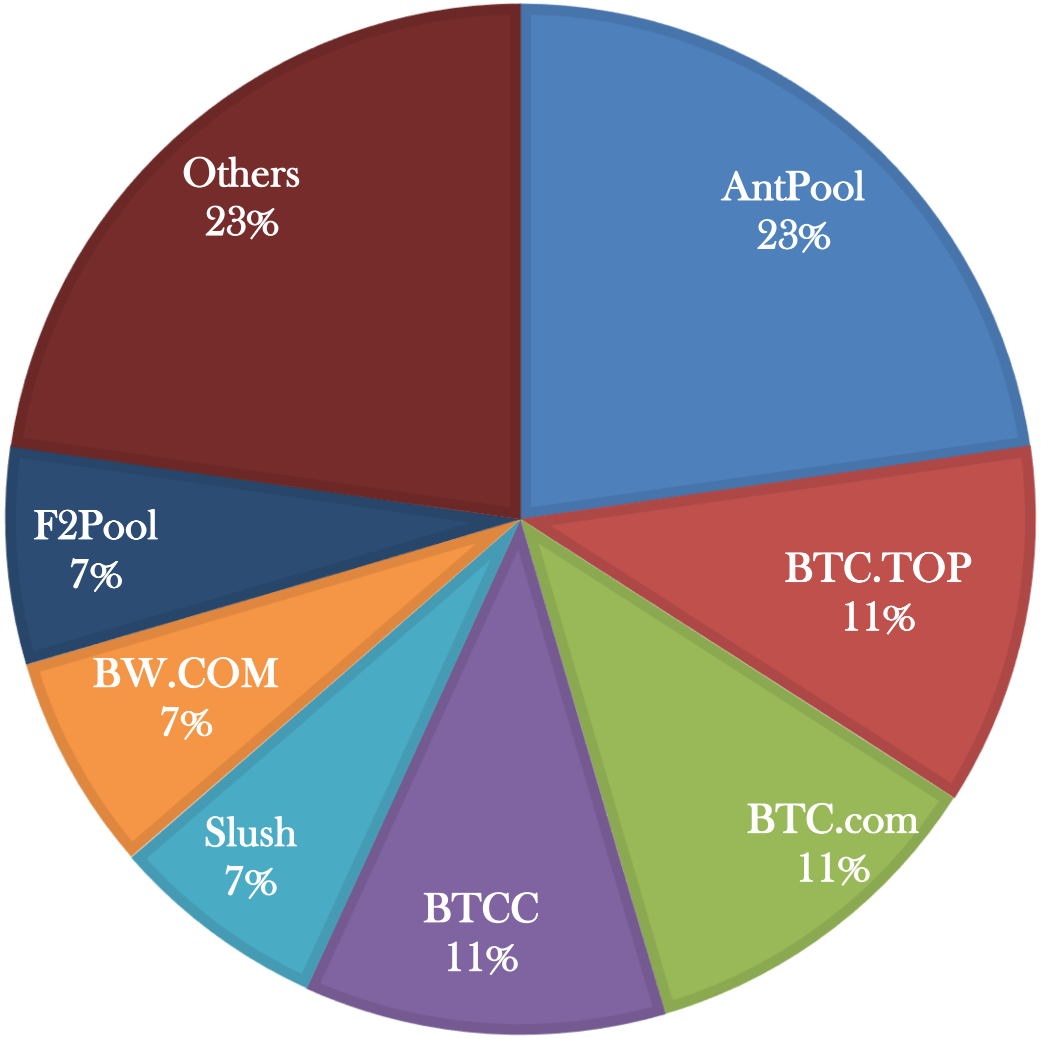
- Only one head is accepted as a valid one among heads.
- An attacker can generate forks intentionally by holding his found block for a while.

Mining Difficulty



- ❖ Bitcoin adjusts automatically the mining difficulty to be an average one round period 10mins.
- ❖ The difficulty increases continuously as computing power increases.

Mining Pool



- ❖ Many miners started to do mining together.
- ❖ Most mining pools consist of a manager and miners.
- ❖ Currently, most computational power is possessed in mining pools.

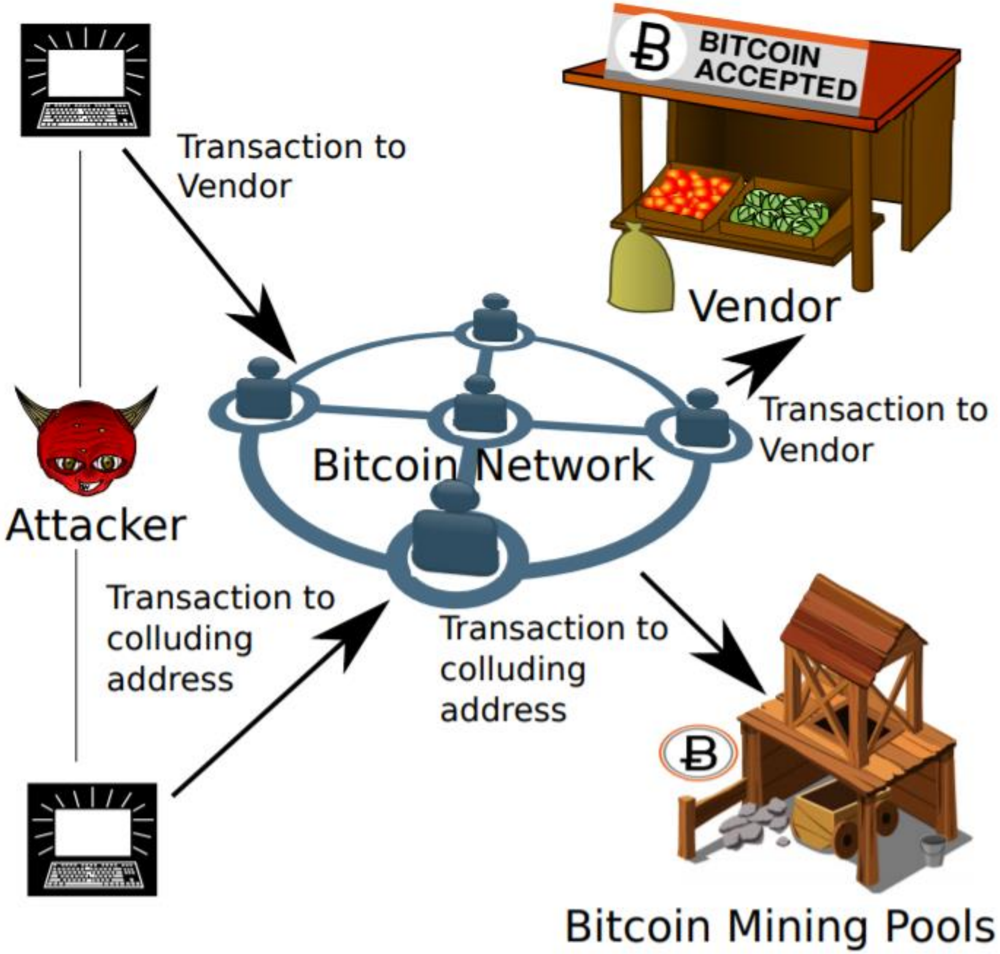
Security of Cryptocurrency

- Double spending
  - Double-Spending Fast Payments in Bitcoin: CCS 2012
- Anonymity (이전 발표)
  - Quantitative Analysis of the Full Bitcoin Transaction Graph: FC 2013
- (Peer-to-Peer) Network
  - Eclipse Attacks on Bitcoin's Peer-to-Peer Network: Usenix 2015
  - Low-Resource Eclipse Attackson Ethereum's Peer-to-Peer Network: ePrint 2018
  - Hijacking Bitcoin: Routing Attacks on Cryptocurrencies: SP 2017
- Mining
  - Miner's Dilemma: SP 2015
  - Fork after withholding (FAW) attacks: CCS 2017 (KAIST 논문)
- Scalability vs Security
  - Security and Performance of Proof of Work Blockchains: CCS 2016

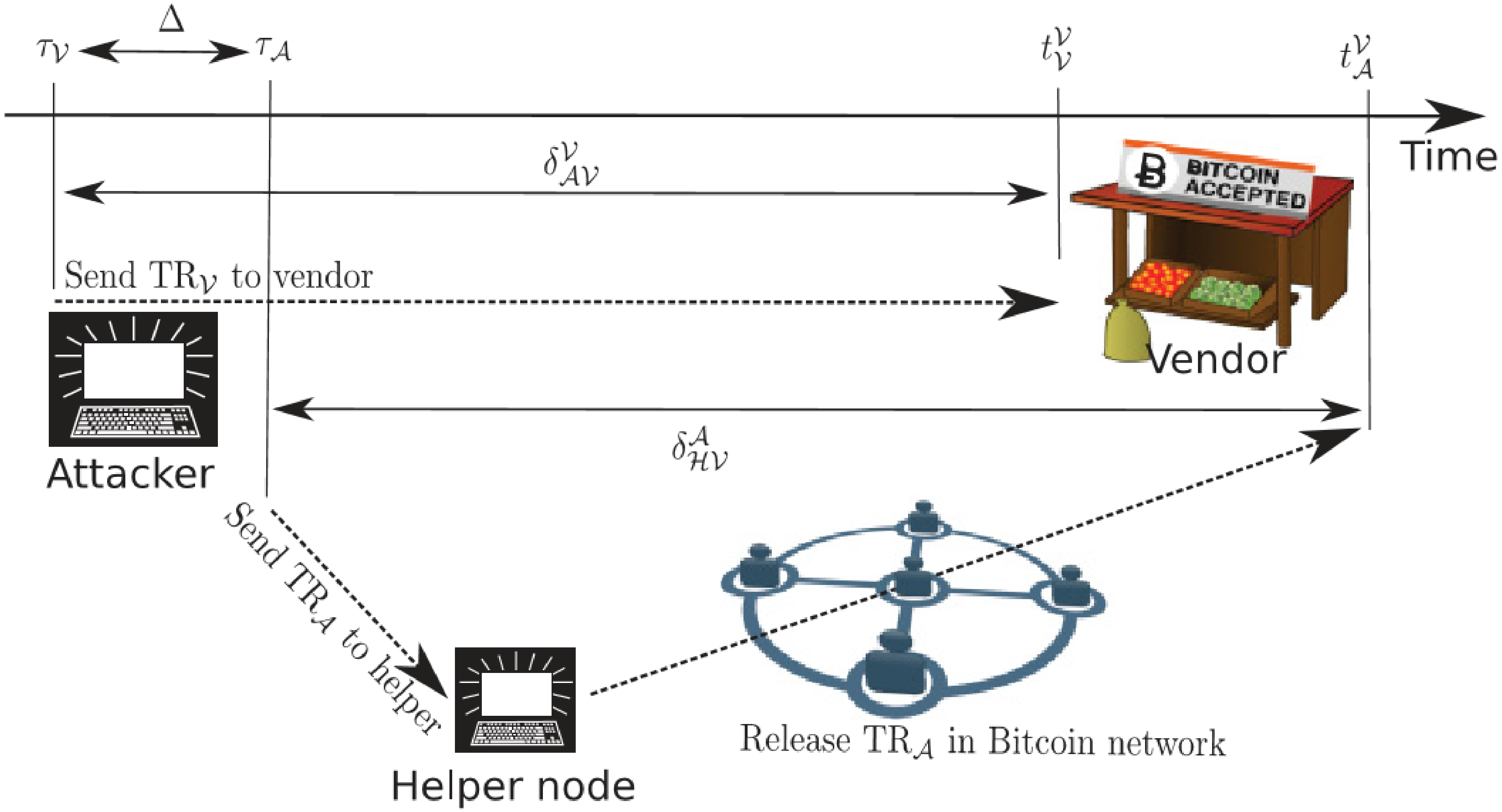
Double Spending Attack

How Can We Launch Double Spending?

- ❖ Key Point: Generate Forks
- ❖ In order that an attacker spends spent Bitcoin, the vendor should consider the Bitcoin is unspent.



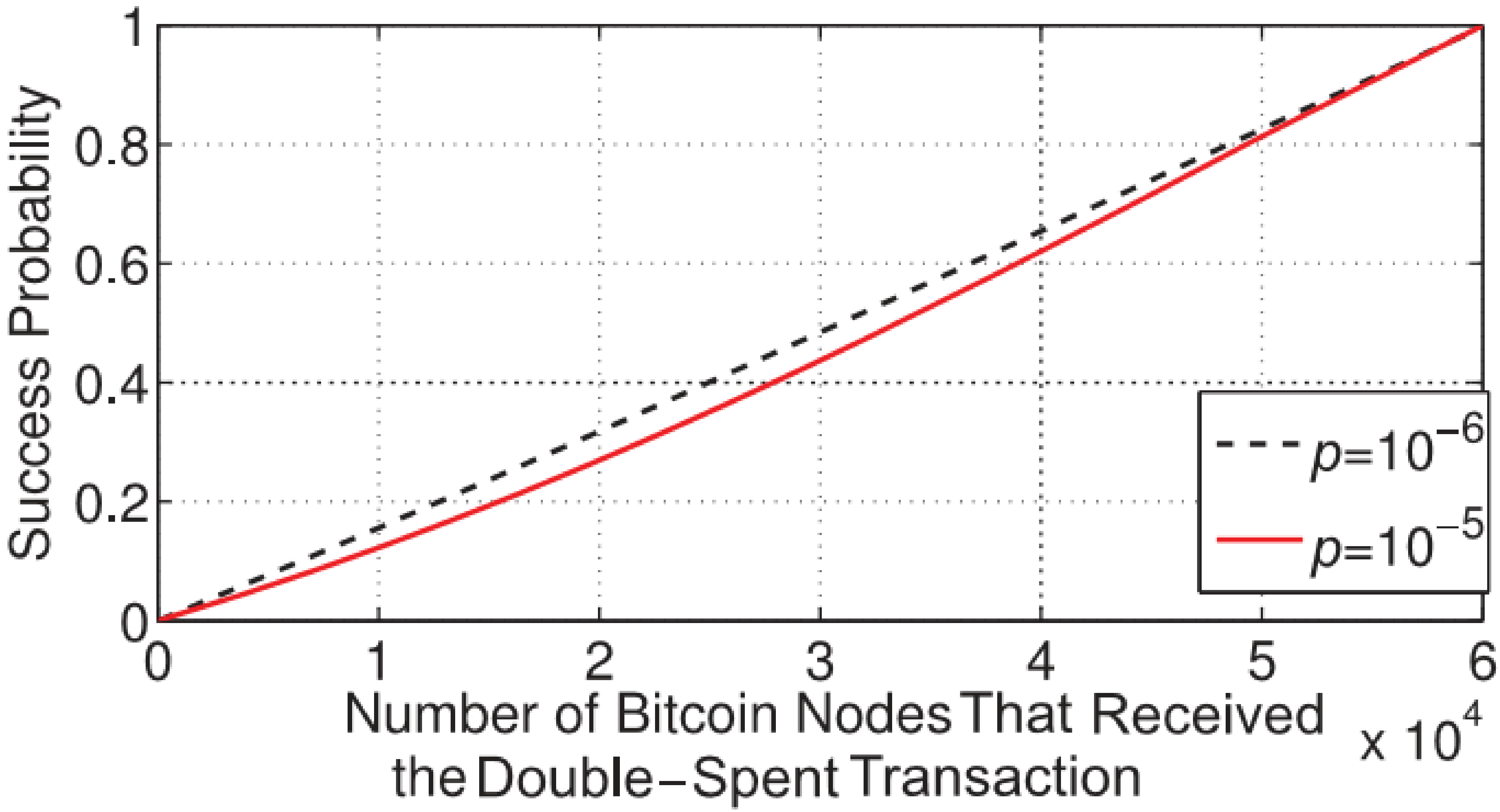
Necessary Conditions for Double-Spending



Δ
$\tau_{\mathcal{V}}$
$\tau_{\mathcal{A}}$
$t_{\mathcal{V}}^{\mathcal{V}}$
$t_{\mathcal{A}}^{\mathcal{V}}$
Time
$\delta_{\mathcal{AV}}^{\mathcal{V}}$
BITCOIN ACCEPTED
Send TR$_{\mathcal{V}}$ to vendor
Vendor
Attacker
$\delta_{\mathcal{HV}}^{\mathcal{A}}$
Send TR$_{\mathcal{A}}$ to helper
Helper node
Release TR$_{\mathcal{A}}$ in Bitcoin network

Fig. 3. Sketch of a double-spending attack on fast payments in Bitcoin. Here, the attacker $\mathcal{A}$ dispatches two transactions that use the same BTCs in the Bitcoin network. The double-spending attack is successful if the BTCs that $\mathcal{A}$ used to pay for $\mathcal{V}$ cannot be redeemed (i.e., when the second transaction is included in the upcoming Bitcoin block).

Performing Double Spending Attack



Eclipse Attack

Bitcoin Network

- Cryptographic authentication between peers is not used, and nodes are identified by their IP addresses.
- Each node uses a randomized protocol to select eight peers with which it forms long-lived outgoing connections, and to propagate and store addresses of other potential peers in the network.
- Nodes with public IPs also accept up to 117 unsolicited incoming connections from any IP address.

Propagating Network Information

- A DNS seeder is a server that responds to DNS queries from bitcoin nodes with a list of IP addresses for bitcoin nodes.
- ADDR messages, containing up to 1000 IP address and their timestamps, are used to obtain network information from peers.
- Nodes accept unsolicited ADDR messages.
- Peers store Public IPs in *tried* and *new* table.
  - Tried: unique addresses for peers to whom the node has successfully established an incoming or outgoing connection.
  - New: addresses for peers to whom the node has not yet initiated a successful connection.

Eclipse Attack

- Populates the tried table with addresses for its attack nodes
- Overwrites addresses in the new table with “trash” IP
- The attack continues until the victim node restarts and chooses new outgoing connections from the tried and new tables in its persistent storage
- With high probability, the victim establishes all eight outgoing connections to attacker addresses;
- Finally, the attacker occupies the victim’s remaining 117 incoming connections.

The BWH Attack

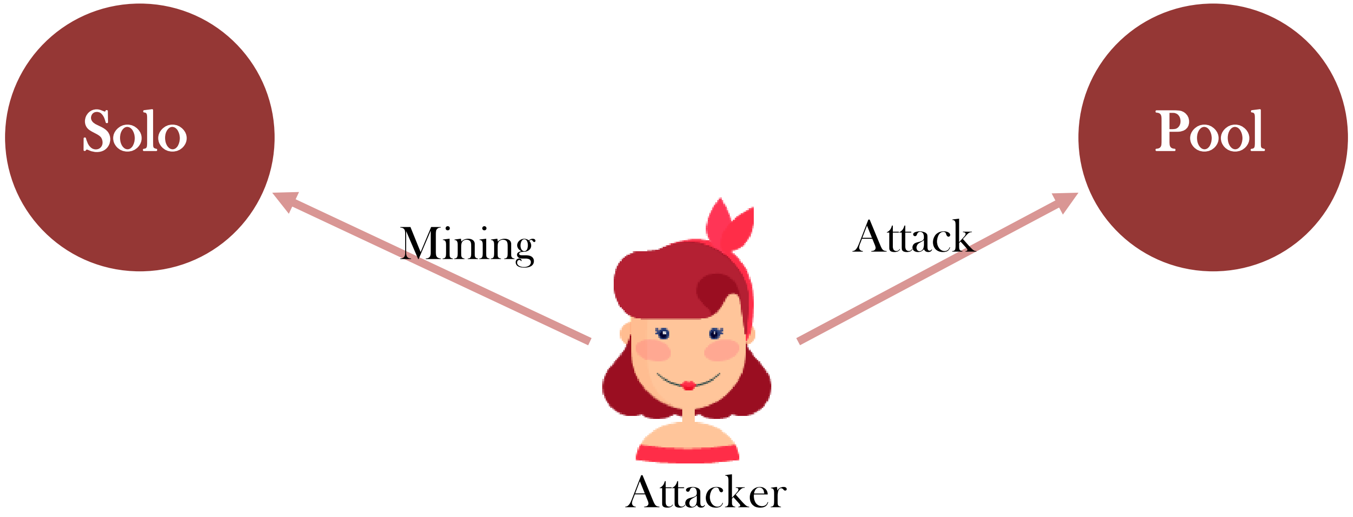
The History of the BWH Attack

- 2011: Analysis of Bitcoin Pooled Mining Reward Systems
  - “This has no direct benefit for the attacker, only causing harm to the pool operator or participants. ”
- 2014 : On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency
  - “They showed that an attacker can earn profit by this attack”
  - In june 2014, Eligius pool made a loss because of the BWH attack.
- 2015 : The miner’s dilemma

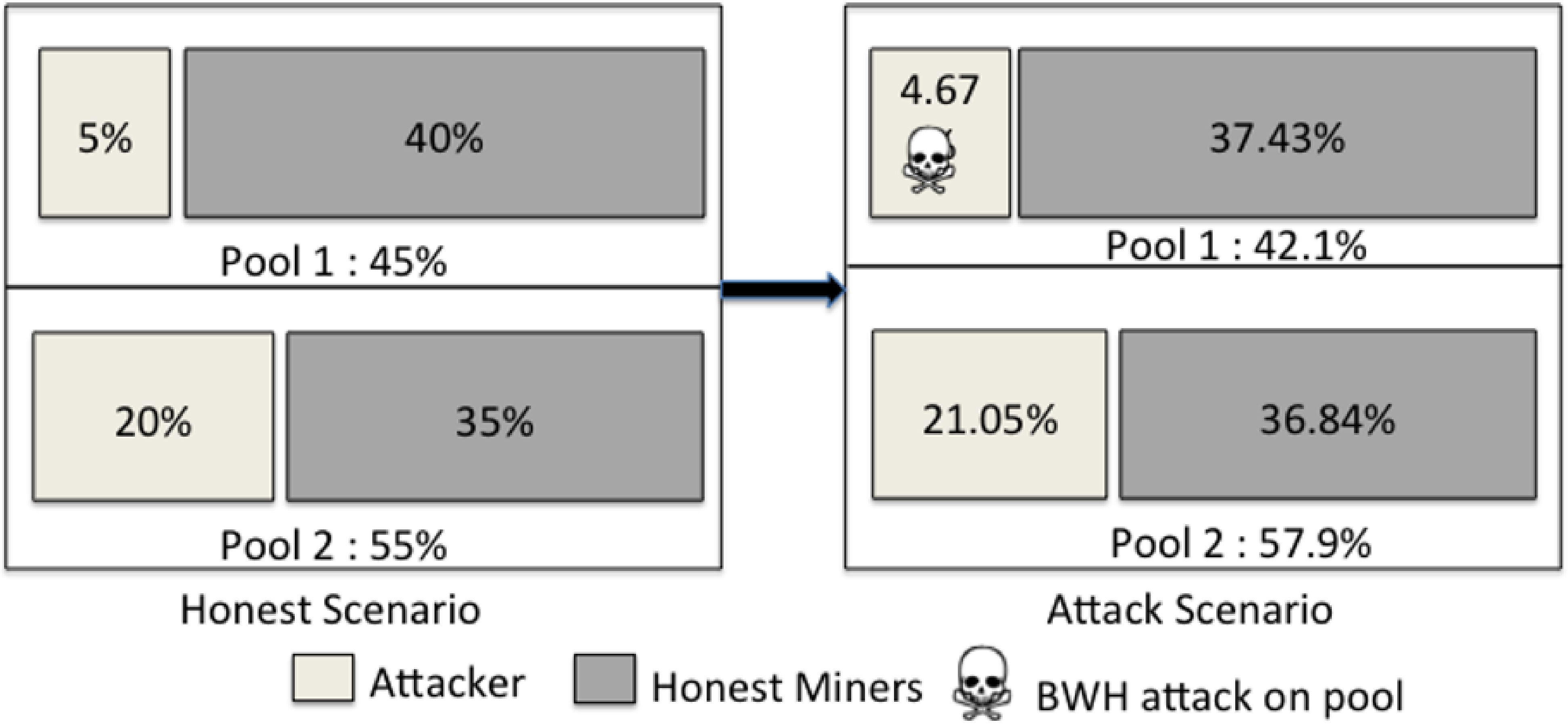
  On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining
  - Attack strategy && game theory

BWH Attack

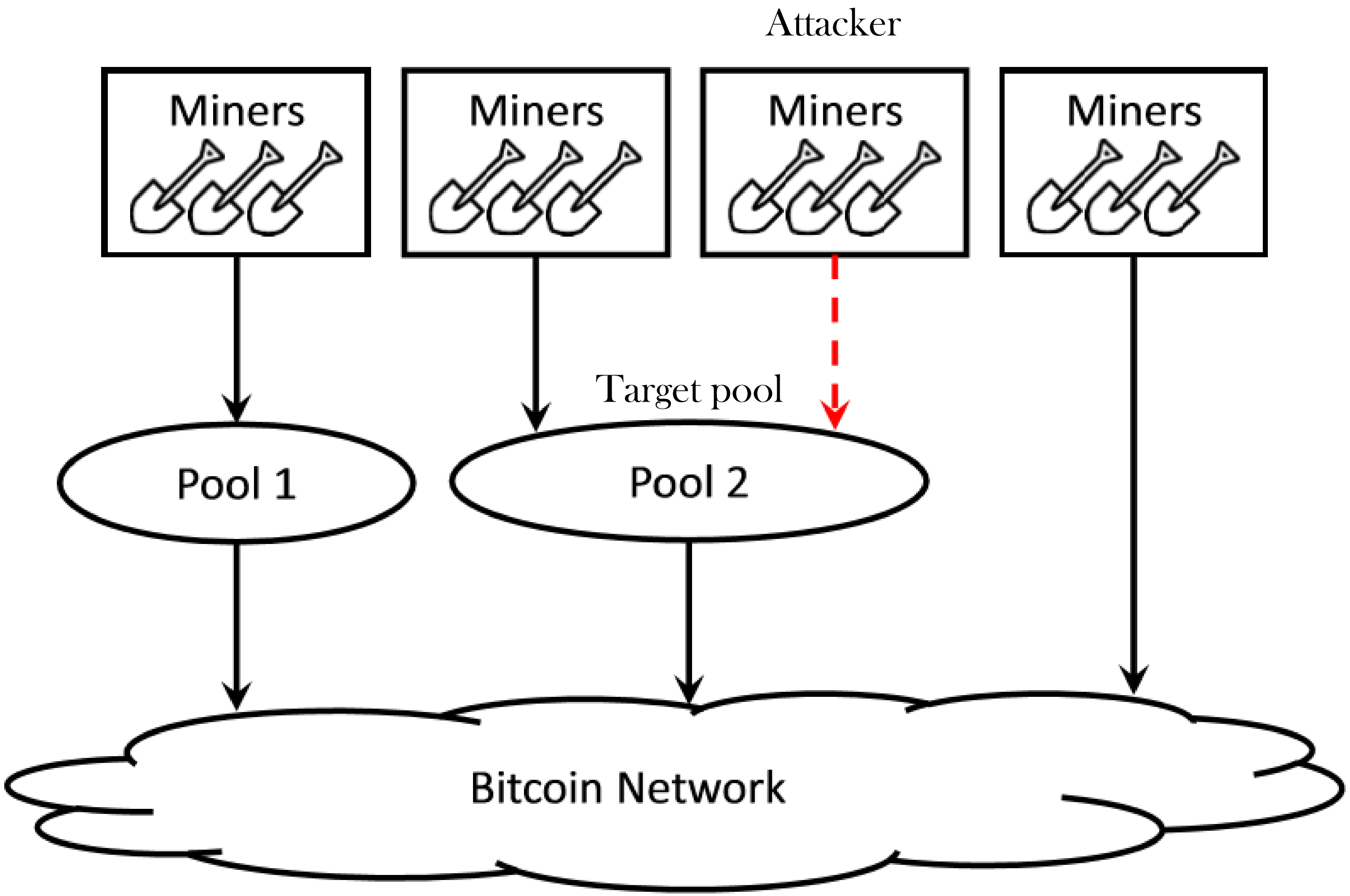
- An attacker joins the target pool.
- She receives unearned wages while only pretending to contribute work in the pool.
- She submits the share which contains only partial solution but not the perfect solution.
- She should split her computational power into solo mining and malicious pool mining.



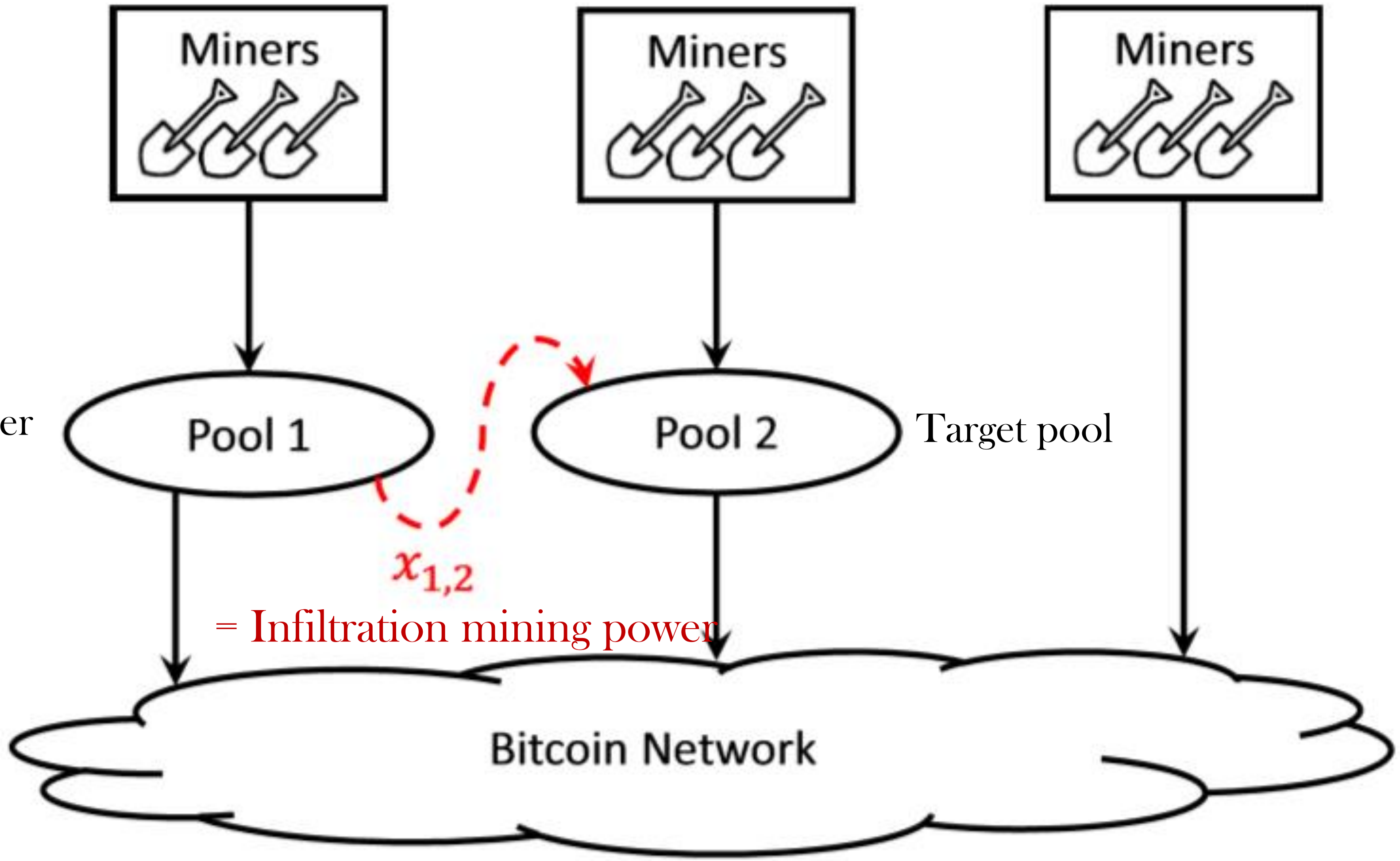
BWH Attack


5%
40%
Pool 1 : 45%
20%
35%
Pool 2 : 55%
Honest Scenario
4.67
37.43%
Pool 1 : 42.1%
21.05%
36.84%
Pool 2 : 57.9%
Attack Scenario
Attacker
Honest Miners
BWH attack on pool

Classical BWH attack



BWH attack among pools

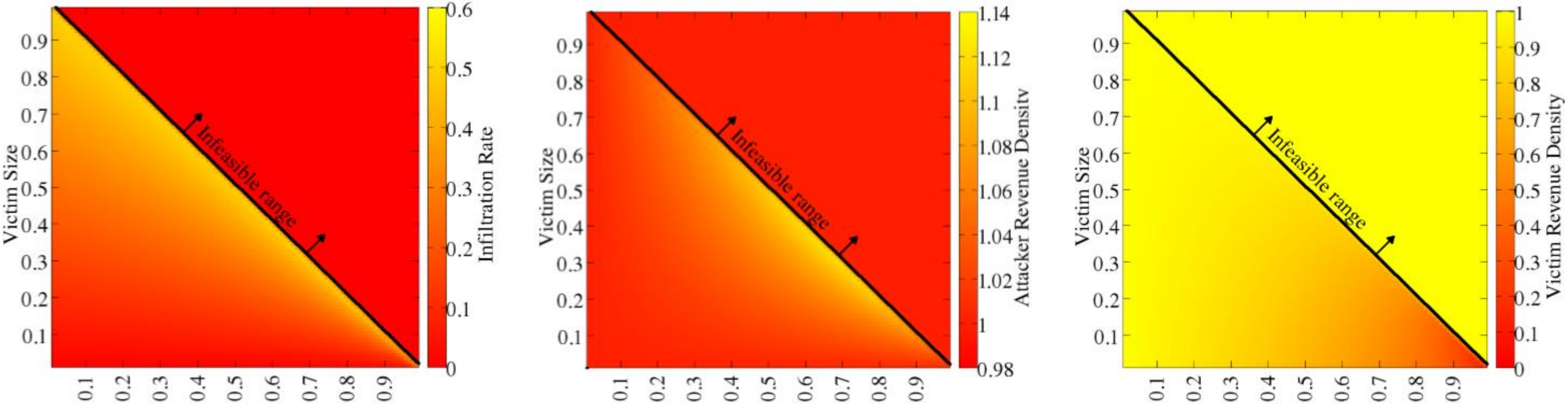


Attacker

Target pool

$x_{1,2}$ = Infiltration mining power

Result



(a) $x_{1,2}$

Infiltration mining power

(b) r_1

Attacker relative reward

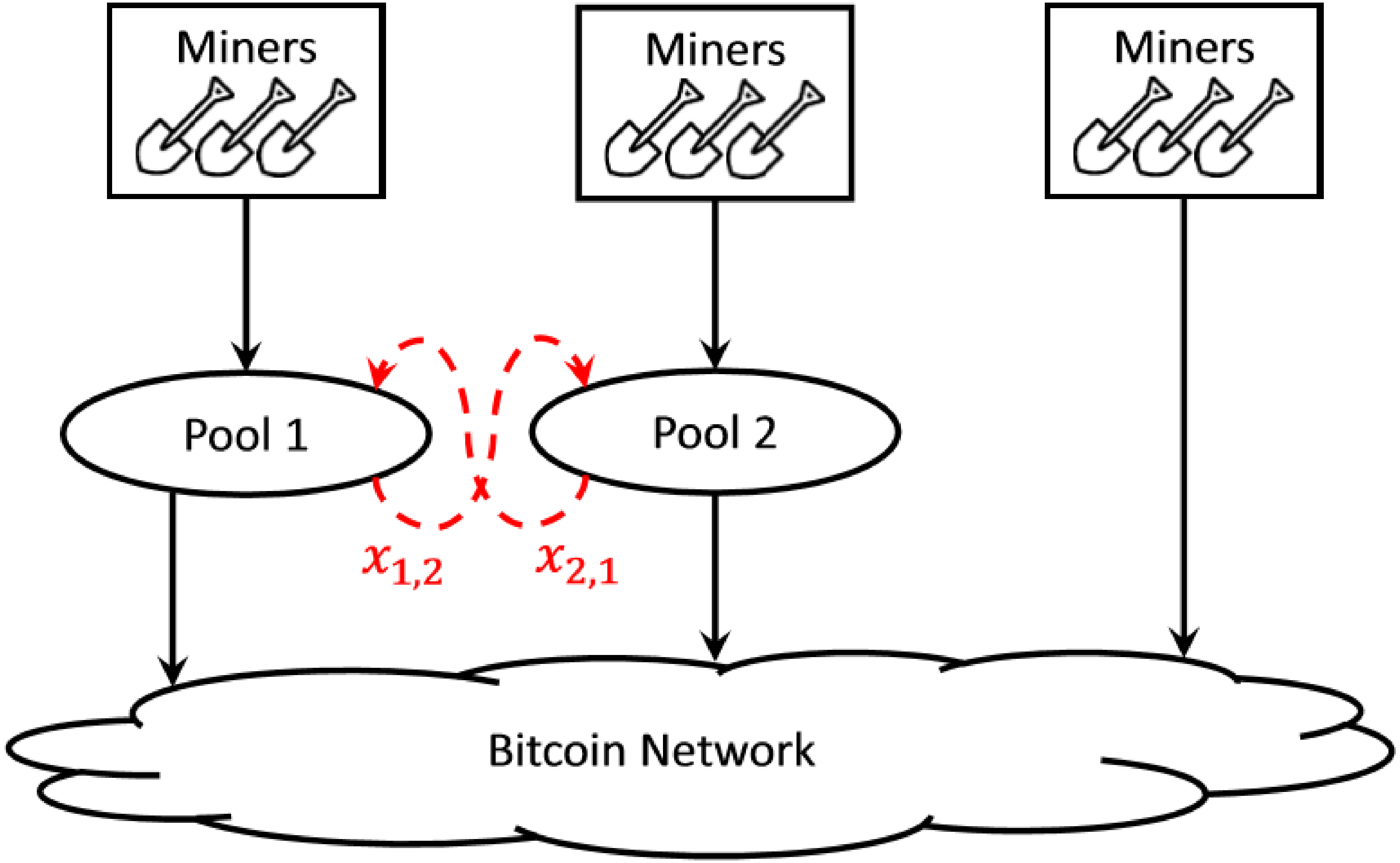
(c) r_2

Victim relative reward

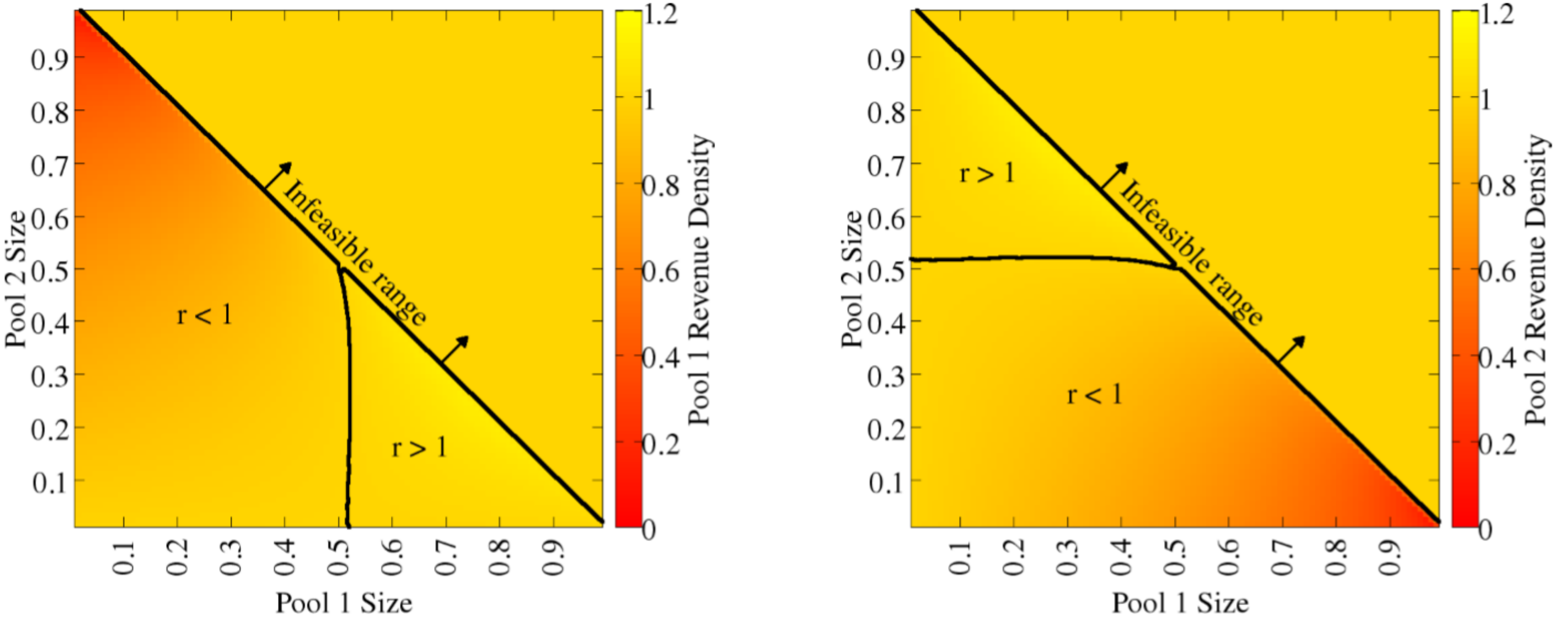
❖ The BWH attack is always profitable.

Between Two Pools

- ❖ Rational two pools can launch the BWH attack each other.
- ❖ It leads to a BWH attack game.



Result

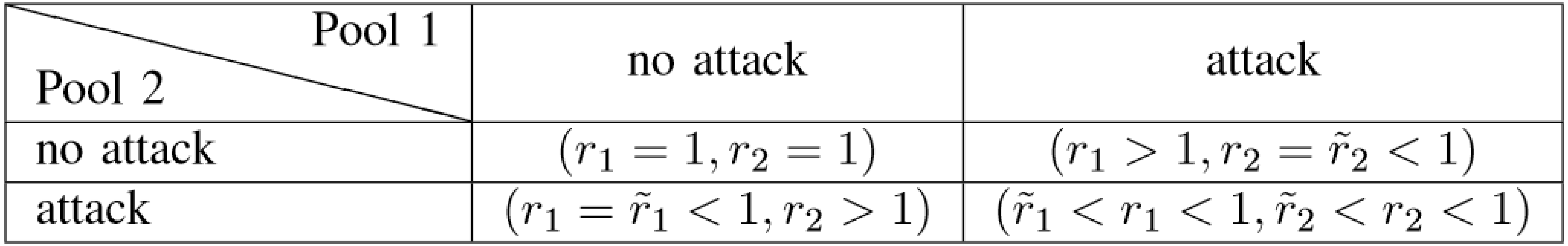


(c) r_1

(d) r_2

- ❖ When they executes the BWH attack each other, both of them make a loss.

Miners' dilemma

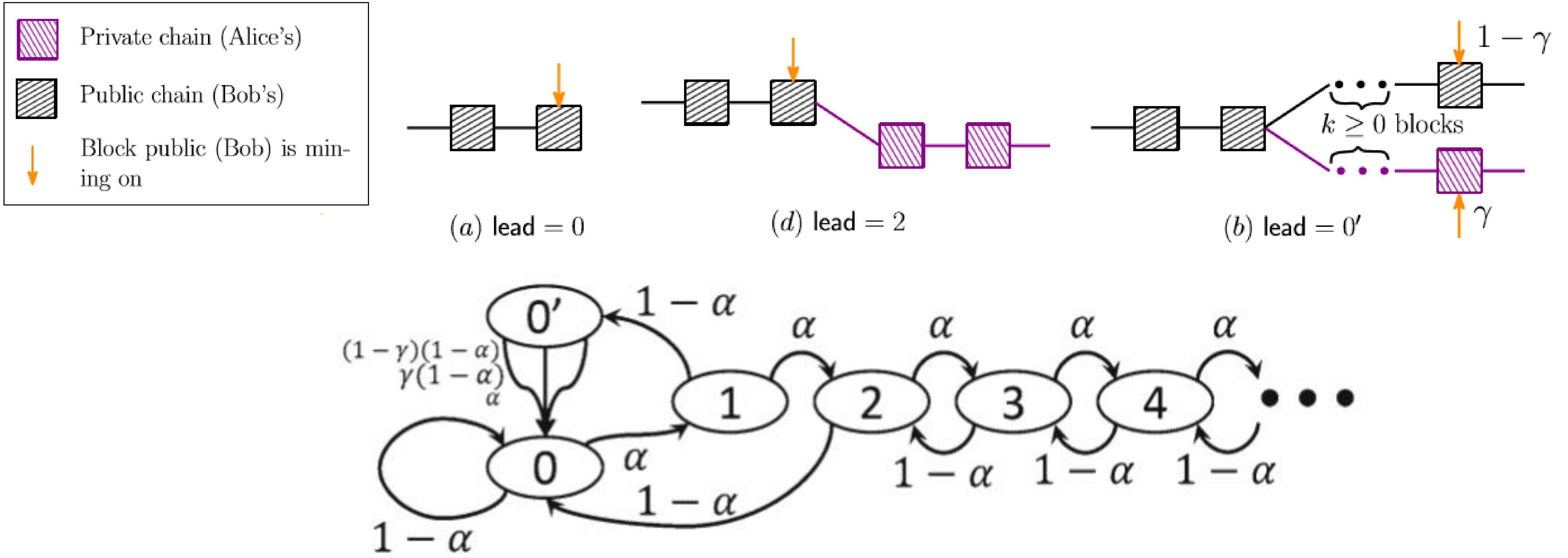


Pool 1 Pool 2	no attack	attack
no attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

- ❖ The equilibrium revenue of the pool is inferior compared to the no-pool attacks scenario.
- ❖ This is equivalent to the prisoner's dilemma.
- ❖ The fact that the BWH attack is not common may be explained by modeling the attack decisions as an iterative prisoner's dilemma.

The FAW Attack

Selfish Mining



(a) lead $= 0$ (d) lead $= 2$ (b) lead $= 0'$

❖ Generate intentional forks adaptively.

❖ Force the honest miners into performing wasted computations on the stale public branch.

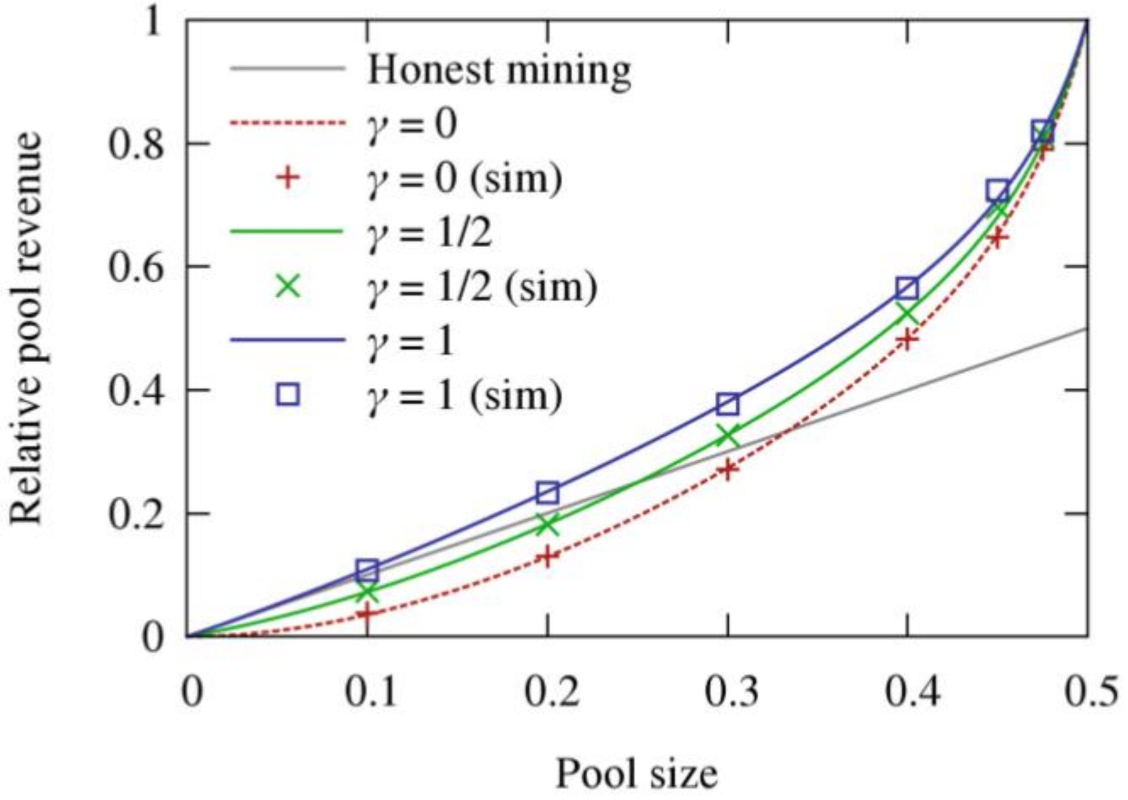
Eyal and Sirer. "Majority is not enough: Bitcoin mining is vulnerable." Financial Crypto, 2014.

Selfish Mining

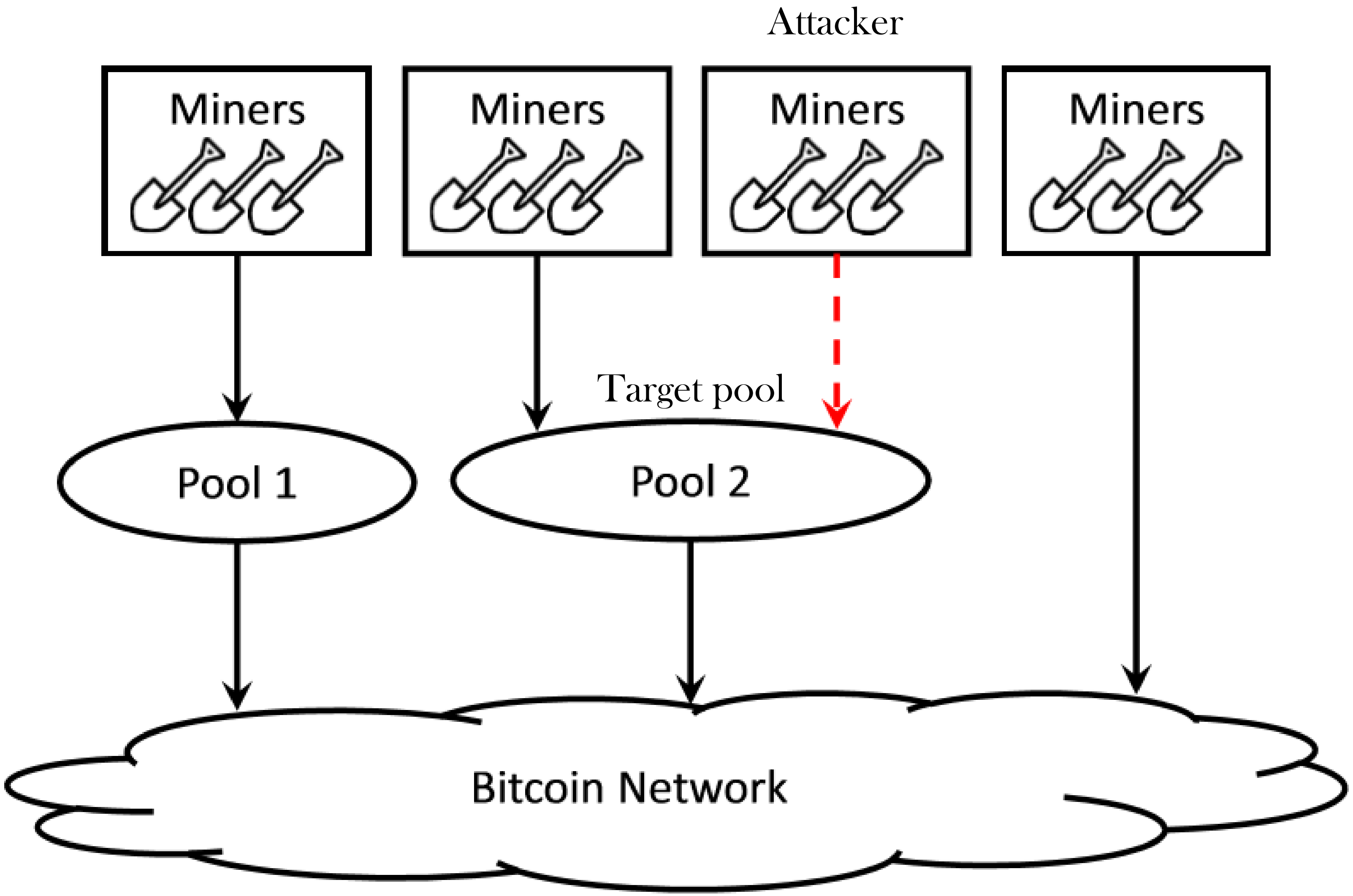
- ❖An attacker can earn the extra reward according to her network capability.

- ❖For example, if an attacker possesses 20% computational power, she can earn the extra reward $6M at most.

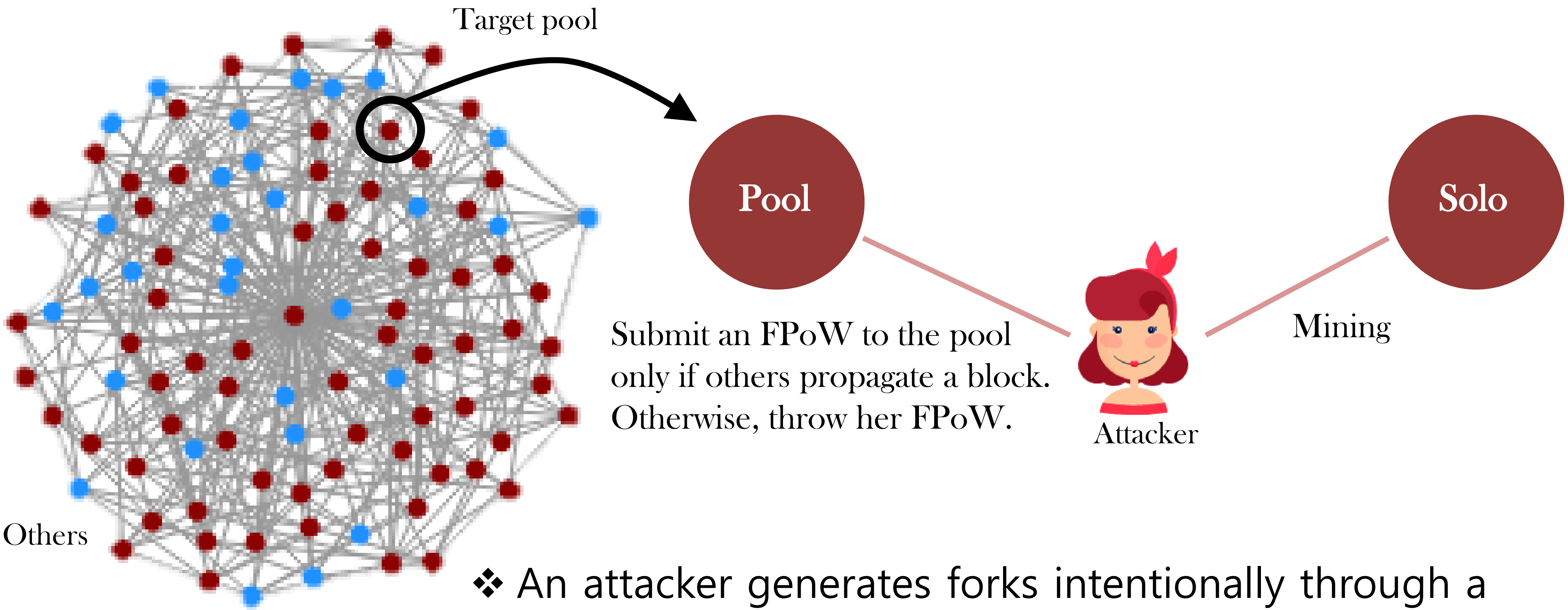
- ❖However, it is not practical.



FAW Attack


Attacker
Miners
Miners
Miners
Miners
Target pool
Pool 1
Pool 2
Bitcoin Network

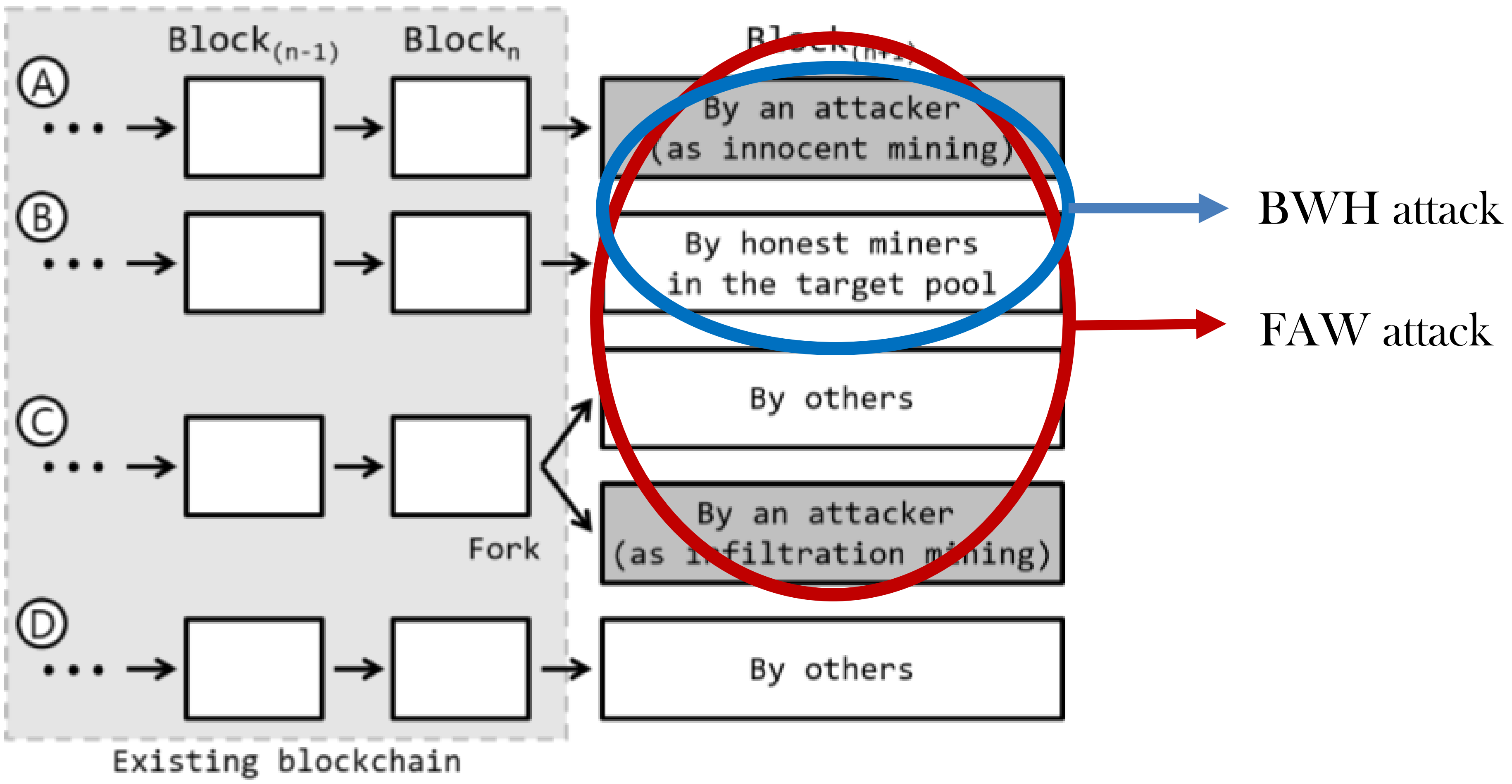
FAW Attack



Submit an FPoW to the pool only if others propagate a block. Otherwise, throw her FPoW.

- ❖ An attacker generates forks intentionally through a pool!

FAW Attack Against One Pool



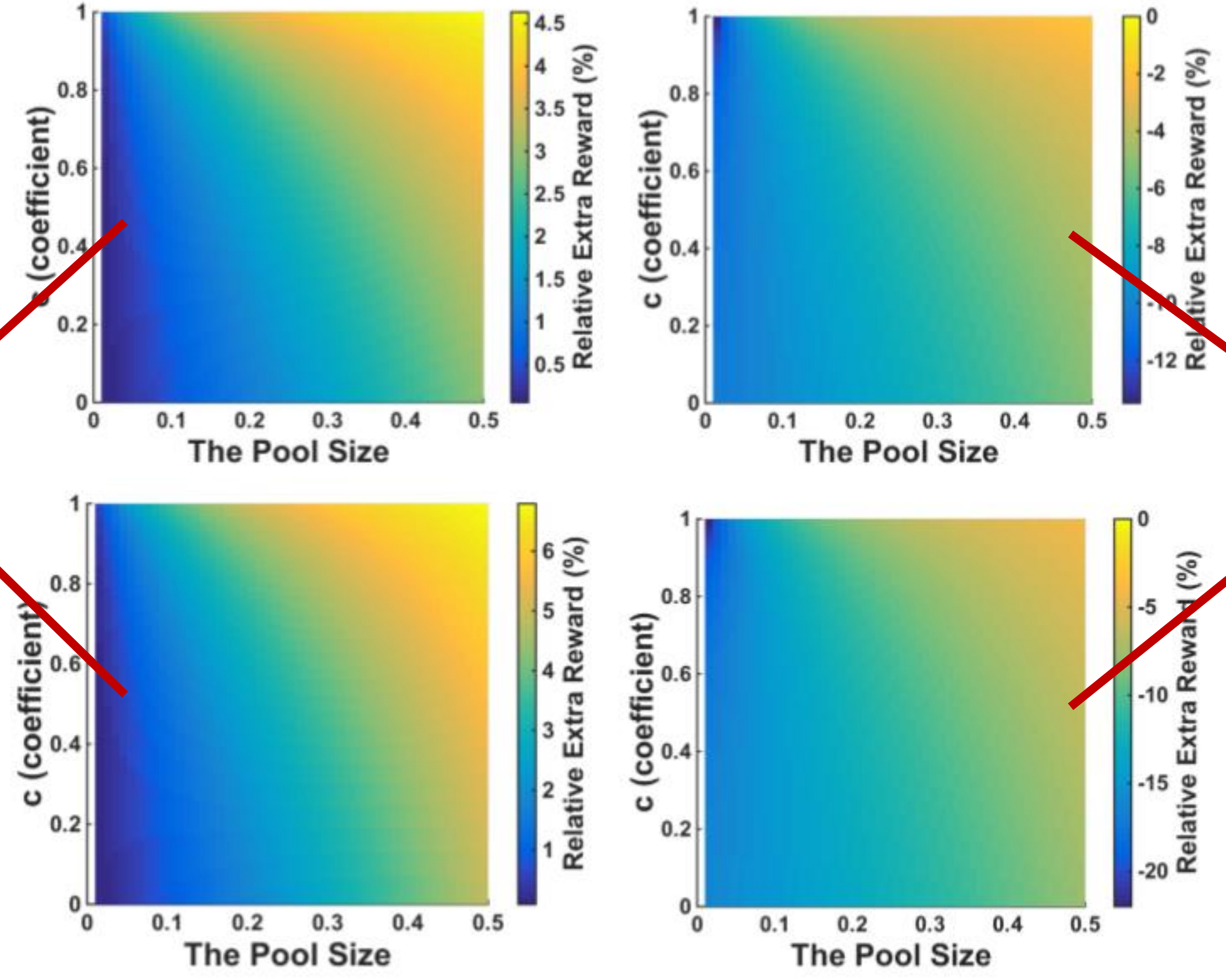
BWH attack

FAW attack

Result

Attacker

Victim



Always positive

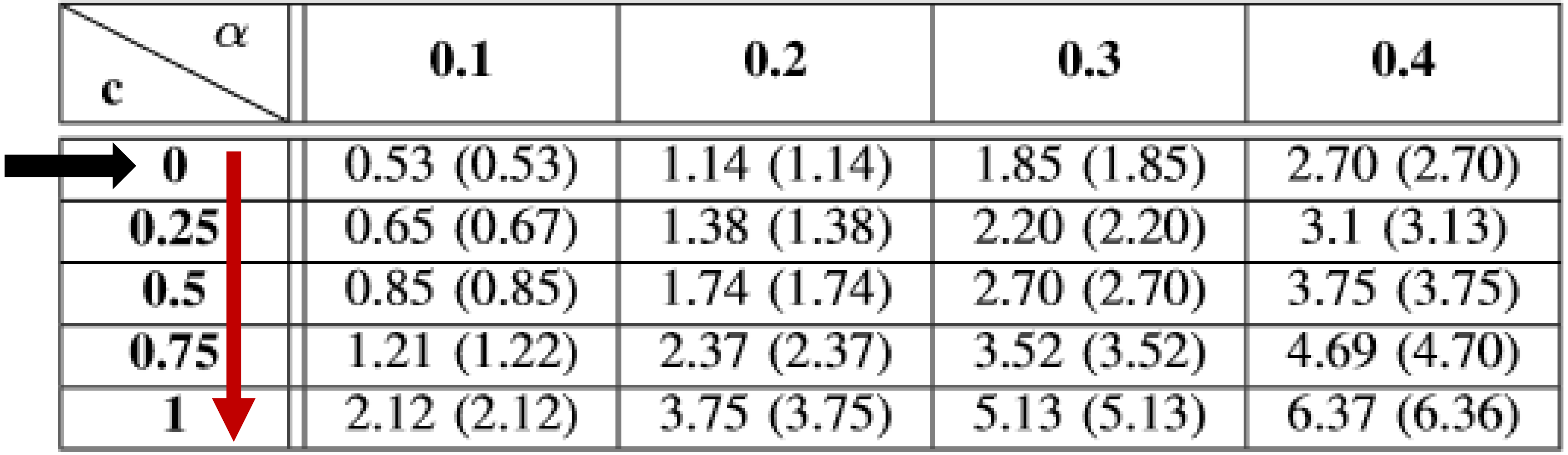
Always negative

- ❖ An attacker with 0.2 power

- ❖ An attacker with 0.3 power

Result

Increasing



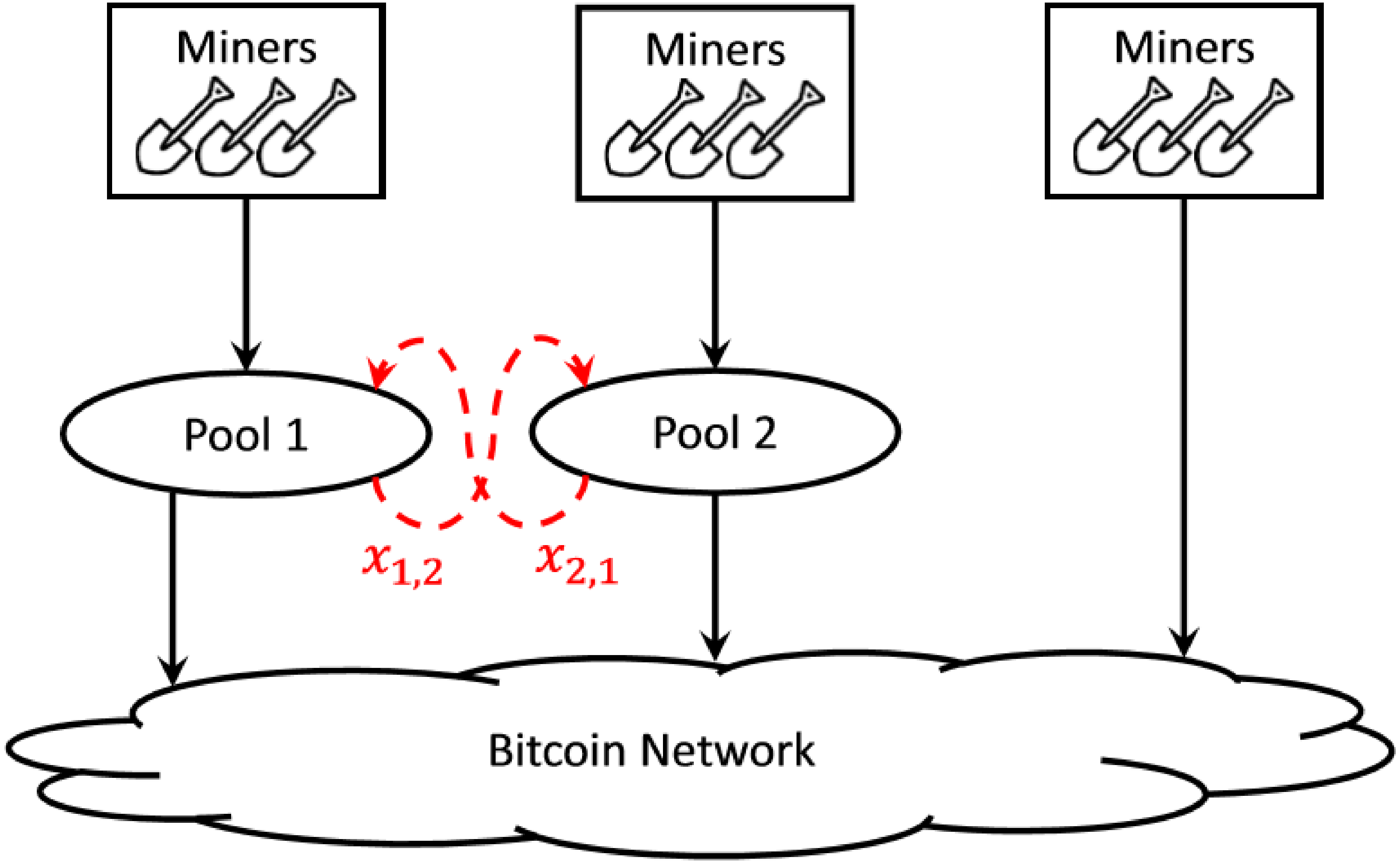
α c	0.1	0.2	0.3	0.4
0	0.53 (0.53)	1.14 (1.14)	1.85 (1.85)	2.70 (2.70)
0.25	0.65 (0.67)	1.38 (1.38)	2.20 (2.20)	3.1 (3.13)
0.5	0.85 (0.85)	1.74 (1.74)	2.70 (2.70)	3.75 (3.75)
0.75	1.21 (1.22)	2.37 (2.37)	3.52 (3.52)	4.69 (4.70)
1	2.12 (2.12)	3.75 (3.75)	5.13 (5.13)	6.37 (6.36)

The case is equivalent to the case of the BWH attack

Increasing

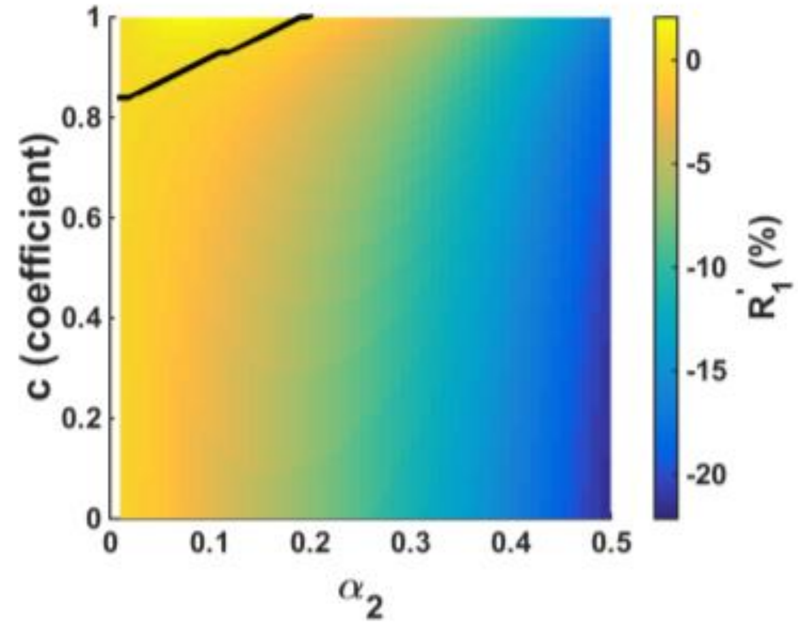
- ❖ We simulated an FAW attack against one pool which possesses a computational power of 0.2, using a Monte Carlo method.

FAW Attack Game

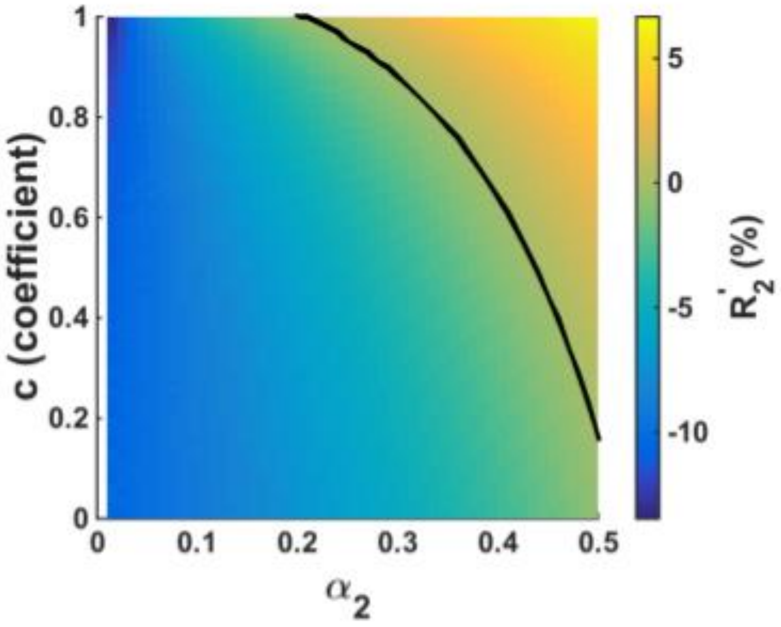


Result

Pool 1’s extra reward

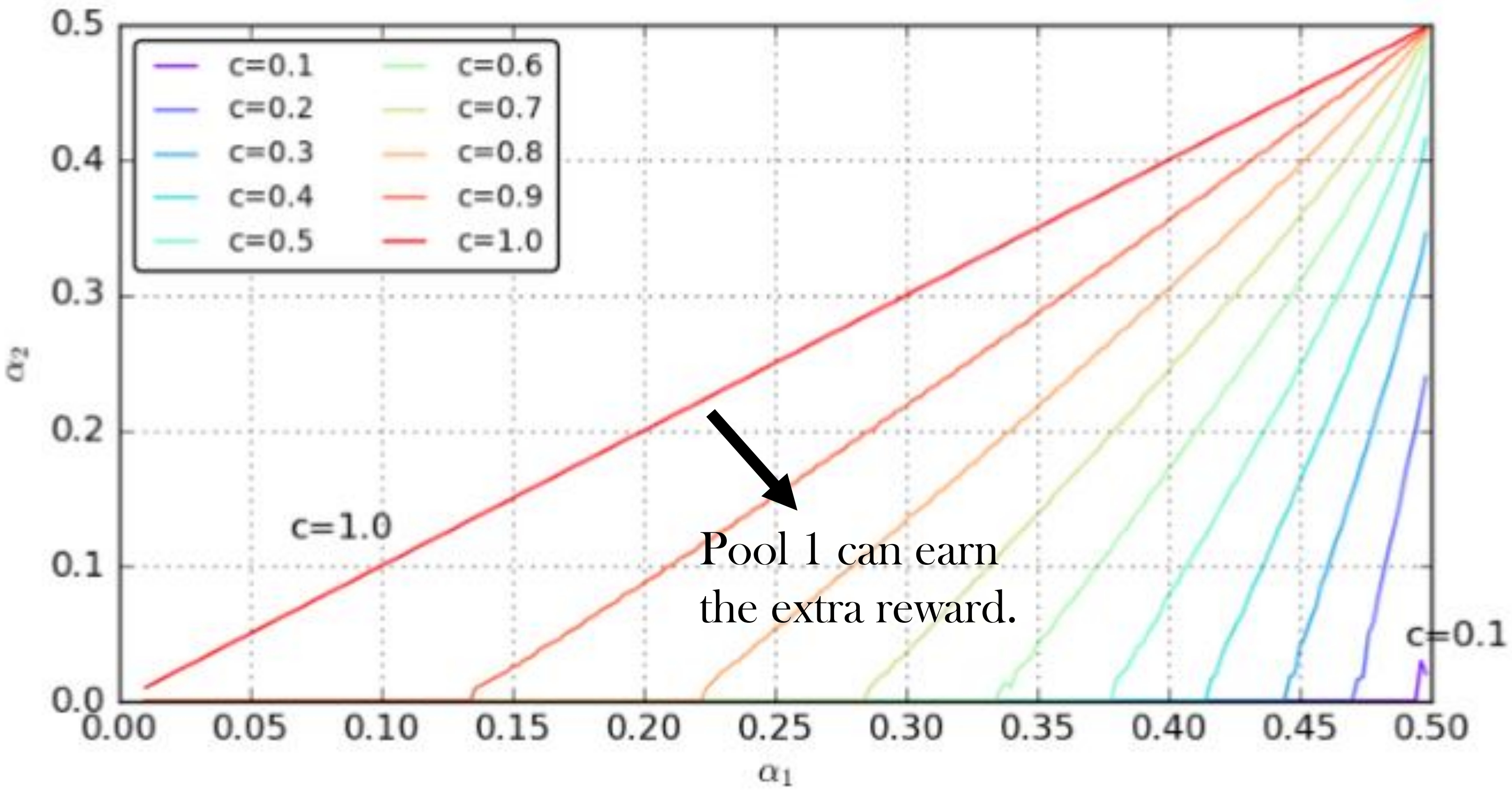


Pool 2’s extra reward



- ❖ Pool 1 possesses 0.2 computational power.
- ❖ The bigger pool can earn the extra reward unlike the miner’s dilemma.

Break Dilemma



❖ The FAW attack game leads to a pool size game: the larger pool can always earn the extra reward.

The DAO 공격 사례

- The DAO : 탈중앙화 자율조직을 구현한 스마트 컨트랙트
  - 투자자들이 보유한 DAO Token을 바탕으로 의결권 행사
  - 전세계에서 약 2천억원의 투자금 모집
  - DAO Token을 Ether(이더리움 화폐)로 환급하는 코드에 취약점 존재 (약 750억 상당의 해킹 피해)

- Attack Example 1
  1. DAO 출금 기능을 악용하는 스마트 컨트랙트 작성 및 호출
  2. 공격자 계좌에 입금 발생 시, DAO에 출금 요청
  3. DAO 출금으로 공격자 계좌에 입금 발생
  4. 잔액 업데이트 전에 2) 3) 과정의 무한 Loop 생성되어 무한 출금

- Attack Example 2
  1. 공격자 계좌에 1 wei 입금
  2. 'Attack Example 1' 응용하여 1 wei 두번 출금
  3. Underflow에 의해서 잔고가 2^256 – 1 wei 로 변환
  4. 잔고 출금

스마트 컨트랙트 취약점 연구

연구명	Making Smart Contracts Smarter	ZEUS: Analyzing Safety of Smart Contracts
출처	CCS 2016	NDSS 2018
목적	자동화 도구를 이용하여 이더리움의 취약한 스마트 컨트랙트 탐지	자동화 도구를 이용하여 이더리움의 취약한 스마트 컨트랙트 탐지
공격	4 종류 공격 - Reentrancy - Unchecked send - Block state dependence - Transaction order dependence	7 종류 공격 - (기존 4종류) - Failed send - Integer overflow/underflow - Transaction state dependence
취약점 점검결과	8,833 / 19,366 (46%) 취약	21,281 / 22,493 (94.6%) 취약 (1524 unique contract)

결론

- 가장 성숙한 기술인 Bitcoin과 Etherium에도 끝없는 취약점
- 다른 암호화폐 및 블록체인들도 비슷
  - Cryptographic vulnerabilities in IOTA
  - Mind Your Credit: Assessing the Health of the Ripple Credit Network, WWW 2018
- 블록체인 및 암호화폐 기술은 앞으로도 끊임없이 취약점 발견, 패치, 수정, 재설계 등의 Cycle을 따라갈 듯.
- 새로운 기술들의 등장
  - Algorand: scaling Byzantine agreements for cryptocurrencies, SOSP'17
- 기술 평가의 중요성!
  - 가치만큼 기술 또한 가변성이 크다!
  - 끊임 없는 기술 평가의 전쟁이 다가올 것으로 예상

Thank You!

https://syssec.kaist.ac.kr