블록체인 기술의 이해와 활용

Blockchain Economy

Heung-No Lee 이흥노

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!

블록체인 기술의 이해와 활용

5월 31일, 이흥노

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
- Future of Blockchains
- Summary

Economy, Currency, Government

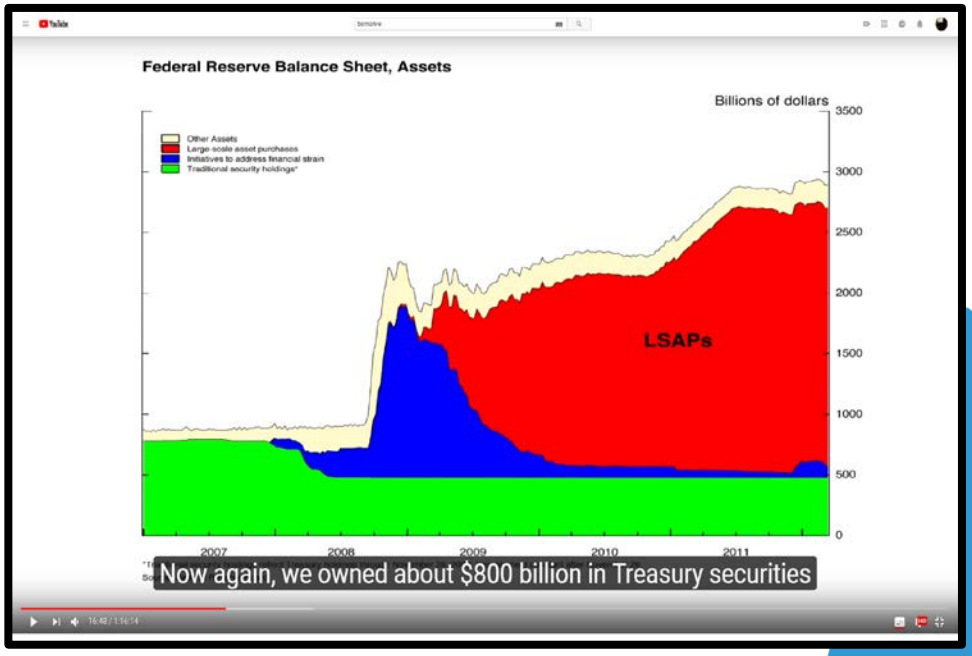
- People want an *ever improving state of self* and economic position compared to what they have enjoyed in previous years.

- **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

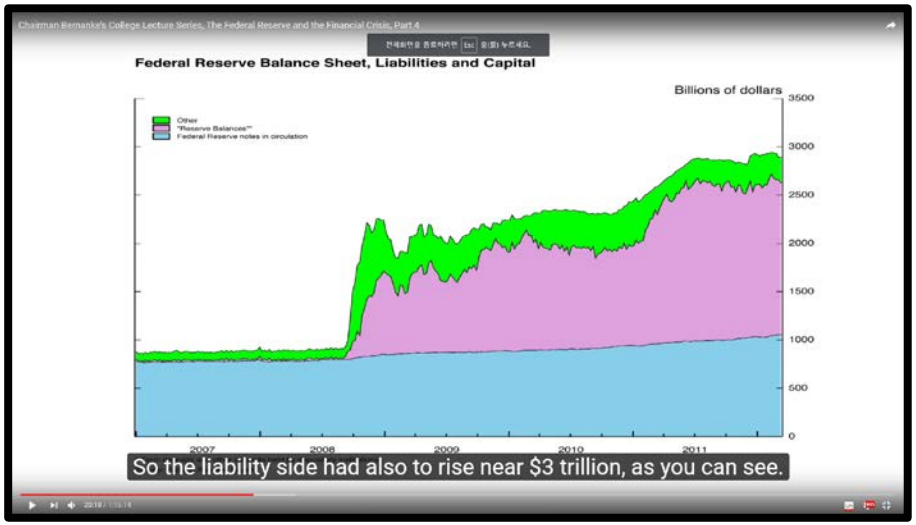
>Large Scale Asset Purchases (QE)
- Control long-term supplies of securities
- Raising the price of these assets
- Lowering the long term interest rate.



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.

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

- Today, currency is not money.
- With frequent financial crises, trust to gov. is down.
- 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

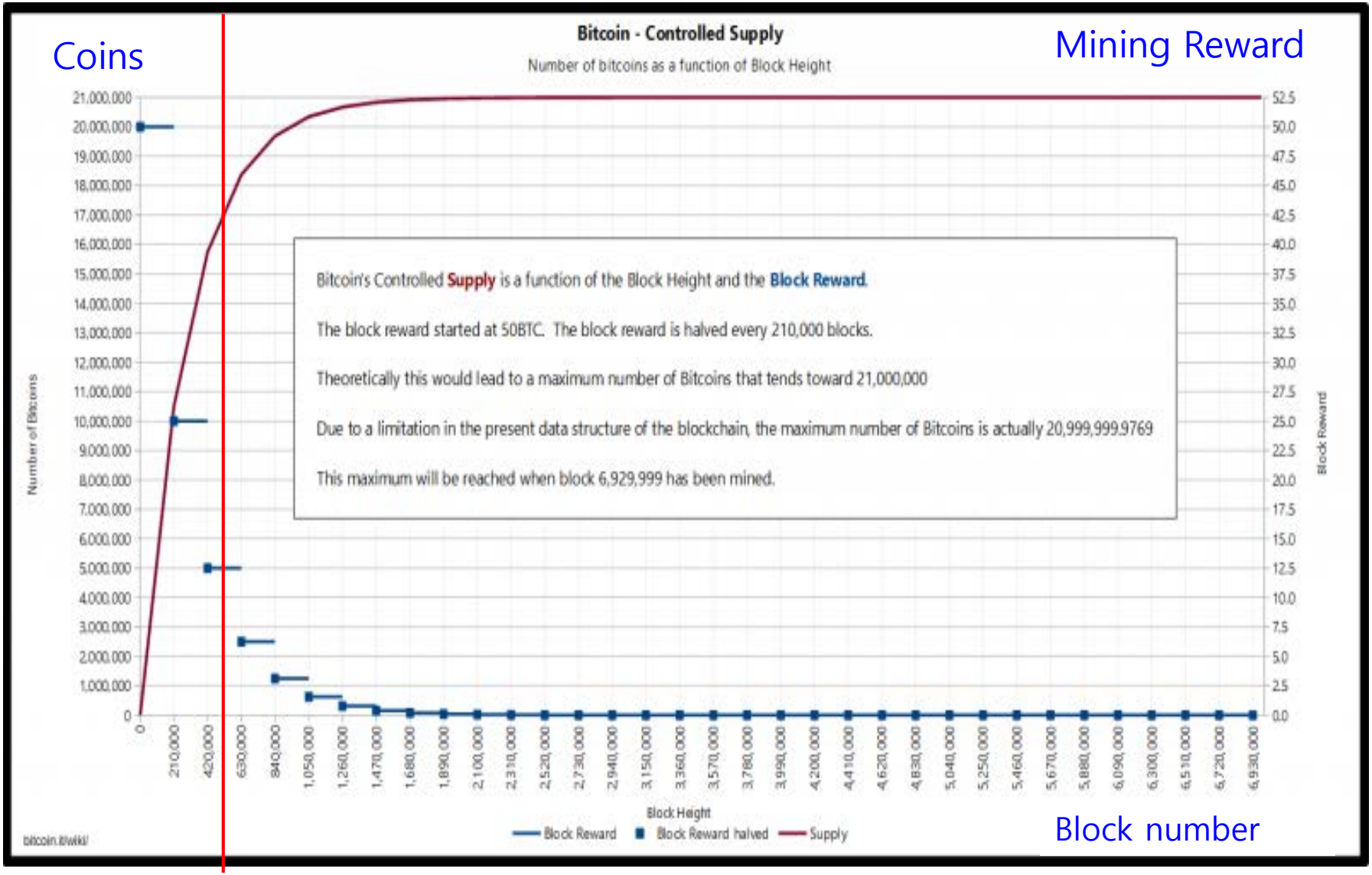
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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

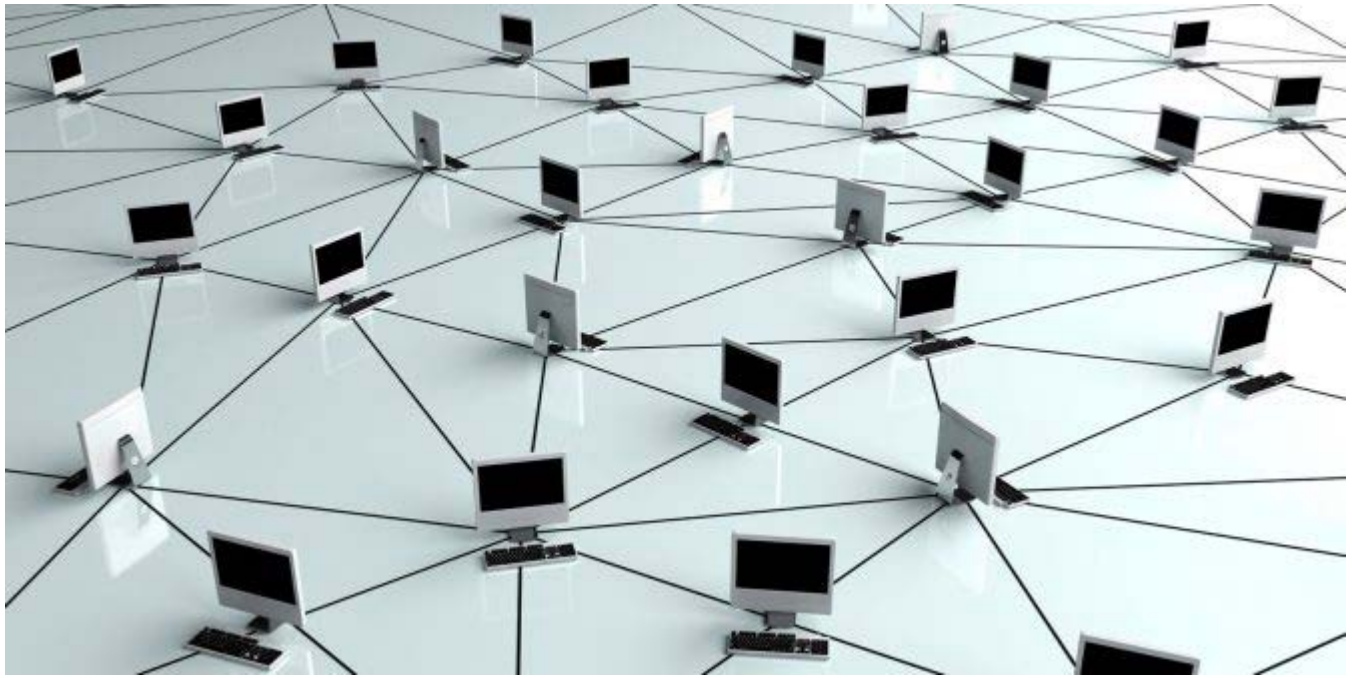


Year 2018

How does Bitcoin work?

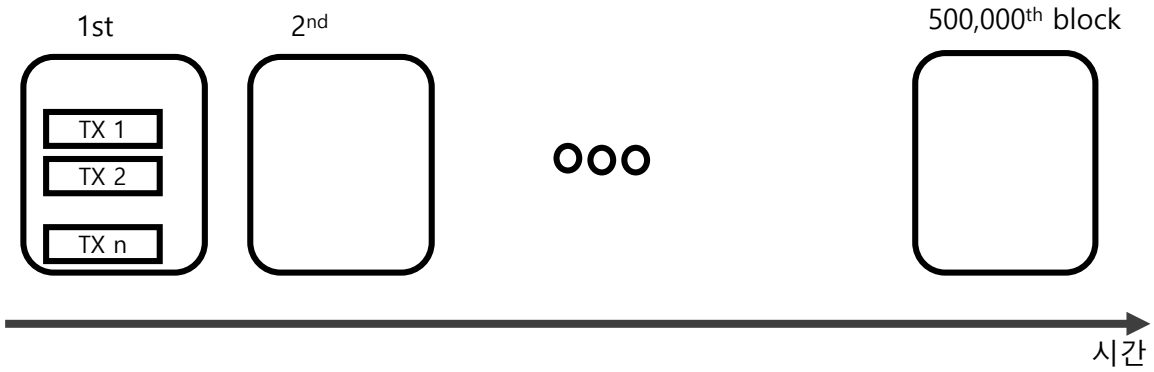
Bitcoin uses the internet.

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)

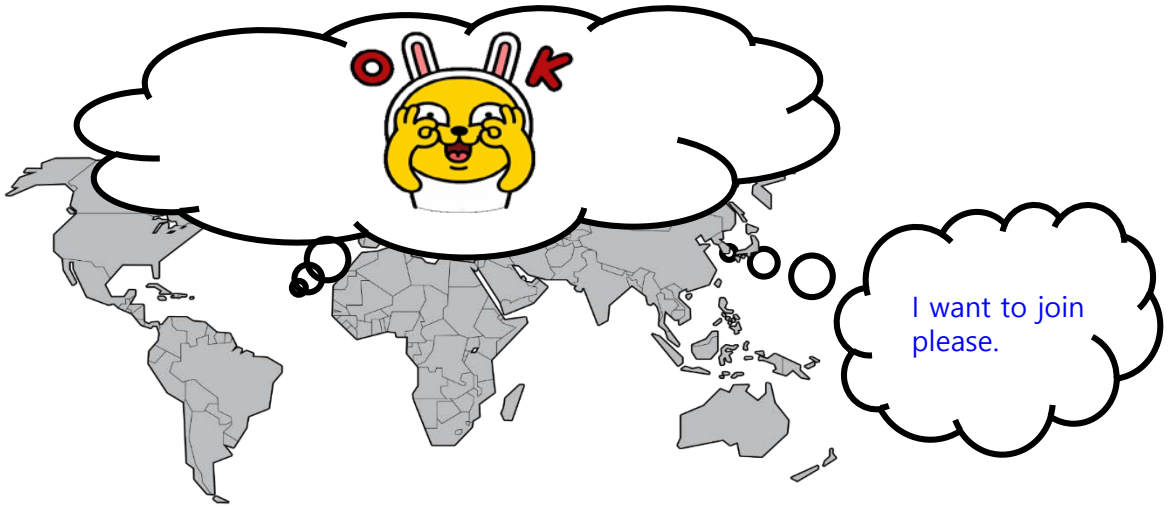
These ledgers are the same except the most recent blocks.

A ledger in America

A leger in Korea

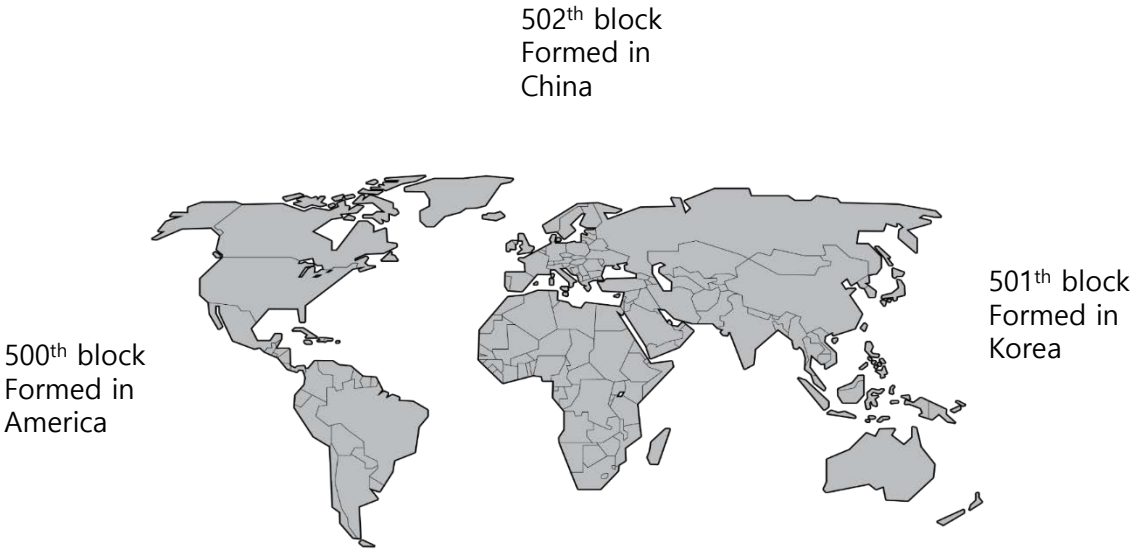
Any new node can join.

- 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.

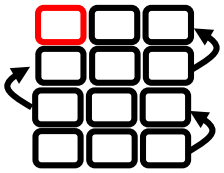


Consensus mechanism plays the key role in blockchain.

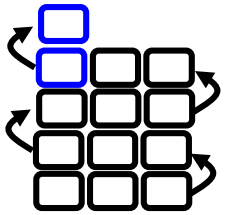
- Multiple different chains are possible, as miners work independently.
- When any two chains are available, miners choose the longer one!

Which one wins when there are two chains announced?

100th block mined
Hooray!



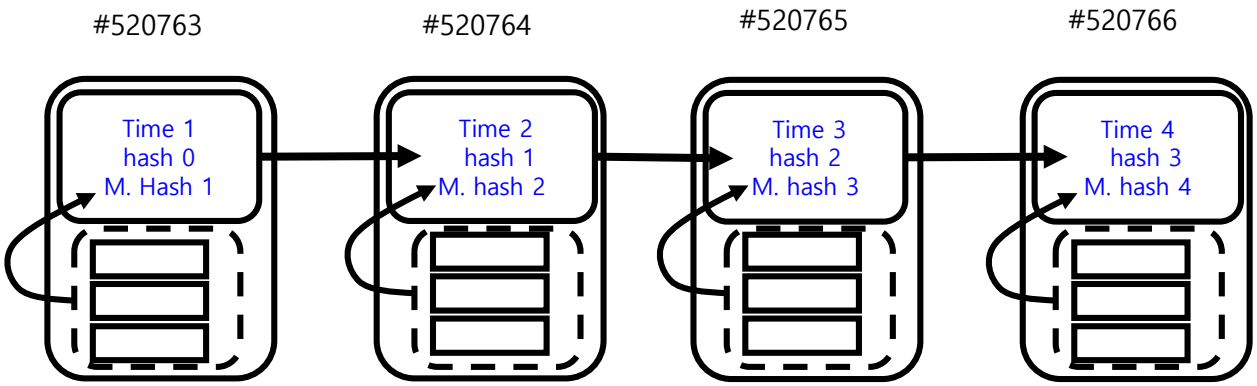
101th block mined
Hooray!



Longer chain wins!

Blocks are cryptographically chained.

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

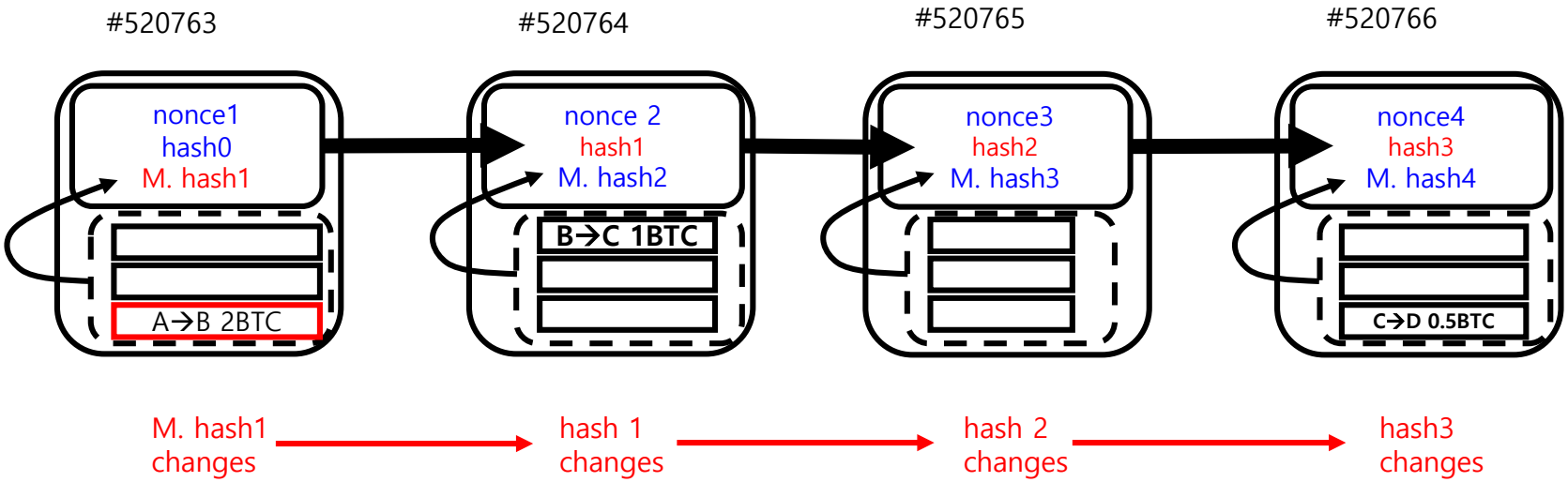


Secure hash function F
F(file) = hash

256 bit string

Content in the blockchain cannot be changed (easily).

- What happens when any alteration is made?
- Proof-of-Work (PoW)
- Immutability and openness allow transactions.
  - A → B 2 BTC
  - B → C 1 BTC
  - C → D .5 BTC



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

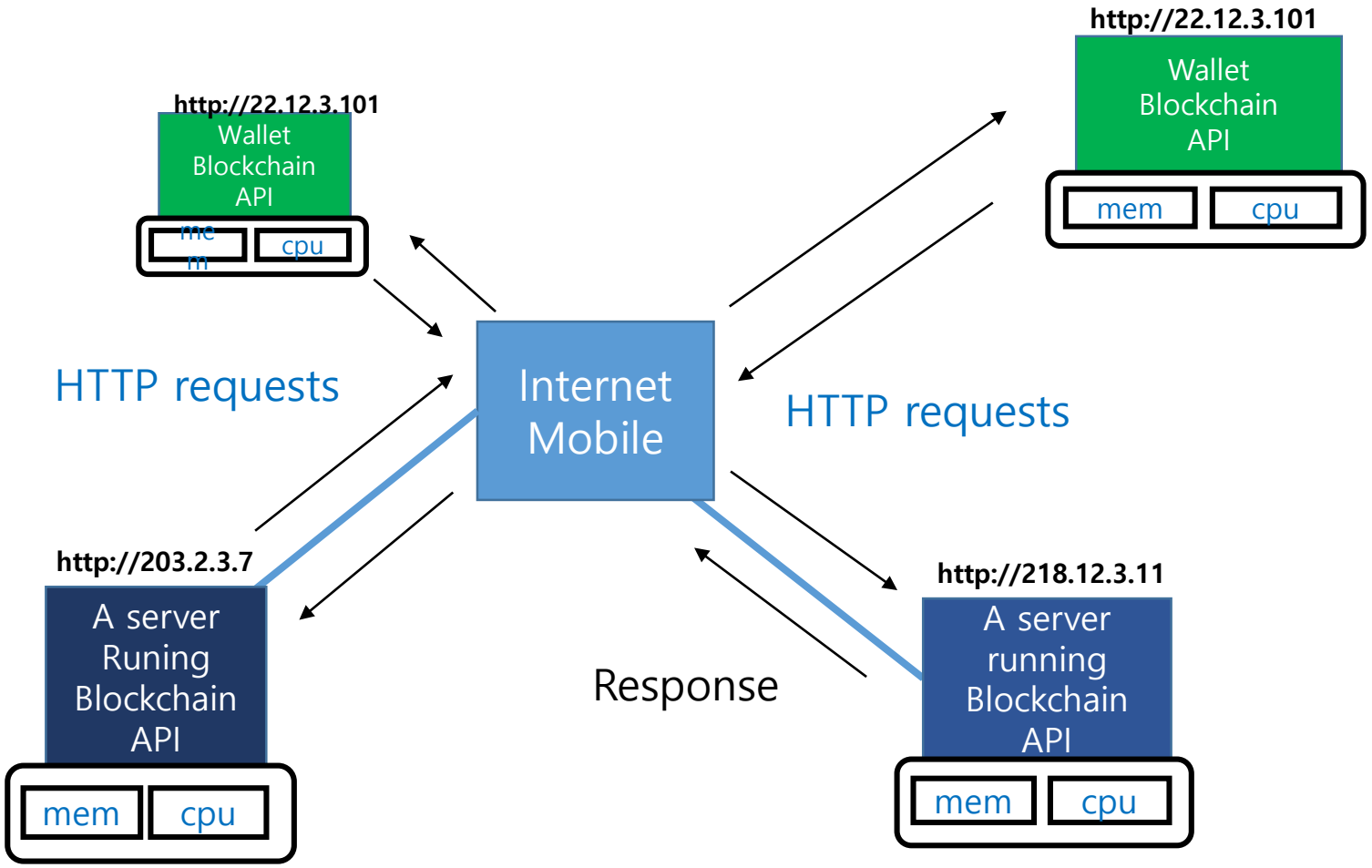
- Data: Genesis block + regular blocks, one block every 10 min, block-size 1Mbyte
- Protocol: consensus, block header, difficulty level adjustment, …
- Mining: Get the longest chain, validate it and all transactions within it, get transactions from mempool and form a block, run SHA repeatedly until you 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

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

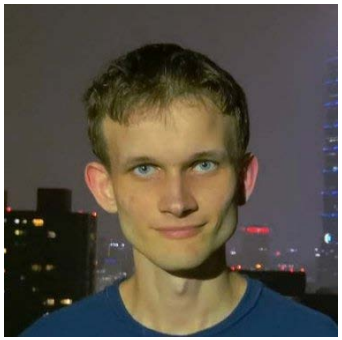
ICO, how did it get started?

- "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

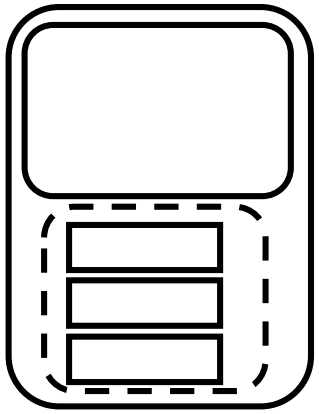
- Ethereum ICO in 2014, raising coins worth millions of dollars.



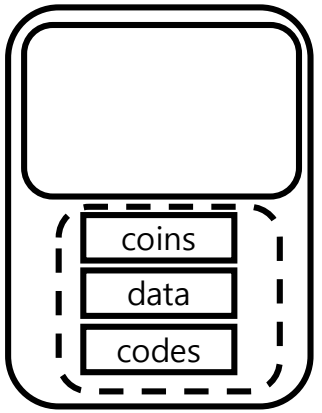
Ethereum

- 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

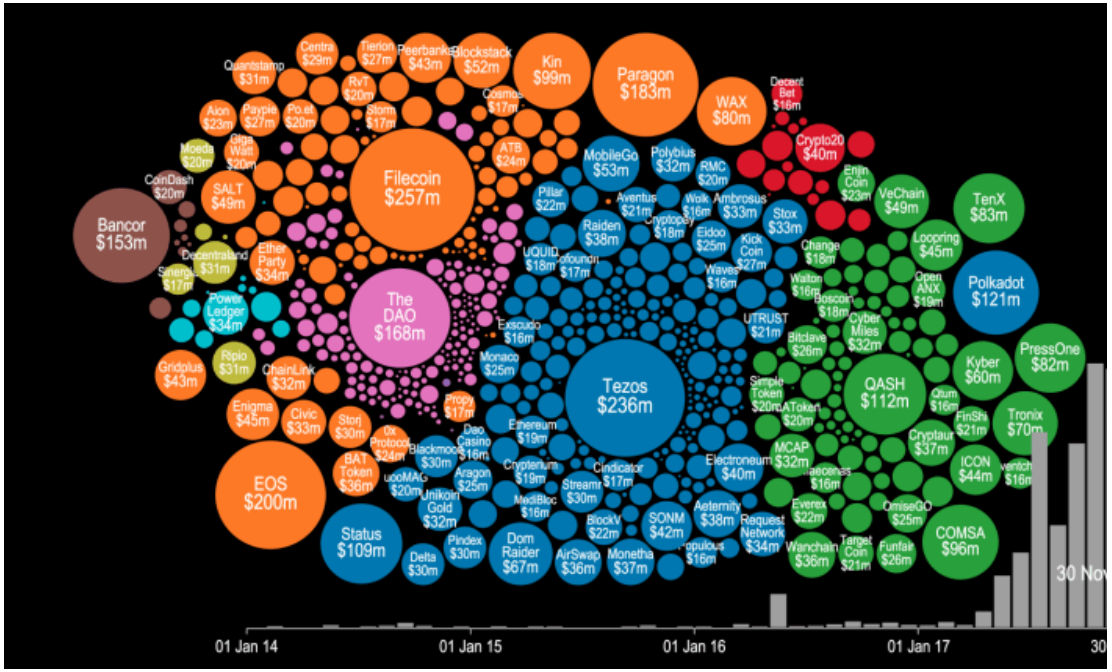
Overview | Comments

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:	0xe450604545f872b311ae7432689a0fece90c9a29
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>

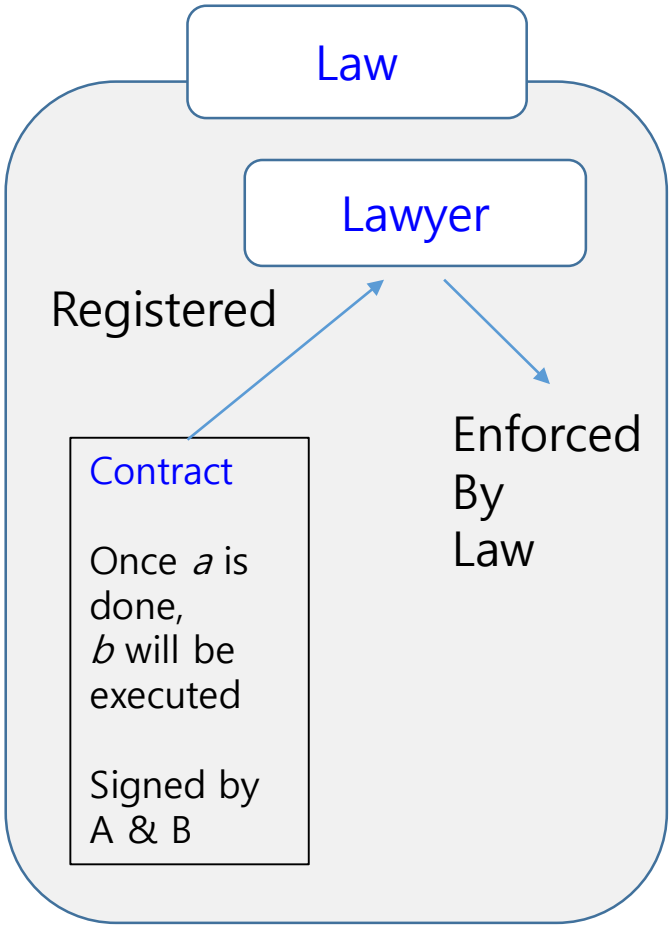
2018.04.28

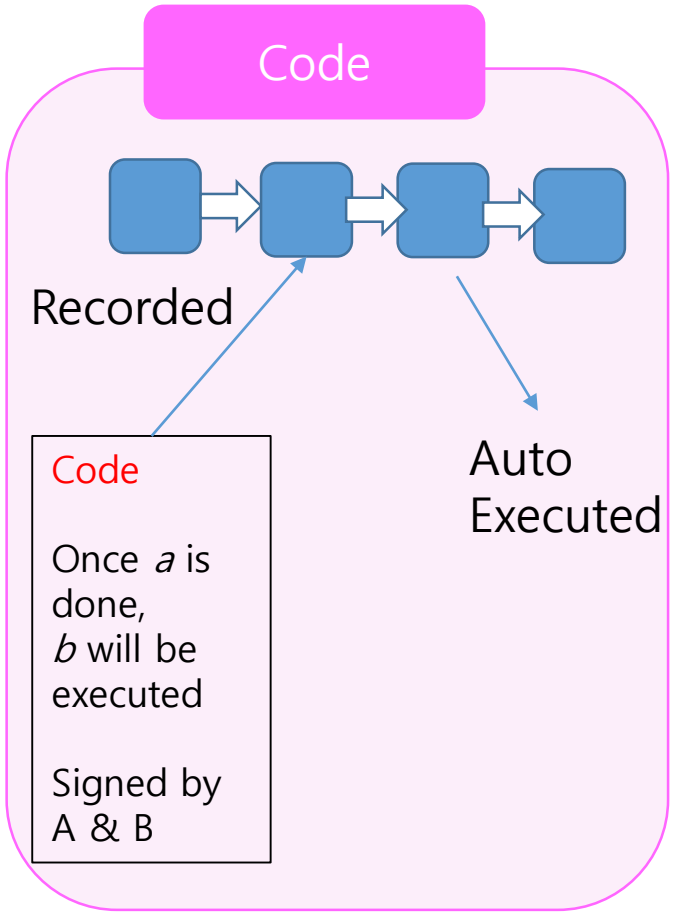
Smart Contracts



- 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

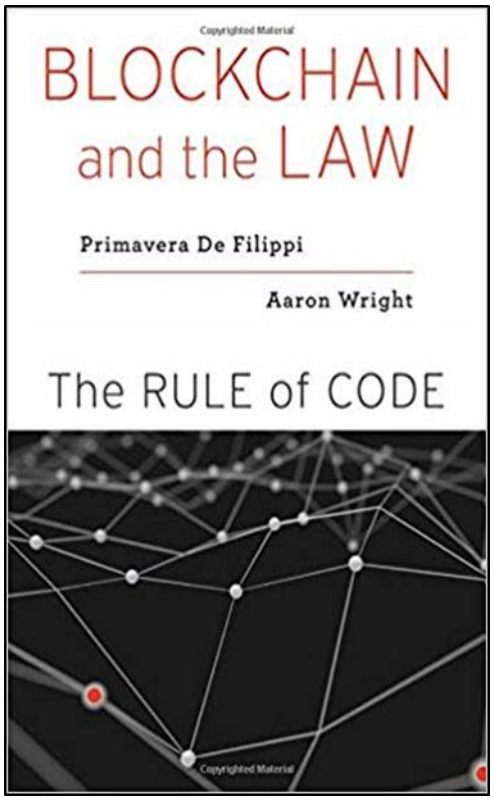
Voting

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

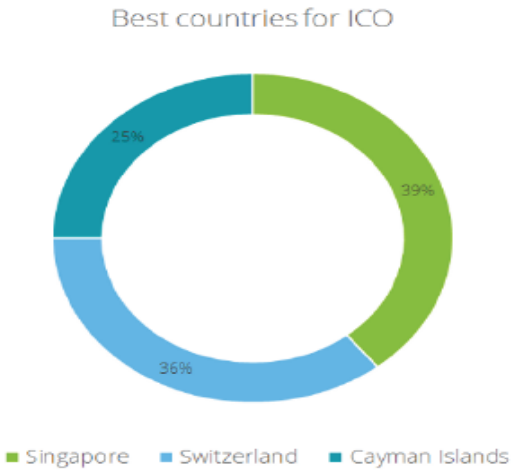
- **Astronomical cost for mining**
- **Smart contracts**
  - **Bugs**
  - **Compliance with the law?**
- *Decentralization?*
  - *Mining pools are re-centralized.*
- **Not very convenient and useful as a currency (medium of exchange, storage of value)**
  - **Slow transactions speed, price fluctuation**
- **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...**

Proliferated 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.

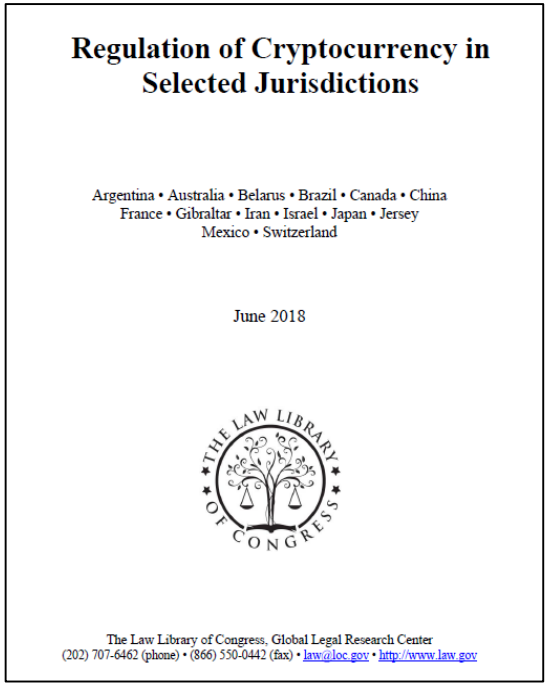
Regulations in the US

- 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.

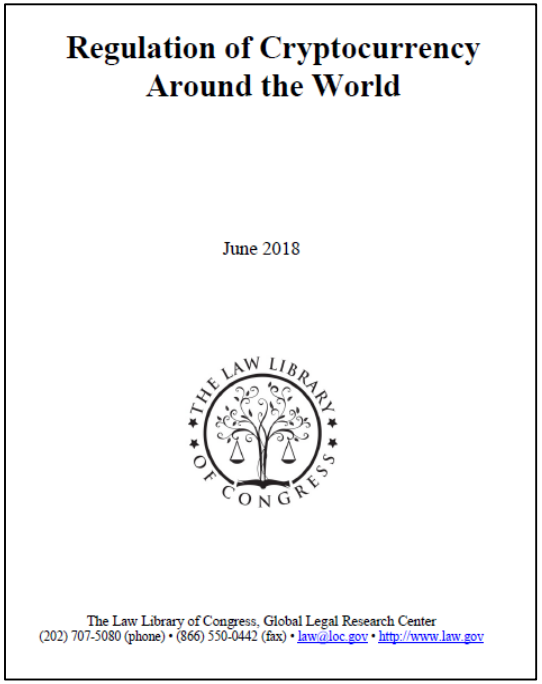
- Korea
- USA
- China
- Japan
- Europe
- East Asia


Regulation of Cryptocurrency in Selected Jurisdictions

Argentina • Australia • Belarus • Brazil • Canada • China
France • Gibraltar • Iran • Israel • Japan • Jersey
Mexico • Switzerland

June 2018

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov


Regulation of Cryptocurrency Around the World

June 2018

The Law Library of Congress, Global Legal Research Center
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

- 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.

New Capabilities of Open Blockchains

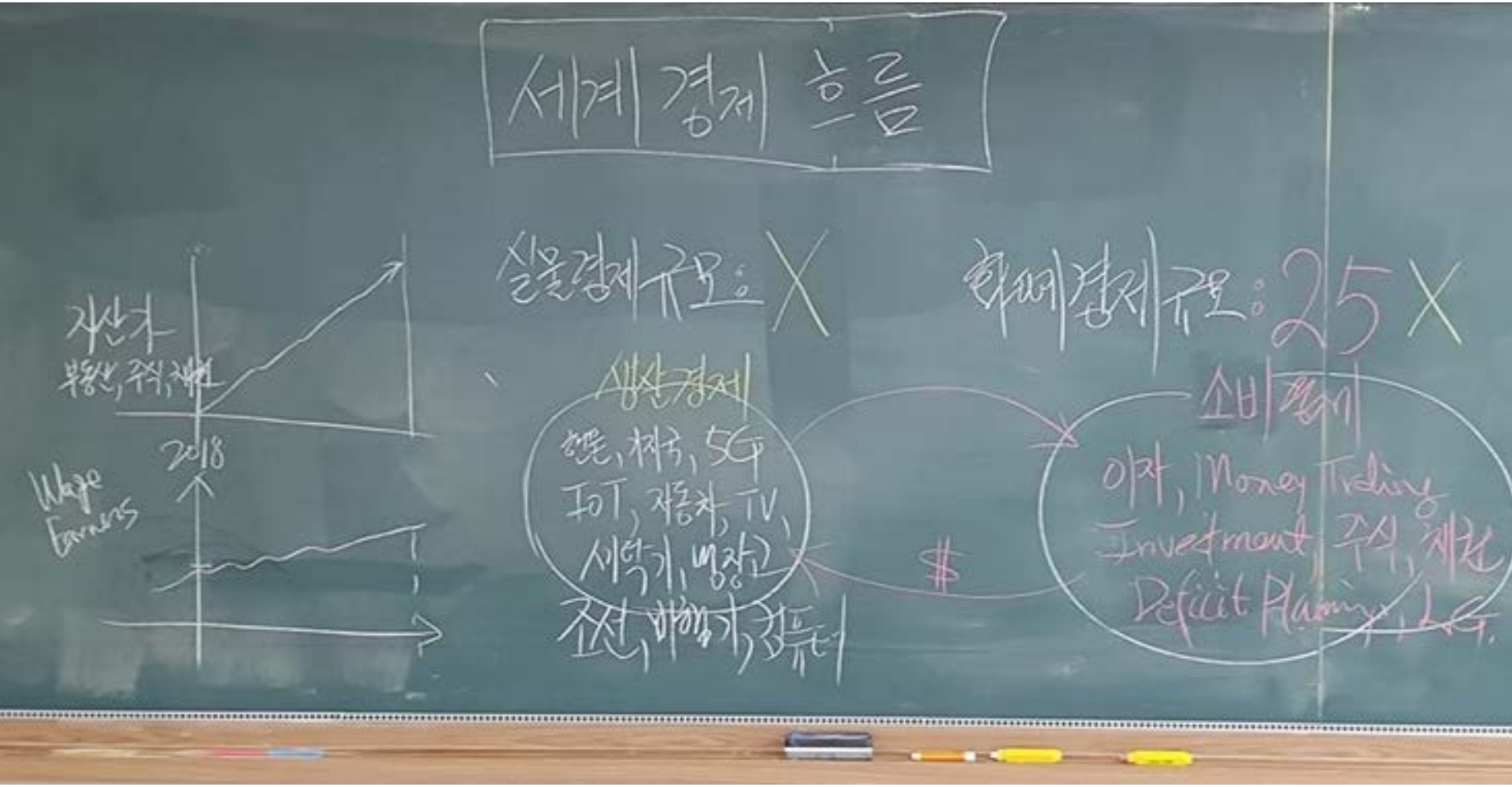
- Global currencies
- P2P transfer of value
- New governance
- Digital economy
- Anonymity
- Freedom
- Empowering individuals
- Inclusive finance

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)


세계 경제 흐름
실물경제규모: X
화폐경제규모: 25 X
자산가
부동산, 주식, 채권
2018
Wage Earners
생산경제
핸드, 차량, 5G
IoT, 자동차, TV,
세탁기, 냉장고
조선, 비행기, 컴퓨터
$
소비경제
이자, Money Trading
Invetmant, 주식, 채권
Deficit Planning, LG.

Monetary Policy에 대한 단상

- 학생들에게 세계 경제의 흐름을 이야기하기 위해 칠판에 그렸던 그림.
- 미국은 기축통화 달러를 갖고 있는 나라. 필요한 건 모두 사서 쓴다. 대금은 달러로 지급. 달러가 모자라면 그냥 만든다. 어떻게? 그냥 Acct에 들어있는 밸런스를 늘리면 된다. 누가? FED가. 국채를 발행하고 달러를 찍어 내다가, 2008년 이후로는 그냥 양적완화하여 만든 달러로 국채를 시장에서 매입한다. 이런 식으로 이자율을 0에 가깝게 만든다. 나아가 은행이 Lending을 통해 만들어 내는 신용 통화가 FED가 늘려준 밸런스에 10배 넘게 창출된다. 즉 FED가 만든 Monetary Base증가액이 2 Trillion USD. 이때 시장에 풀려나가는 신용통화는 대략 10배인 20 Trillion USD. 미국 GDP가 20 T USD.
- 중국, 한국 등은 실물경제로 돌아가는 나라. 수출로 경제 성장. 수출 품목은 핸폰, 자동차, 세탁기, 냉장고 등. 이런 것들을 미국에 팔고 대금으로 달러를 받는다. 달러 위기가 올까봐 달러를 잔뜩 비축해 놓는다. 그래도 남는 것은 미국 국채를 산다.
- 위 두 문단을 요약하면 물건은 미국으로, 달러는 전세계로 퍼져 나간다. 저렇게 퍼져나간 달러가 어디로 갔나? 대부분 화폐경제 부분으로 흘러 들어가 주식버블, 부동산버블을 만든다. 자산을 갖고 있는 사람들은 부가 증식이 된다.
- 버블경제에서는 저축은 장려되지 않는다. 왜? 이자률이 낮아서 은행에 넣어놓으면 오히려 손해가 된다. 돈의 양이 많아지면 가치가 떨어지니까. 빚을 얻어서라도 자산을 사 놓아야 한다. 그래야 가치가 올라 가니깐. 저축하기 보다는 빚을 내서라도 자꾸만 소비하라고 말한다. 소비가 production 이라며. 부의 편중이 극심해 진다. 일자리를 통해 소득을 얻는 사람들은 박탈감을 느낀다.
- 이런 것들이 미국에서 논의되고 있는 QE관련, FED관련, Modern Monetary Theory관련에 대한 저의 단상입니다.
- Bitcoin으로 수출대금을 결제해 달라고 하면, 미국은 어떻게 될까요?

네덜란드 중앙은행 W. Paper

1 vs. 99

Monetary Policy로 만든 돈 다 어디로 갔나?

Data analysis from 1920 to 2015.

Wage로 갔을까?

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

Mehdi El Herradi* Aurélien Leroy †

April 2019

Abstract

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

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

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.

Thank you!

이흥노

heungno@gist.ac.kr

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

Facebook/Publication ID: Heung-No Lee

You can download this lecture note from slideshare.net!