Blockchain Future Society

Heung-No Lee

GIST, South Korea

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

Facebook/Publication ID: Heung-No Lee

You can download this lecture note from slideshare.net!

Flow of talk

- Birth of Bitcoin, any meaning?
- Bitcoin and blockchain, how does it work?
- What does Ethereum do?
- Possible applications of blockchains
- ICO and cryptoeconomics
- Policies around the world
- Speakers Invited
- Summary

Economy, Currency, Government

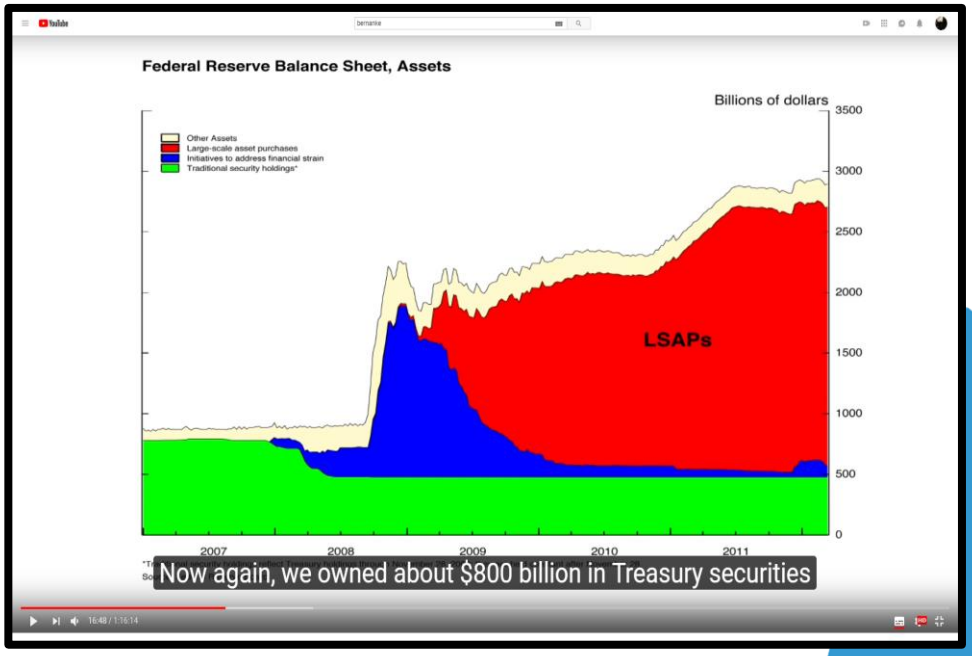
- People want an *ever improving state of self* and economic position compared to what they have enjoyed in previous years.

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

Financial Crisis, FED and LSAPs

>Financial Panic 07 ~ 08
>Housing bubble popped!
>Fed began lowering interest rate.
> Housing and Economic Recovery Act of 2008
>Bankruptcy of Lehman Brothers
>Too Big to Fail Problem
>> Fed saves AIG, Goldman Sachs, Morgan Stanley

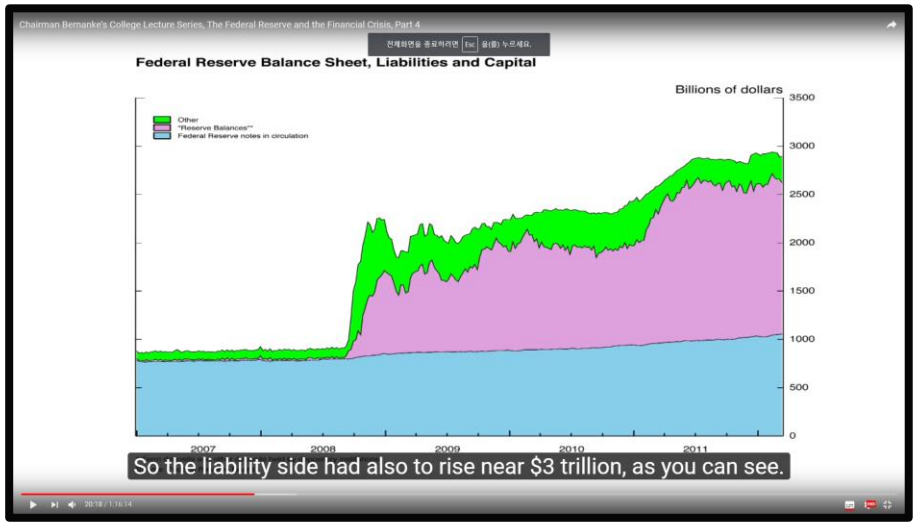
>Large Scale Asset Purchases (QE)
- Control long-term supplies of securities
- Raising the price of these assets
- Lowering the long term interest rate.



How did they pay for LSAPs?

the liability side had also to rise near $3 trillion… But as a literal fact, the Fed is not printing money to acquire these securities. The amount of currency in circulation has not been affected by these activities. What has been affected is the purple area. Those are the accounts that banks, commercial bank, holds with the FED. They are part of what's called the monetary base. But again, they are not – they certainly aren't cash.

Watch for yourself right here.



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.

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.

I am the 1%. Let's talk.

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

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

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

조회수 1,265,631회 2.9만 2천 공유 저장 ...

At the birth of Bitcoin, there were many issues which made us to think!

- Today, currency is not money.
  - USD does not have any internal value (No more gold standard).
  - Currency is created by banks when someone takes out a loan or government issues bonds (I.O.U.) to banks, or by increasing an electronic balance to the commercial banks at the whim of FED.
- With frequent financial crises, trust to gov. has been greatly tarnished.
  - People are grown wary of budget deficit and currency expansion.
- Issues around bitcoin are
  - Decentralization
  - Reforming Wall Street
  - Unbundling big corporations
  - Reducing inequality

Birth of Bitcoin
Trust enabled by peers

Bitcoin: A Peer-to-Peer Electronic Cash System

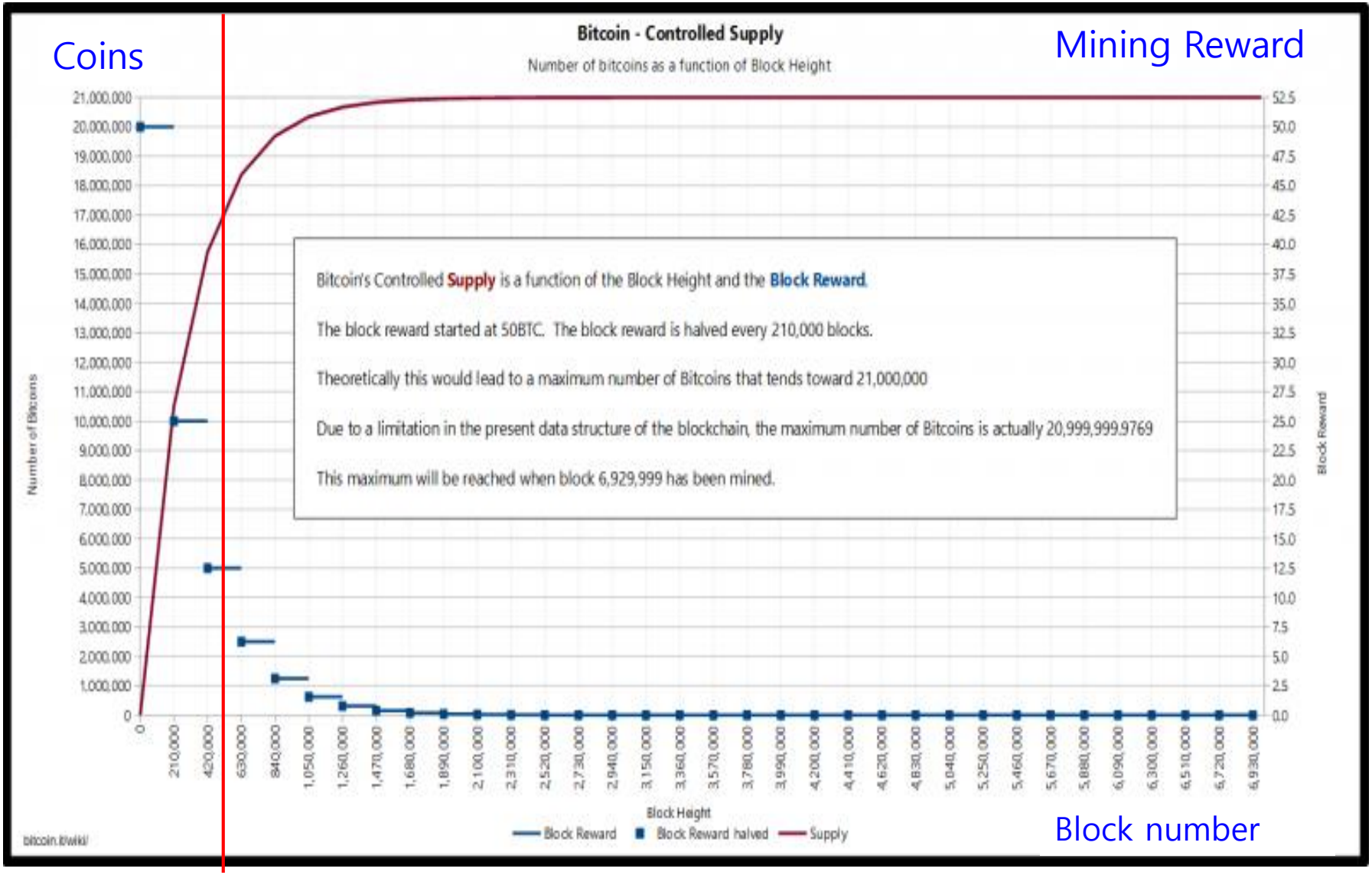
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

Bitcoin

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

Bitcoin' Minting Schedule

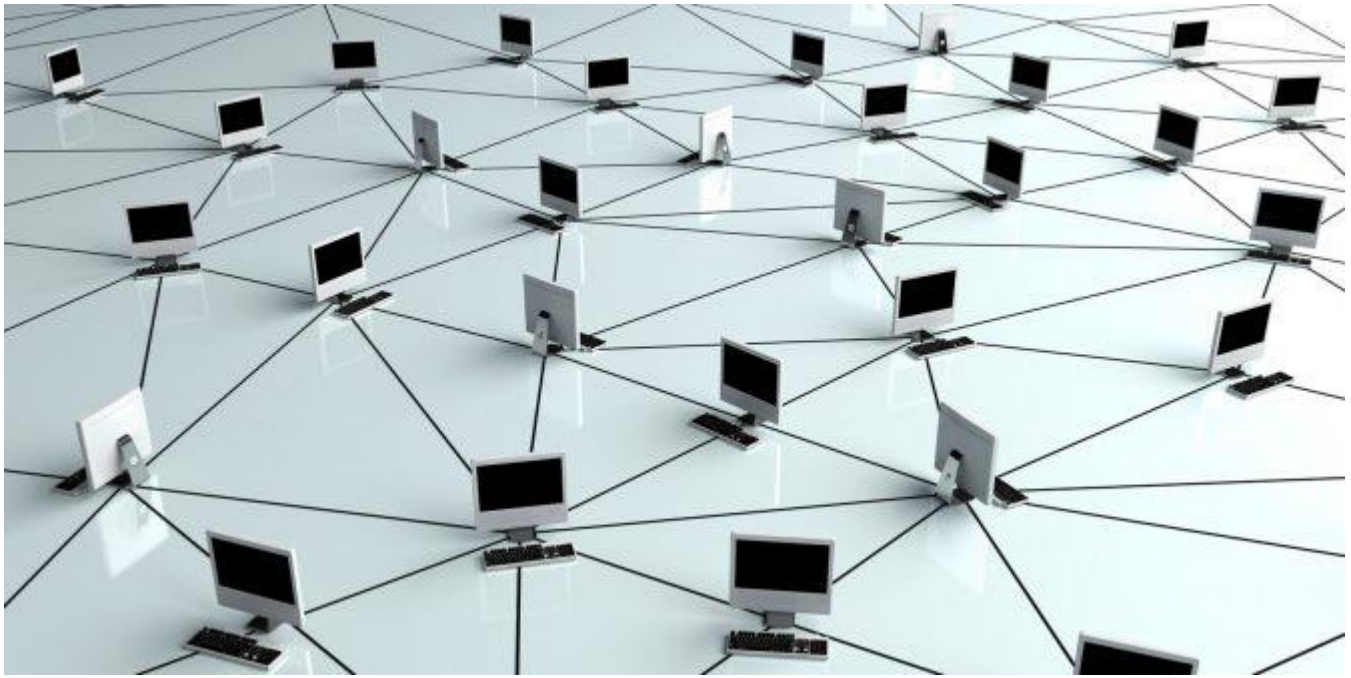


Year 2018

How does Bitcoin work?

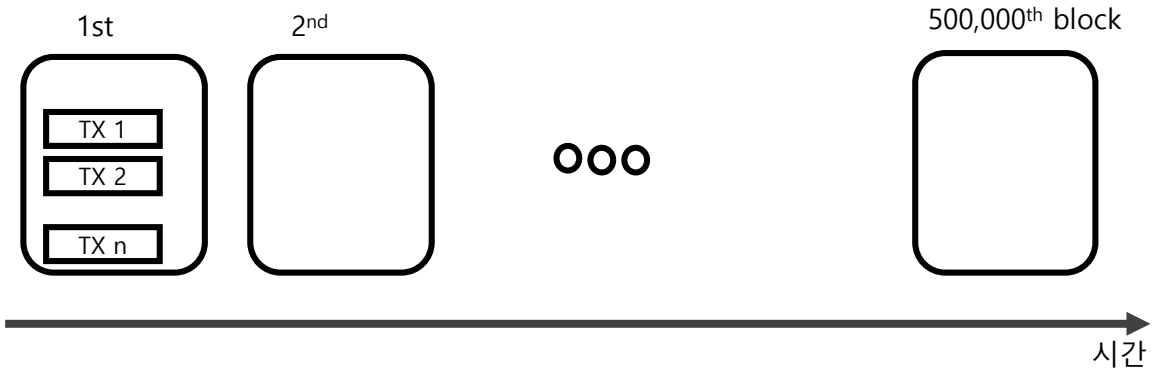
Bitcoin uses the internet.

Bitcoin attracts P2P nodes.



P2P nodes share a blockchain.

- Blockchain is to mean a digital leger:
  - Blockchain is a chain of blocks.
  - Each block is time stamped.
  - Each block stores TXs.
- Blockchain also implies the technology itself.



The blockchain is left open for viewing.

- The digital ledger is left open.
- Anyone can talk to a node and view the ledger. (Public Blockchain)

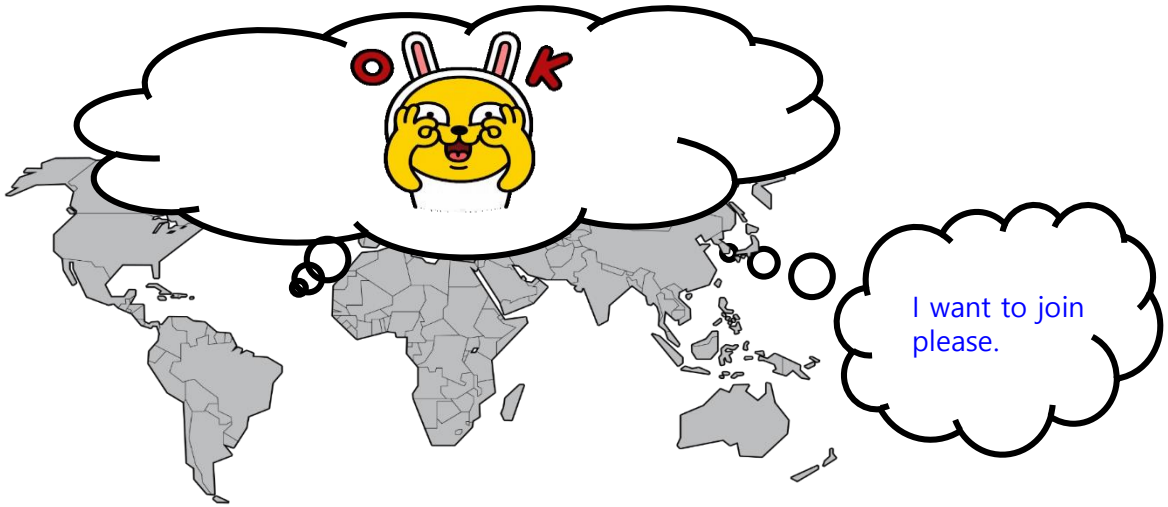
These ledgers are the same except the most recent blocks.

A ledger in America

A leger in Korea

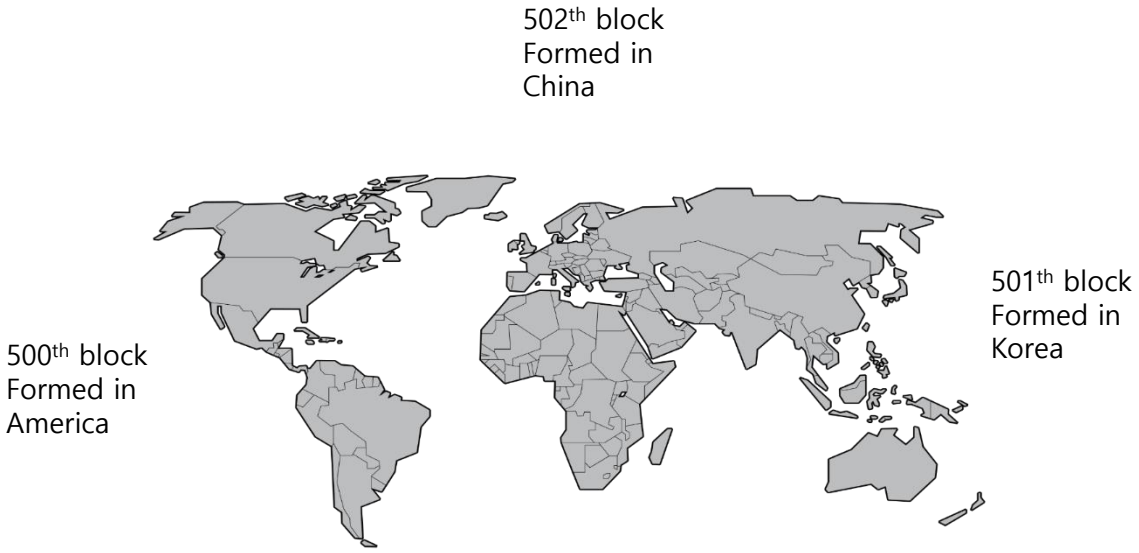
Any new node can join.

- In the public blockchain network, anyone can join and become a guard (miner).



Miners are everywhere.

- Each block is formed by a node.
- A node gathers TXs, validates them, forms a block.
- As a reward, the node which formed a block is given a block mining reward (e.g. 12.5 BTC).
- Thus, they are called miners.

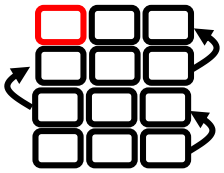


Consensus mechanism plays the key role in blockchain.

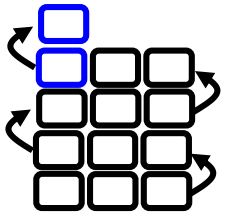
- Multiple different chains are possible, as miners work independently.
- When any two chains are available, miners choose the longer one!

Which one wins when there are two chains announced?

100th block mined
Hooray!



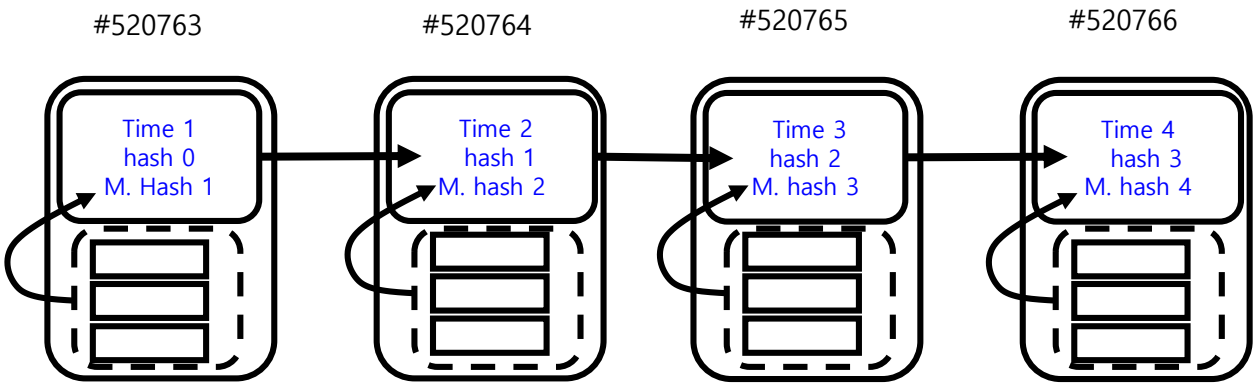
101th block mined
Hooray!



Longer chain wins!

Blocks are cryptographically chained.

- Blocks are cryptographically chained.
- Any alteration made to the content can be easily noticed.



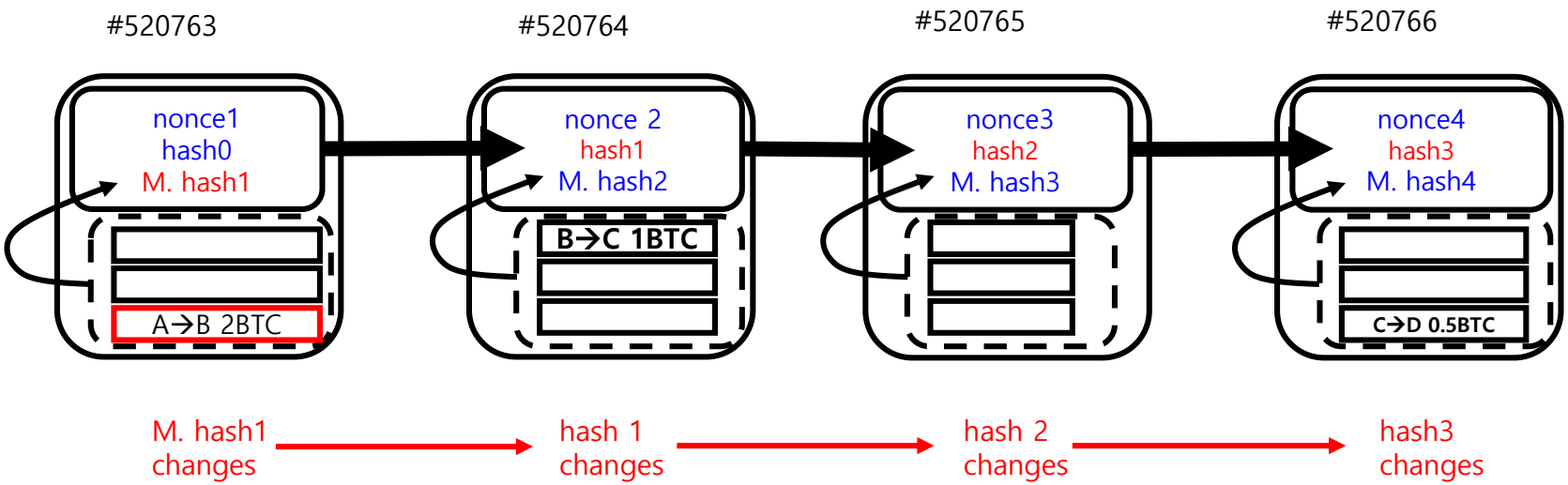
Secure hash function F
F(file) = hash

256 bit string

Content in the blockchain cannot be changed (easily).

- What happens when any alteration is made?
- Any alteration is easily noticeable!
- If an unnoticeable change were wanted, the whole alteration would be needed.
- The whole alteration is to redo all the hashes of the subsequent blocks.
- Proof-of-Work (PoW) is imposed to the chain and thus the whole job cannot be redone easily.

- Immutability and openness allow one to transact with the other over the internet.
  - A→ B 2 BTC
  - B → C 1 BTC
  - C → D .5BTC



Blockchain is a Program Suite.

블록체인 구성 요소 3가지

1. Networking of P2P nodes over the web interface

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

2. Wallet app for TX generations

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

3. Blockchain Protocol

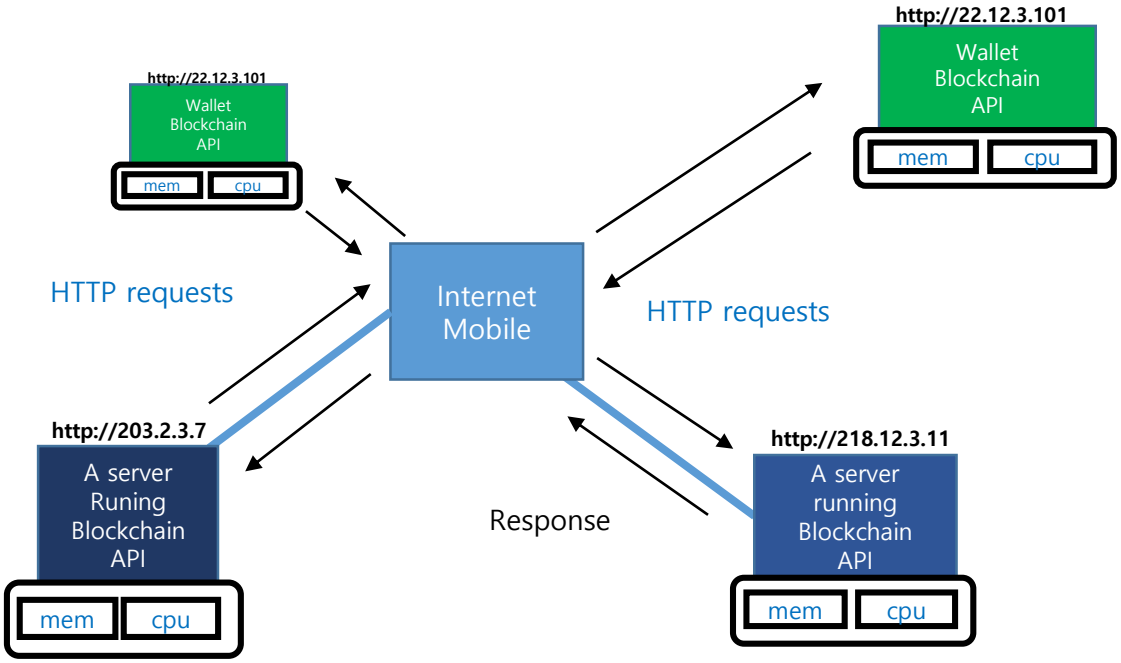
- Data: Genesis block + regular blocks, one block every 10 min, block-size 1Mbyte
- Protocol: consensus, block header, difficulty level adjustment, …
- Mining: Get the longest chain, validate it and all transactions within it, get transactions from mempool and form a block, run SHA repeatedly until you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

Program Suite

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

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

the blockchain internet



Bitcoin Blockchain Verticals

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

Cryptoeconomic Design

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

Unexpected but there are

- Exchanges
- Investors
- Crowd funding: ICO

Multiple perspectives on cryptos

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

WEF's Perspective on Cryptocurrency

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

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

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

ICO and Ethereum

ICO

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

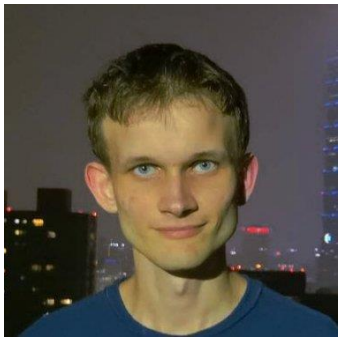
ICO, how did it get started?

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

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

Ethereum ICO

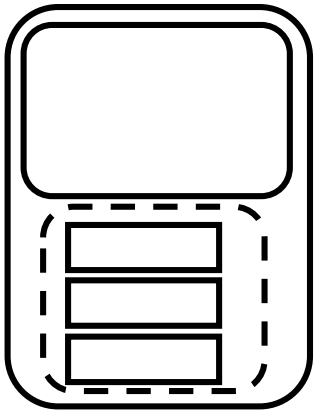
- Ethereum ICO in 2014, raising coins worth millions of dollars.



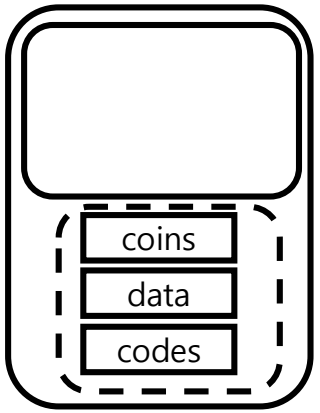
Ethereum

- It allows full computer codes in blockchain.
- Blockchain is platformized so that anyone can use.
- Smart contracts and tokens can be generated easily.
- Decentralized applications (Dapp) are proliferated.

Bitcoin only
records coin TXs



Ethereum allows
data and codes as well



The Ethereum's block that stored the Panmunjeom Declaration

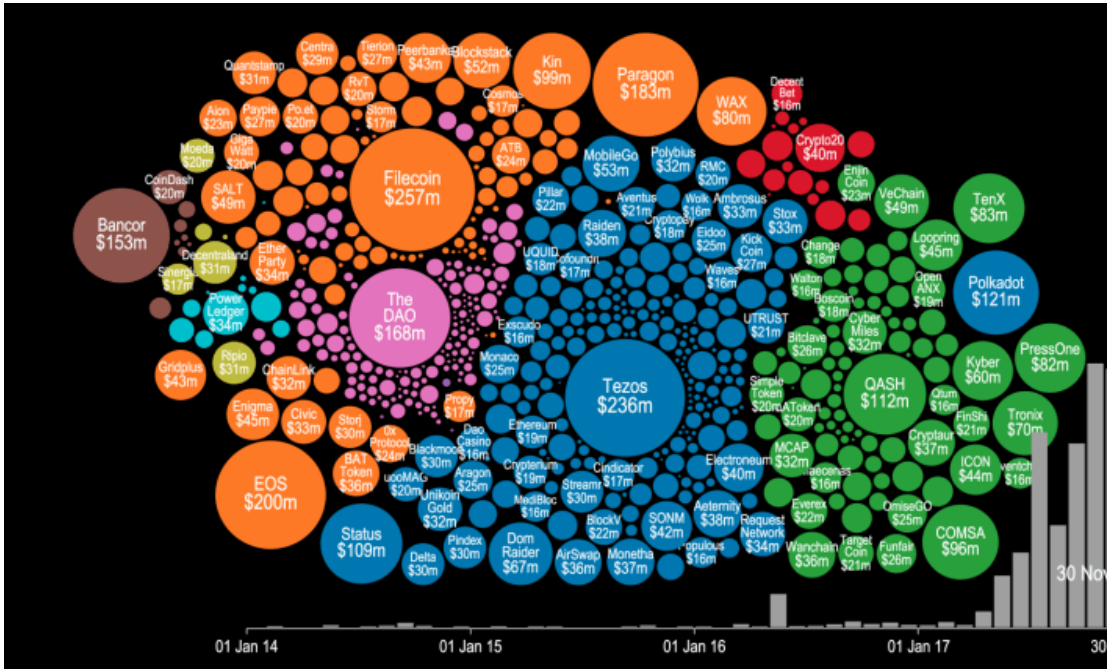
Overview | Comments

Transaction Information

TxHash:	0xe4ee15d3f63db8464a649e3237ed83e930f9b3e40e842537a626745d1c96553c
TxReceipt Status:	Success
Block Height:	5517596 (1257 block confirmations)
TimeStamp:	5 hrs 13 mins ago (Apr-28-2018 12:00:37 AM +UTC)
From:	0xe484c512c156c7f30c85cf432b8e2e70fd499058
To:	0xe456064545f872b311ae7432689a0fece90c9a29
Value:	0 Ether ($0.00)
Gas Limit:	800000
Gas Used By Txn:	434032
Gas Price:	0.000000012 Ether (12 Gwei)
Actual Tx Cost/Fee:	0.005208384 Ether ($3.47)
Nonce:	0
Input Data:	0x2018년 4월 27일 한반도 판문점 선언 1. 남과 북은 남북 관계의 전면적이며 획기적인 개선과 발전을 이룩함으로써 끊어진 민족의 혈맥을 잇고 공동번영과 자주통일의 미래를 앞당겨 나갈 것이다.
	Switch Back
Private Note:	<To access the private Note feature, you must be logged in>

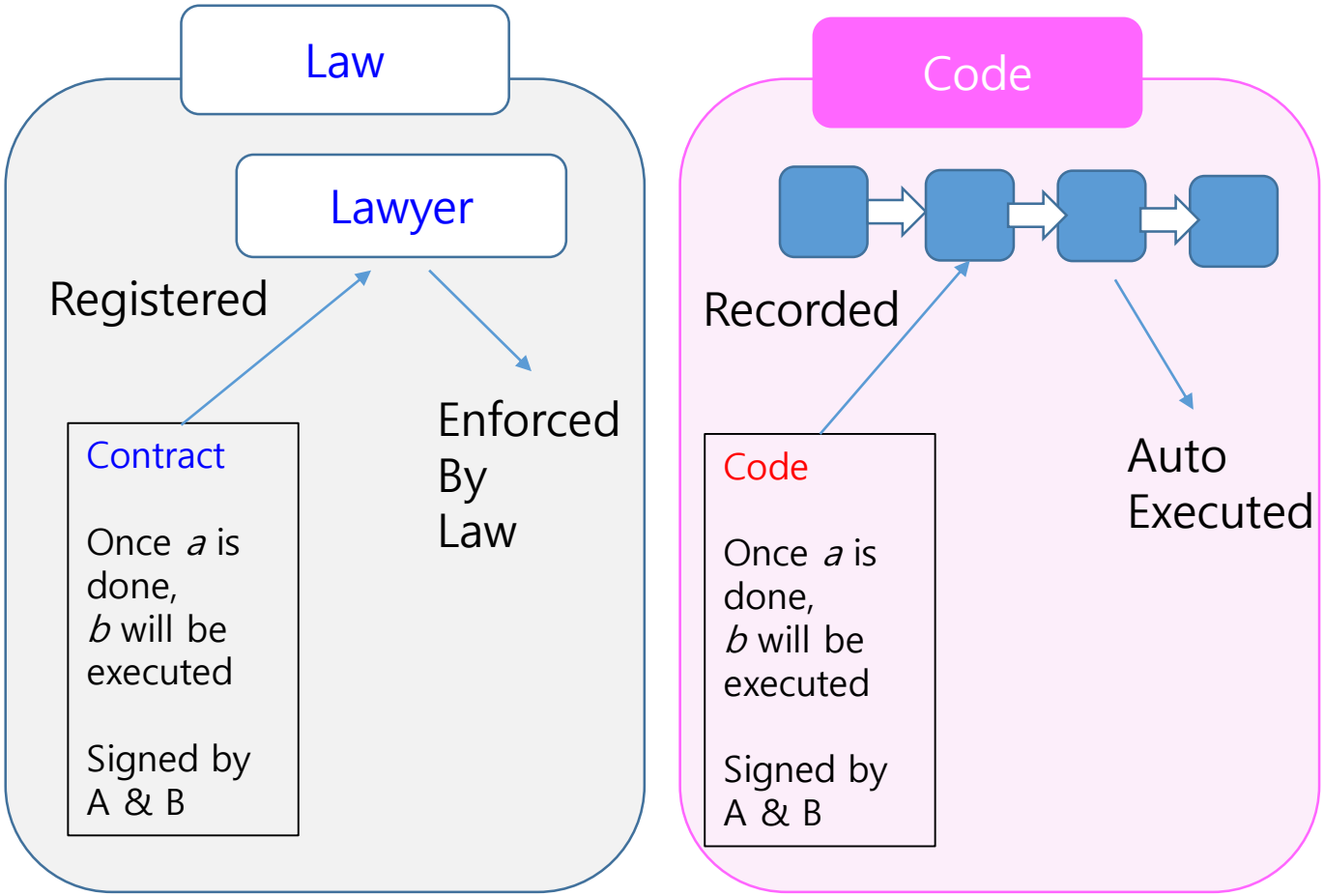
2018.04.28

Smart Contracts



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

Legal Contracts vs. Smart Contracts



Sharing Economy

Insurance

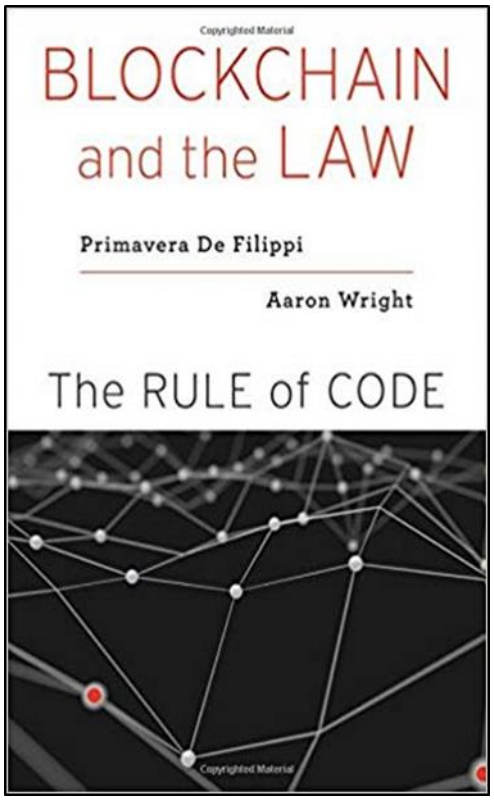
Voting

MediChain

Real Estate

Law

Lex Cryptographia



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

---

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

Problems with blockchains

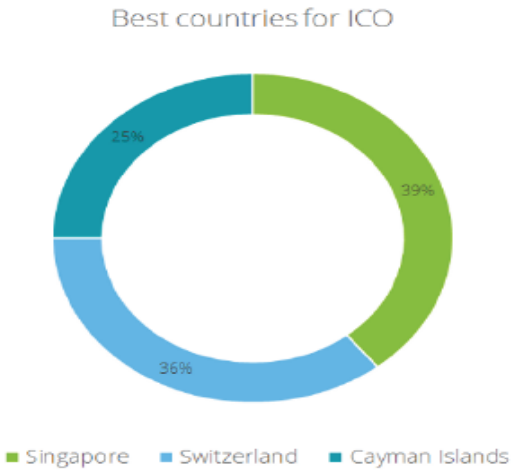
- Astronomical cost for mining
- Smart contracts
  - Bugs
  - Compliance with the law?
- *Decentralization?*
  - *Mining pools are re-centralized.*
- Not very convenient and useful as a currency (medium of exchange, storage of value)
  - Slow transactions speed, price fluctuation
- Possibilities of cyberattacks and hacking.
  - Availability of renting services of mining equipment.
  - Astronomical amount of assets were lost due to 51% attacks, such as Monacoin, Bitcoin Gold, Zencash, Verge, Litecoin cash...

Proliferation of ICO projects, BUT

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

Best countries for ICOs include

- Singapore
- Switzerland
- Cayman Islands



USA is not!

Why?

Note that we decided not to include the United States in the list after the SEC issued the Munchee order which prevented Munchee Inc., a California based company that created a blockchain application that allowed its users to post the reviews of restaurants, from continuing its ICO campaign on its second day. Although the company states in its white paper that "a Howey analysis has been conducted to determine that, as currently designed, the sale of MUN utility tokens does not pose a significant risk of implicating federal securities laws.", the order argued that its MUN tokens were actually "securities" because they are considered to be "investment contracts". The fact that the Howey test is currently the only reliable way for people planning an ICO to determine whether its token is deemed to be a "security" but the SEC can simply disagree with the "in-house" analysis implies that potential entrepreneurs could be more or less at the mercy of the SEC's decision if they don't register their tokens as securities or qualify for exemption. The unpredictable nature of the SEC ruling led us to exclude the United States from our analysis.

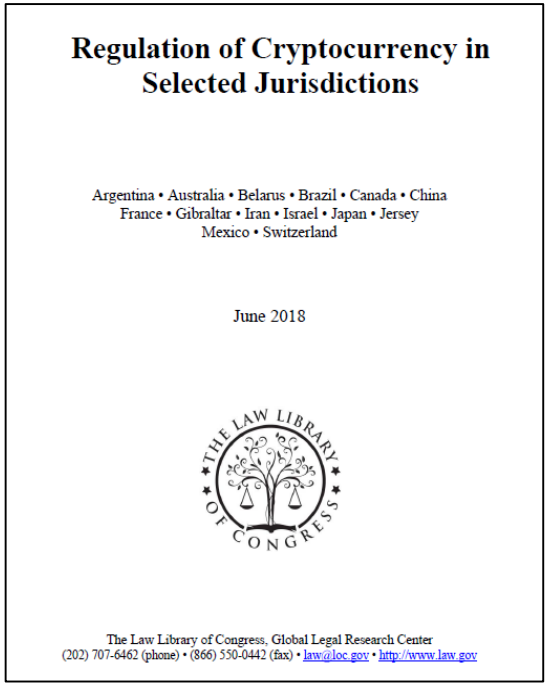
Regulations in the US

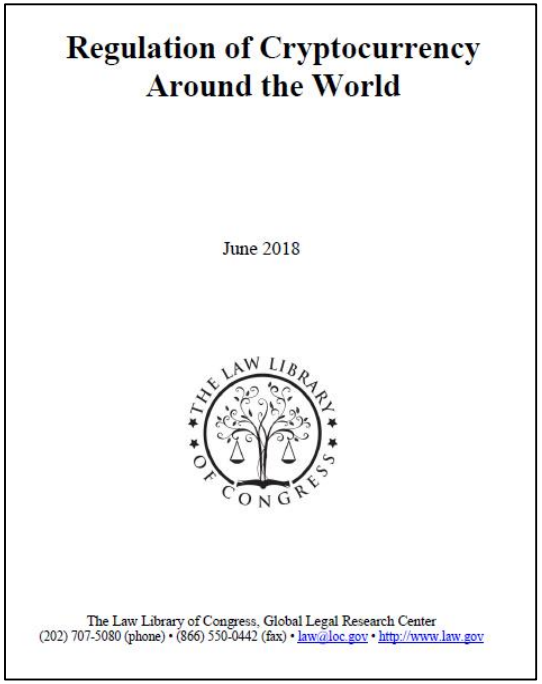
- One of the recent regulatory developments in reference to ICOs has come from the US Securities and Exchange Commission (SEC).

- In its latest ruling on July 25, 2017, the SEC described some of the "coins" offered through ICOs as securities.

Regulations in large countries tend not to make a firm decision yet.

- Korea
- USA
- China
- Japan
- Europe
- East Asia





- No countries treat it as a legitimate currency, but almost all treat it as digital assets for tax purposes.

Is there a direction for nice regulation?

- Needed are investor protection in ICO/IEO projects and regulations to crypto-exchanges
  - Pump and dump
  - Insider trading
  - Compliance with the law
    - money laundering, anti-terror funding, know-your-customer
- No serious harm done?
- Then why don't we wait-and-see.

암호화폐/블록체인 질문목록

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

암호화폐/블록체인 질문목록

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

Experts have been Invited.

Concluding Remarks

- Many possibilities of Blockchain
- Verified by the market are Bitcoin and Ethereum.
- To explore new territory, experiments are needed
  with budgets and man power invested.

- Regulations should be kept at the minimal level to promote new ideas and new industries.

- Huge economical and societal advance is expected with the advent of the blockchain-internet.
- I term this **Blockchain Economy** which is yet to be defined precisely.