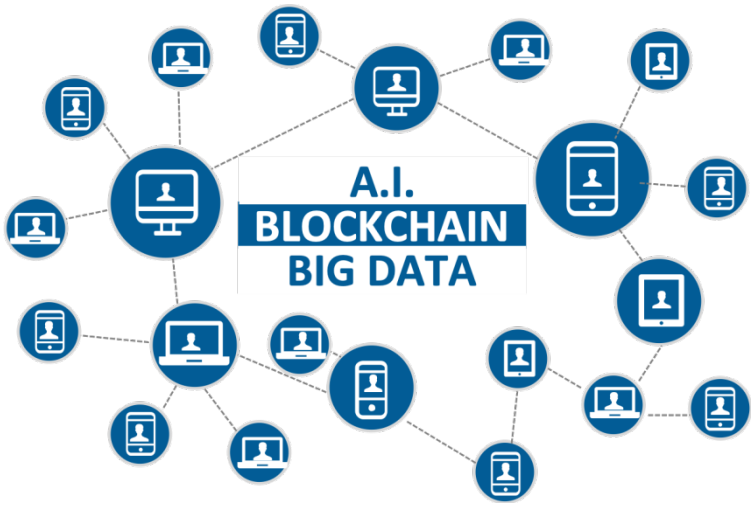
GIST 기초전기전자컴퓨터 특론 자료집

블록체인경제



◇ 일 시 : 2019년 03월 07일 ~ 06월 06일 매주 목요일 16:00

◇ 장 소 : GIST 대학A동 227호

◇ 주 최 : GIST

◇ 주 관 : GIST블록체인경제센터

◇ **Content: 강의자료 및 YouTube 동영상 링크**

2019년 봄학기 EC4301
기초전기전자컴퓨터 특론

블록체인경제

강좌기간	2019. 03. 07(목) ~ 06. 06(목) <매주 목요일 16:00~19:00>
대상&인원	블록체인에 관심있는 누구나 / 70명
장소	GIST대학 A동 227호
신청기간	2019.02.21(목) ~ 2019.02.27(수) 18:00
신청방법	하단 링크 혹은 QR코드에서 선착순 접수 (https://goo.gl/forms/4lBp7hlvNWPdR9Fm2) ※ 정원의 150% 도달 시 접수 마감 (선착순 70명, 대기자 35명)
수강료	무료
문의전화	062) 715-3140 (블록체인인터넷경제 연구센터) 062) 715-2282, 2251 (INFONET 연구실)
이메일	kdgjwj@gist.ac.kr

GIST College Special Topics Course EC4310 (Spring 2019)

Date: Jan 29th 2019

Primary Instructor: Professor Heung-No Lee, GIST EECS

Objectives: 본 교과목을 관통하고 있는 핵심은 블록체인 경제이다. 블록체인 경제가 과연 무엇인가 생각해 본다. 블록체이니즘이라 불리는 새로운 사조가 생겨나고 있는데, 그게 무엇이며 생성원인을 고찰해 본다. 암호화폐란 무엇이며 그 본질성이 어디에 있는지 연구해 본다. 간단한 실습을 통해 암호화폐를 직접 만들어 보는 경험을 해 본다. 블록체인과 암호화폐가 어떻게 사회를 변화시킬 수 있는지 살펴본다. 블록체인경제, 블록체인거버넌스, 토큰이코노미, 암호화폐거래소, Radical Markets 등 새로운 정치 및 경제 개념이 생겨나고 있다. 이들이 국가경제 나아가 세계경제에 미치는 영향을 살펴 본다. 나아가 국제경쟁 속에서 생존해야 하는 일개 단위 국가가 지속 발전이라는 목표를 달성하려면 어떤 방식의 기업지원이 필요한지, 어떤 속도의 변화를 지원할 것인지, 또한 어떻게 국내정책과 법체계를 변화시켜 나가야 하는 지 연구해 본다.

Primary Students: GIST EECS College Students

Off Campus Students: Public Servants/Research Staffs at Government Funded Research Institutes/Staffs/Citizen

On-line participants: Everyone in the world

Official Language of Lecture: English

- **If K-Mooc Approved**, Korean lecture with English caption or English lecture with Korean caption can be an option.

Day of Lecture: Every Thursday from 16:00 to 19:00

Place of Lecture: GIST Main Campus in Gwangju

| 시작하는 글

이 흥 노

GIST 교수

안녕하십니까,

GIST College Special Topics Course EC4310 에서 강의를 해 주시는 특강 강사분들께 다시 한번 감사드립니다. 바쁘신 가운데에 광주까지 오셔서 3 시간 강의를 한다는 게 보통 일은 아닌 게 사실입니다. 좋은 교육프로그램을 만드시느라 달려와 주시는 강사님들께, 다시 한 번 감사말씀 올립니다.

GIST 대학 학생 40 여명과 학교 내외의 청강생 20 여분이 등록해서 강의를 듣고 있습니다. GIST 학생에게는 3 학점이 부여되는 신설 정규 교과목입니다. 외부에서 강사 분들을 모시고, 정규교과목을 운영하는 것은 GIST 역사상 제가 처음 시도 해 보는 일입니다. 그러므로 많은 분들이 주목하고 있습니다. 저는 과학기술 특성화대학 GIST 가 이제는 좀더 사회에 열려 있기를 바라는 마음에, 특론을 신설하고 추진하였습니다. 개교 26 주년을 맞이한 GIST 는 교수 일인당 논문이 세계에서 3 위(2018 년 기준)입니다. 그러나 GIST 가 이제 논문만 잘 쓰는 대학이라는 이미지를 뛰어넘어야 한다고 생각합니다. 캠퍼스의 담을 허물어 사회에 개방하고 국민과 소통하고 동반 성장해야 할 때라고 생각합니다. 저는 따로 <블록체인과 미래사회>라는 대학원 교과목을 가르치고 있습니다. 대학원 과목으로 저의 책임 시수를 완수 합니다. 블록체인은 기술, 경제, 규제 등이 종합된 새로운 분야 입니다. 기술 부분은 대학원 과목에서 커버 할 수 있습니다. 그러나 나머지 부분은 해당 분야 전문가들이 직접 가르쳐야 파급효과가 큽니다.

이번 학기에 본 특론이 성공적으로 잘 운영되어서 대한민국이 암호화폐와 블록체인 분야에서 세계를 이끌어 갈 수 있도록 젊은 인재들이 많이 육성되기를 희망합니다.

2019 년 3 월 1 일

EECS 이홍노

블록체인경제 센터장

센서지능화 센터장

블록체인경제 1부

1강

2019.03.07.(목)
Introduction to Blockchain Economy
이흥노 | 광주과학기술원 교수

Blockchain and Civil Society
홍은표 | 대법원 판사

2강

2019.03.14.(목)
Blockchain and Smart City
김태원 | ㈜글로스퍼 대표

3강

2019.03.21.(목)
Tokenomics and Governance of Cryptocurrency
박창기 | ㈜팍스데이터테크 대표

4강

2019.03.28.(목)
Aritificial Intelligence, Big Data, Blockchain
이영환| ㈜딜라이트체인 대표

5강

2019.04.04.(목)
Making Ethereum Tokens and DApps
이광열 | ㈜업라이프 대표

6강

2019.04.11.(목)
Understanding Ethereum Blockchain
정순형 | ㈜온더 대표

블록체인경제 2부

7강
2019.04.25.(목)
Stablecoin & Commercial Payment BM Design
정상호 | ㈜델리오 대표

8강
2019.05.02.(목)
ICO/ IEO/ STO/ Crypto Economy
장중혁 | ㈜아톰릭스컨설팅 이사

9강
2019.05.09.(목)
Blockchain and World Economy
오정근 | 한국금융ICT융합학회 회장

10강
2019.05.16.(목)
Blockchain and Financial Policy
김기흥 | 경기대학교 교수

11강
2019.05.23.(목)
Blockchain and Regulation Reform
구태언 | 로펌 Tek&Law 변호사

12강
2019.05.30.(목)
Blockchain and Judicial System
황경태 | 법무법인 헤리티지 변호사

13강
2019.06.06.(목)
Blockchain and Innovative Nation
전하진 | 한국블록체인협회 위원장

오시는 길

광주송정역에서 GIST대학 강의동까지 택시로 약 15분 소요 (진곡산단로)
유스퀘어 광천터미널에서 GIST대학 강의동까지 택시로 약 16분 소요
※ 단시간의 버스노선이 없으므로 택시 이용 추천

Contents

블록체인경제 1부

1-1 강: Blockchain Economy 1

/ **이흥노** GIST 블록체인경제센터 교수

1-2 강: Blockchain and the Civil Society 27

/ **홍은표** 대법원 판사

2 강: Blockchain and Smart City 49

/ **김보규** 글로스퍼 본부장

3 강: Trilemma of Blockchain & Cryptocurrency Governance 68

/ **박창기** 팍스데이터테크 대표

4 강: Consensus Algorithm and Tokeneconomy 129

/ **이영환** 딜라이트 대표

5 강: Ethereum Dapp 175

/ **이광열** 업라이프 대표

6 강: Ethereum Yellow Paper & Plasma MVP 194

/ **정순형** 온더 대표

블록체인경제 2부

7 강: Blockchain and Innovative Nation 264

/ **전하진** 한국블록체인협회 위원장

8 강: Crypto Economy 설계 322

/ **장중혁** 아톰릭스컨설팅 이사

9 강: 블록체인과 세계경제 351

/ **오정근** 한국금융ICT융합학회 회장

10 강: Blockchain and Financial Policy 426

/ **김기흥** 경기대학교 교수

11 강: 디지털 혁신의 규제환경과 네거티브 법률 시스템 497

/ **구태언** 로펌 Tek&Law 변호사

12 강: Cryptocurrency and Regulation 585

/ **황경태** 법무법인 헤리티지 변호사

13 강: Stablecoin & Business Strategy 597

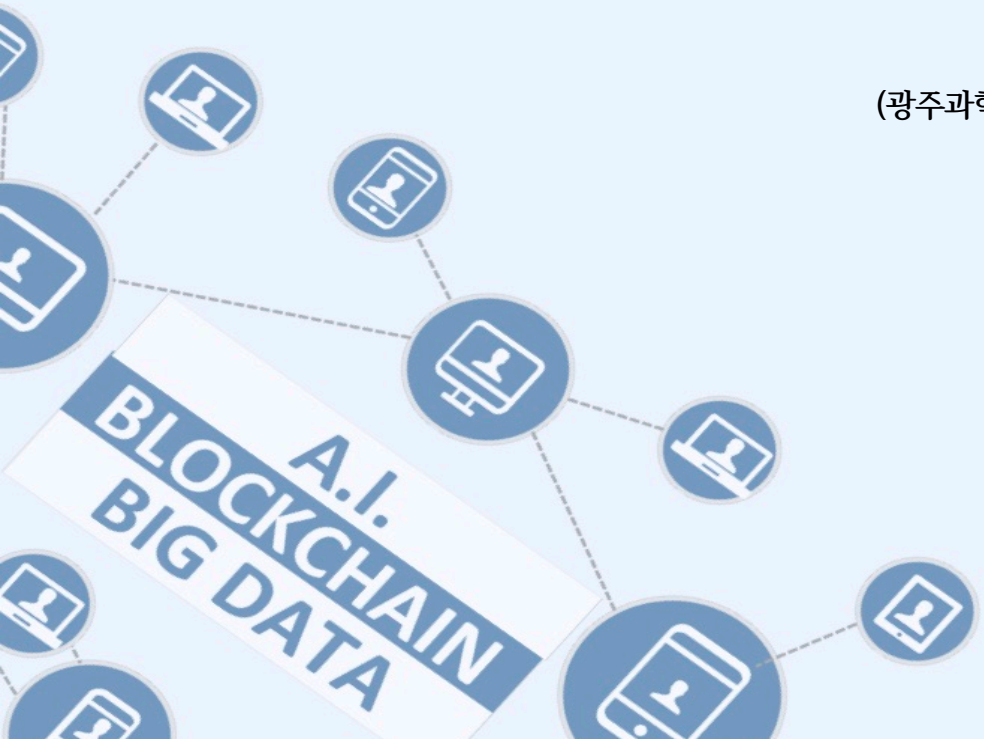
/ **정상호** 델리오 대표

1-1강

Blockchain Economy

이 흥 노 교수

(광주과학기술원 블록체인경제센터)



강의 동영상 URL

1 부: https://youtu.be/1_xI0SibZAE

Blockchain Economy

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

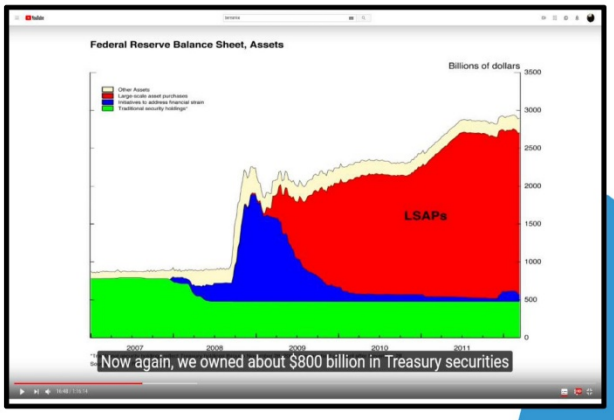
- People want an *ever improving state of self* and economic position compared to what they have enjoyed in previous years.

- **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

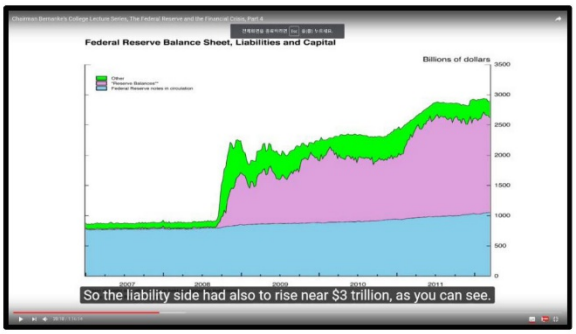
>Large Scale Asset Purchases (QE)
- Control long-term supplies of securities
- Raising the price of these assets
- Lowering the long term interest rate.



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.

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

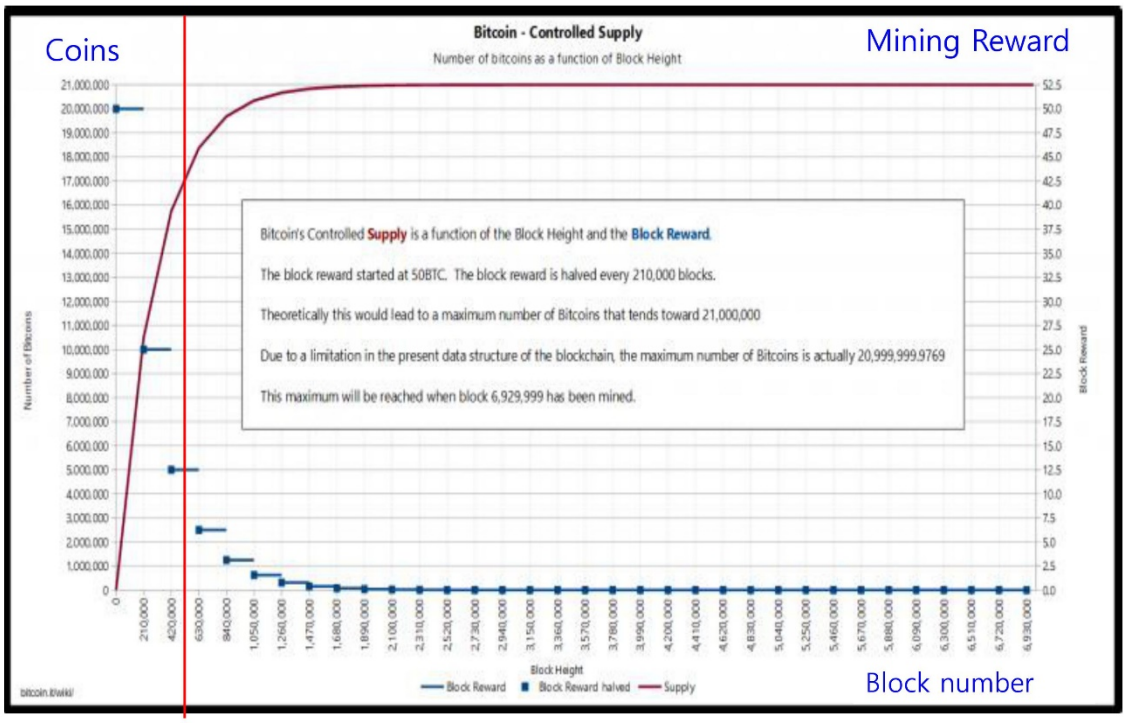
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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?

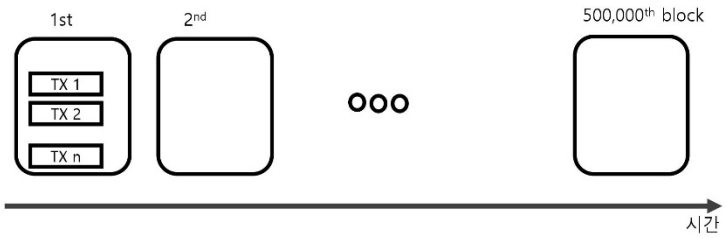
Bitcoin uses the internet.

Bitcoin attracts P2P nodes.

15

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.



16

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

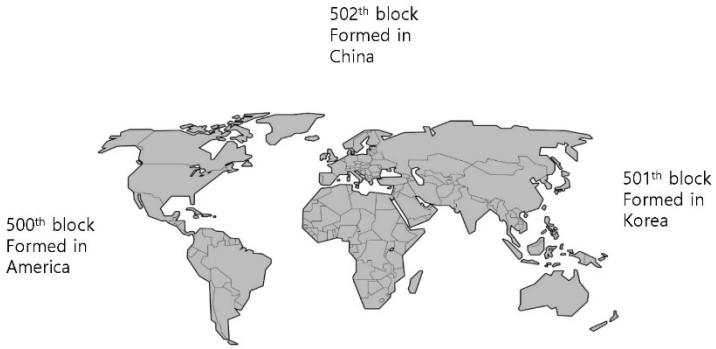
A leger in Korea

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.

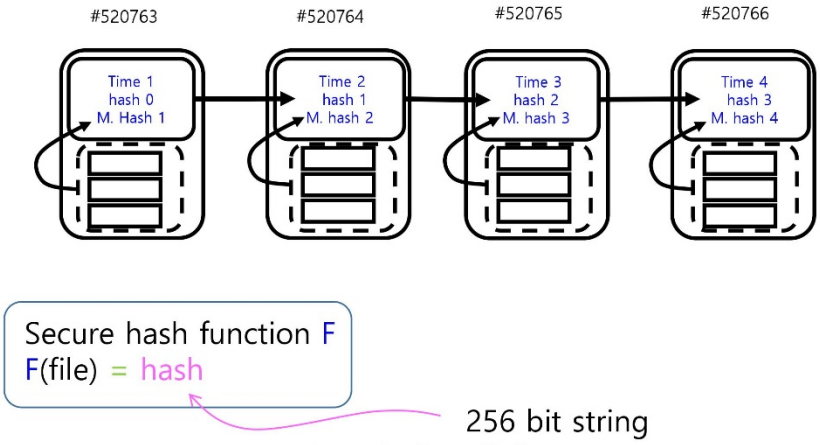


Consensus mechanism plays the key role in blockchain.

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

Blocks are cryptographically chained.

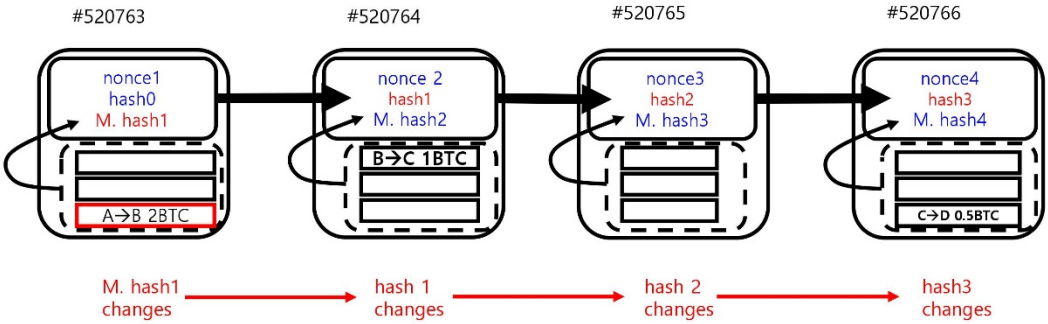
- Blocks are cryptographically chained.
- Any alteration made to the content can be easily noticed.



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.

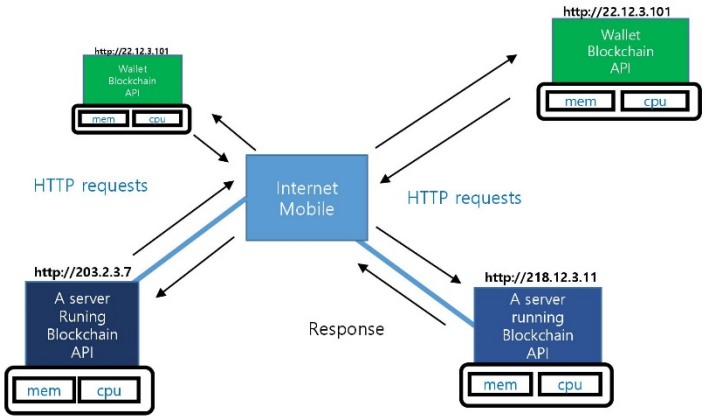
Program Suite

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

23

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

the blockchain internet



24

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

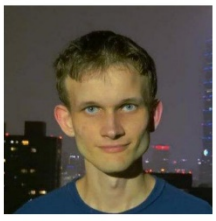
ICO, how did it get started?

- "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

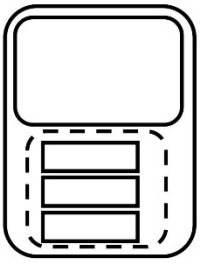
- Ethereum ICO in 2014, raising coins worth millions of dollars.



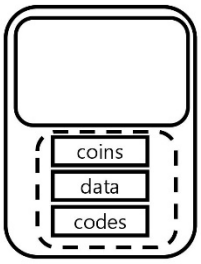
Ethereum

- 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.

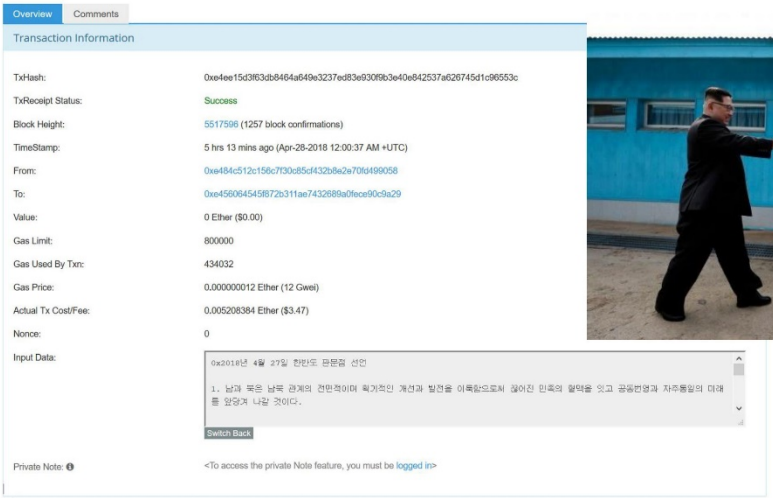
Bitcoin only
records coin TXs



Ethereum allows
data and codes as well

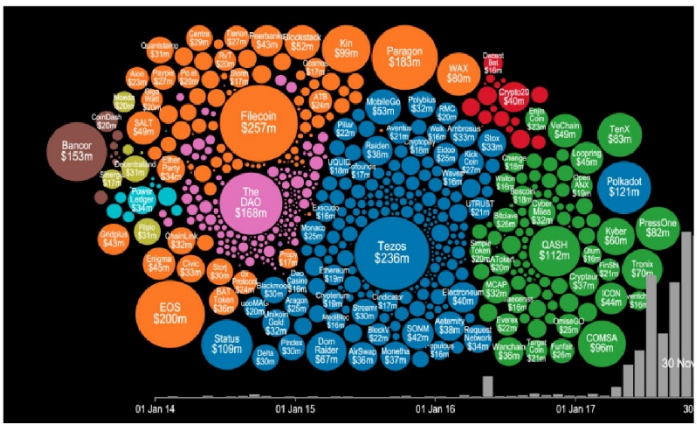


The Ethereum's block that stored the Panmunjeom Declaration



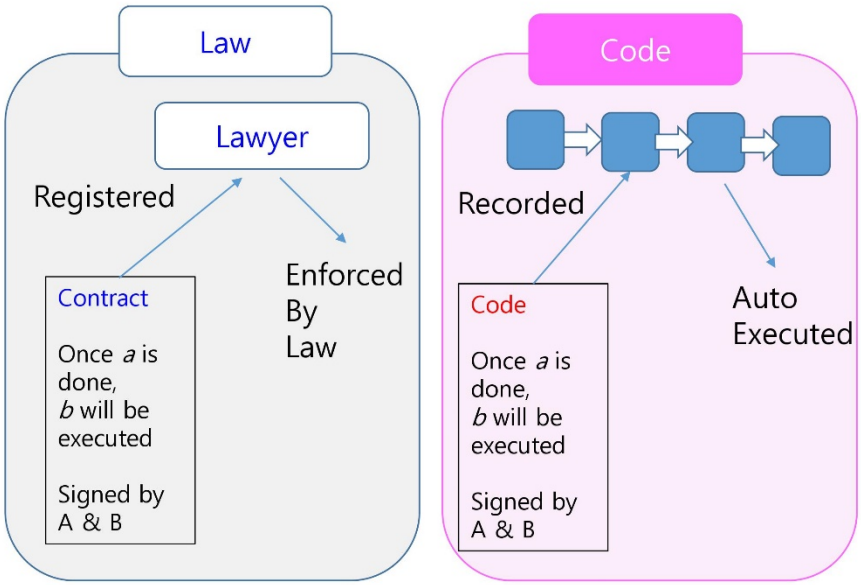
2018.04.28

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

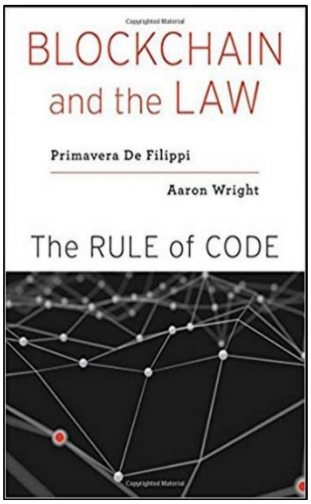
Voting

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

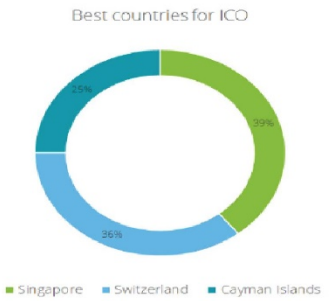
- Astronomical cost for mining
- Smart contracts
  - Bugs
  - Compliance with the law?
- *Decentralization?*
  - *Mining pools are re-centralized.*
- Not very convenient and useful as a currency (medium of exchange, storage of value)
  - Slow transactions speed, price fluctuation
- Possibilities of cyberattacks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

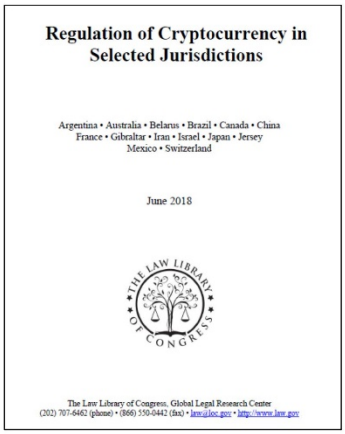
Note that we decided not to include the United States in the list after the SEC issued the Munchee order which prevented Munchee Inc., a California based company that created a blockchain application that allowed its users to post the reviews of restaurants, from continuing its ICO campaign on its second 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


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.

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.

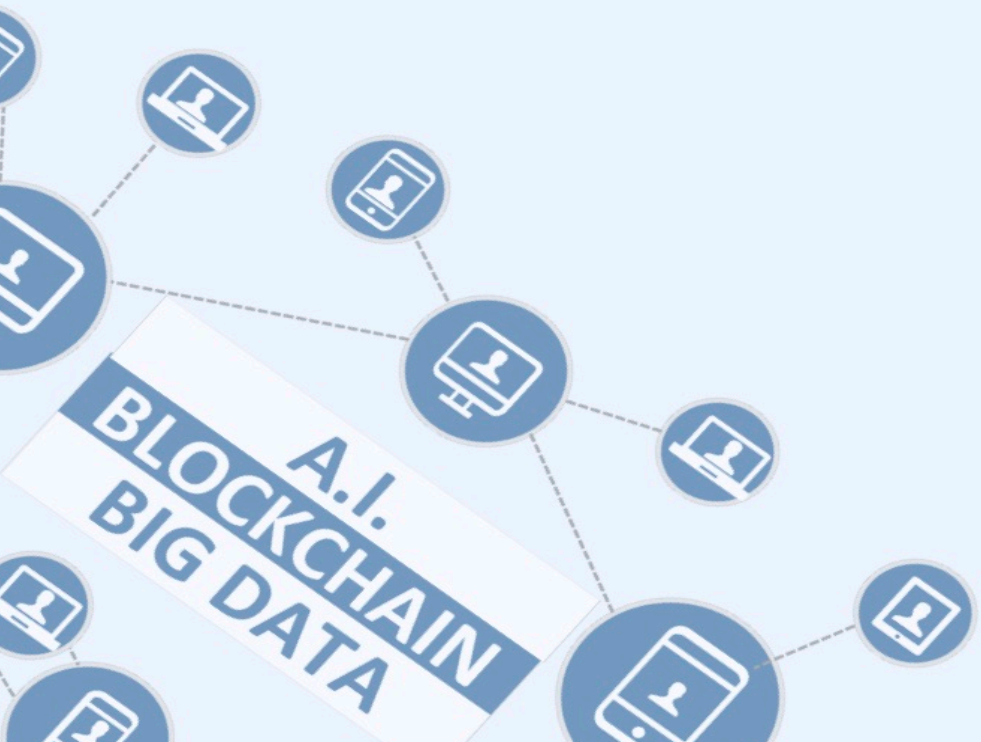
- Huge economical and societal advance is expected with the advent of the blockchain-internet.
- I term this **Blockchain Economy** which is yet to be defined precisely.

1-2강

Blockchain and the Civil Society

홍 은 표 판사

(대법원)



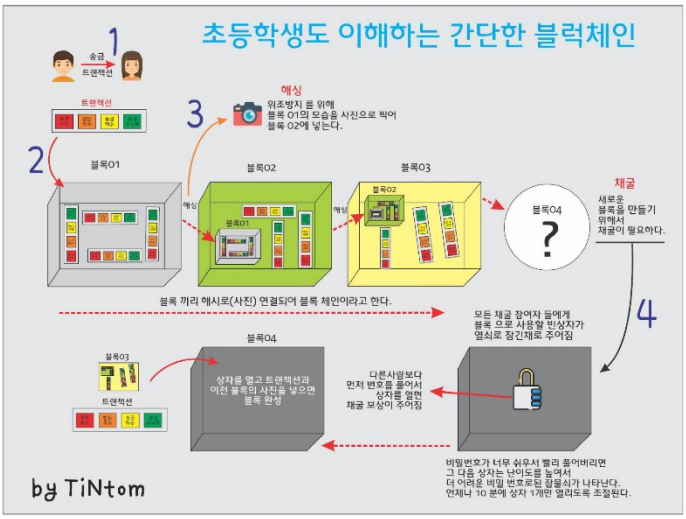
강의 동영상 URL

1 부: https://youtu.be/hQy5NXb89is

Blockchain and the Civil Society

홍은표(Eunpyo Hong)
Supreme court research judge

What Blockchain means to you?



What Blockchain means to you?

Distributed Trusted Computing

Offline Computing -> Server Computing -> Cloud Computing -> Distributed Trusted Computing

Distributed -> p2p, no central authority

Trusted -> data has value

What Blockchain means to you?

What can be done with distributed trusted computing?

Enhance individual right

- Society which respects various voices
- Society which respects individual characteristics
- Rebalance between individual and government

What Blockchain means to you?

Blockchain as a civil right

How Blockchain enhance Individual's Right?

How Blockchain enhance Individual's Right?

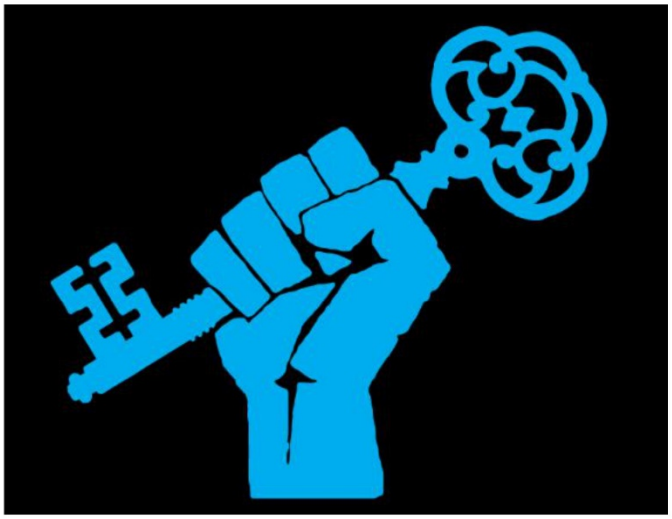
Two approach

1 Request someone to do something

2 Improve condition of individual's freedom

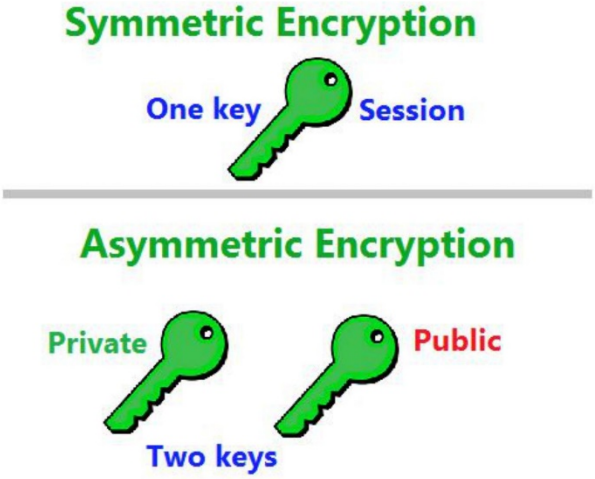
How Blockchain enhance Individual's Right?

1. Individual creation and holding of the private key



How Blockchain enhance Individual's Right?

Individual creation and holding of the private key



How Blockchain enhance Individual's Right?

2000 B.C. in Egypt

Caesar Cipher

World War II - Enigma

1976 - Diffie–Hellman key exchange

1991 - Phil Zimmermann. PGP (Pretty Good Privacy)

1992 - David Chaum, Achieving Electronic Privacy

the Arms Export Control Act

How Blockchain enhance Individual's Right?

Individual creation and holding of the private key

anti-virus software?
financial institutions?
Windows?

1996 Bernstein v. Dept of State

- software source code was speech protected by the First Amendment and that the government's regulations preventing its publication were unconstitutional

2008 - Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

How Blockchain enhance Individual's Right?

Different meaning of technology in …

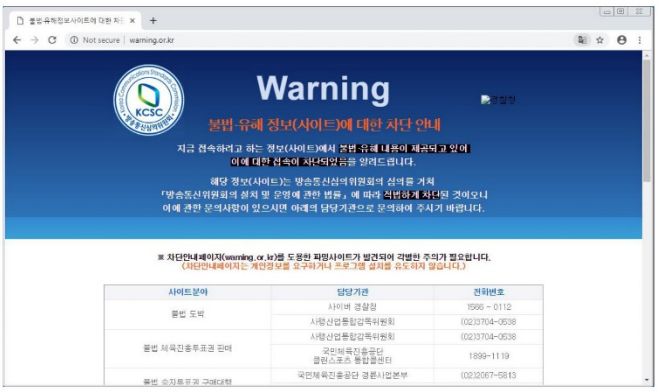
Old rural area

City

Telegraph - radio

Internet

Crypto asset

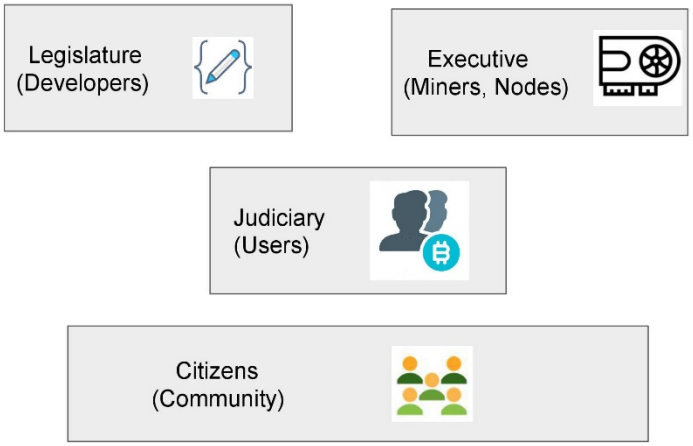


How Blockchain enhance Individual's Right?

2. Voluntary participation

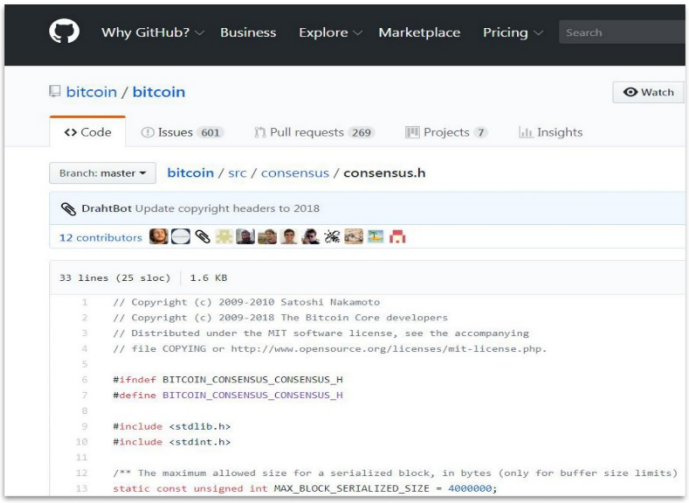
The checks and balances system

in the blockchain network



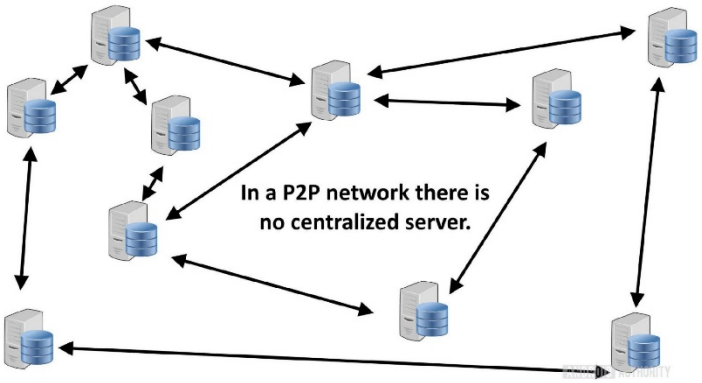
How Blockchain enhance Individual's Right?

3. Share the database and code



How Blockchain enhance Individual's Right?

4. Censorship resistance(no delete or shutdown by the government)



How Blockchain enhance Individual's Right?

2018 was the year Chinese internet users evaded censorship — briefly

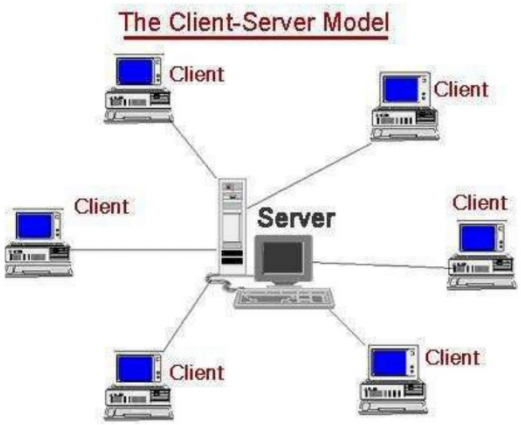
By Shannon Liao, Dec 20, 2018, The Verge

… In April, student activists posted a #MeToo open letter — written by a student who had been threatened by her college not to discuss sexual assault — into the metadata of an Ethereum blockchain transaction. Then, in July, the blockchain was used again as citizens collectively fought to preserve an investigative story that exposed how Chinese babies were being given inferior vaccines.

How Blockchain enhance Individual's Right?

Problem of Centralized Computing

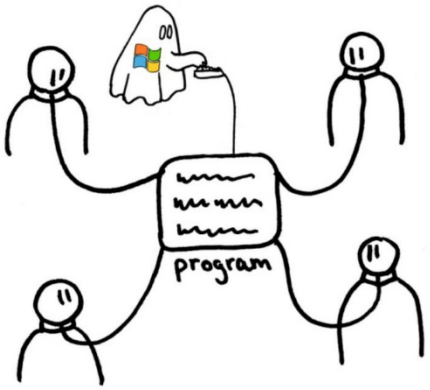
- Database concentration
- Service as a surveillance



How Blockchain enhance Individual's Right?

Problem of Centralized Computing

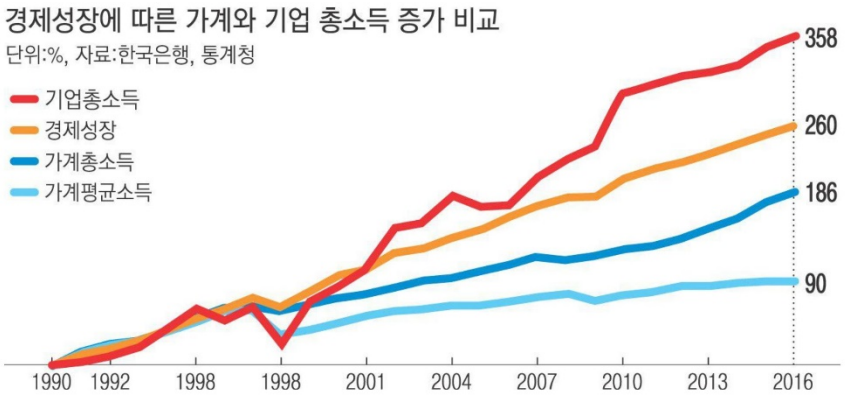
- Mind control machine
- (J.C.R. Licklider, Man-computer symbiosis. IRE Transacl 1, pages 4-11, March 1960)



Richard Stallman

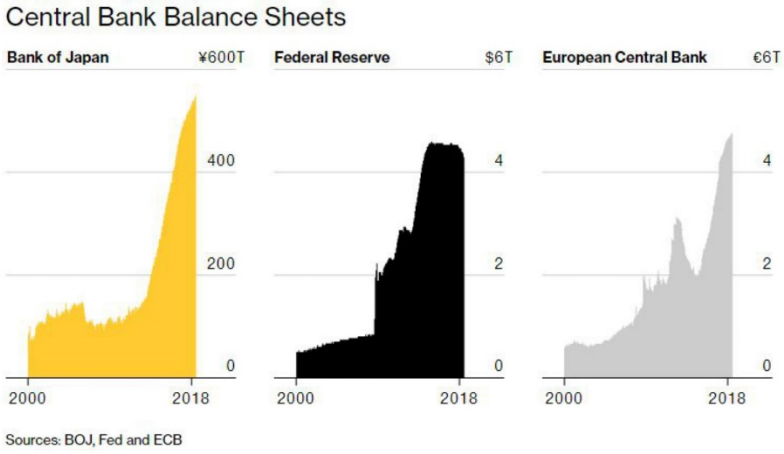
How Blockchain enhance Individual's Right?

Problem of Centralized Institution



How Blockchain enhance Individual's Right?

Problem of Centralized Institution



Freedom of Transfer of Value

Transfer of Value

1. Define and create value : by system allowing private ownership
2. Protect value : by system protecting private ownership
3. Free to make a contract
4. Protect the execution of contract : by system physically enforcing execution of contract

Freedom of Transfer of Value

Freedom of Transfer of Value without 3rd party

1. Define and create value : can choose any blockchain ecosystem + self sustainable crypto economy
2. Protect value : private key + no shutdown
3. Free to make a contract
4. Protect the execution of contract : code(an algorithmic enforcement)

Freedom of Transfer of Value

CONSTITUTION OF THE REPUBLIC OF KOREA

Article 37 (2) The freedoms and rights of citizens may be restricted by Act only when necessary for national security, the maintenance of law and order, or for public welfare. Even when such restriction is imposed, no essential aspect of the freedom or right shall be violated.

Freedom of Transfer of Value

Important Regulation about Blockchain in Korea

- AML, KYC
- Capital market regulation
- The Financial Services Commission issued a press release banning ICO

Freedom of Transfer of Value

Restrictions on Blockchain must be evaluated by the freedom of transfer of value

Restrictions on Blockchain must pass the constitutional test

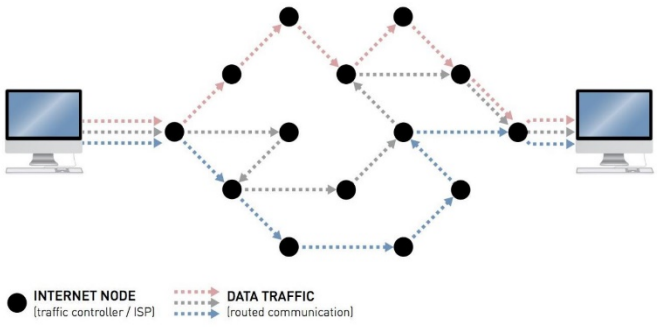
- must be provided for by law
- may only be imposed for legitimate grounds
- must conform to the strict tests of necessity and proportionality

Right to asset -> Freedom of thinking, Freedom of expression

Internet regulation, Capital market regulation and Blockchain

Internet regulation, Capital market regulation and Blockchain

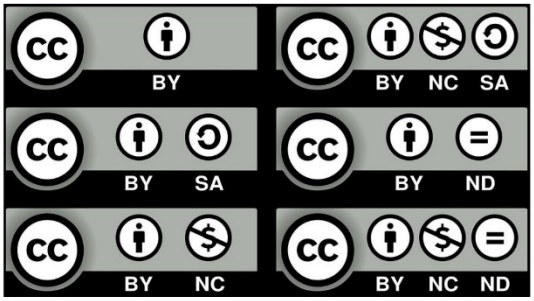
Internet - Free transfer of information



Internet regulation, Capital market regulation and Blockchain

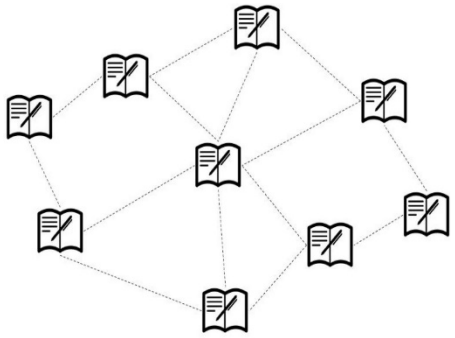
Copyright, Adult content regulation -> Freedom of expression

Internet regulation, Capital market regulation and Blockchain



Internet regulation, Capital market regulation and Blockchain

Blockchain -> Freedom of transfer of value



Internet regulation, Capital market regulation and Blockchain

기존 자본시장 도움 없이 자본 조달이 가능 - 금융기관 규제체계를 블록체인 기술에도 그대로 관철

□ 금일 '17.9.29.(금) 10:00 **김용범 금융위원회 부위원장** 주재로 「**가상통화 관계기관 합동 TF**」를 개최*

* 금융위 국조실 기재부 공정위 법무부 방통위 국세청 경찰청 한은 금감원 인터넷진흥원 관계자

○ 최근 **국내외 시장·규제 동향**에 대한 **대응조치**를 논의하고, 지난 9.1일 발표한 '**가상통화 대응방향**'의 **관계기관별 추진현황을 점검**

Ⅱ. 주요내용

□ 관계기관은 이번 회의에서,

○ 정부의 입법조치는 **가상통화 거래를 제도화하는 것이 결코 아니며,**

○ **가상통화 거래업**을 **유사수신**의 영역에 포함하되, **철저히 통제**하면서 살펴보고 **대응조치를 시행**할 것임을 강조

□ 또한, 최근 **시중자금이 비생산적·투기적인 방향**으로 몰리는 현상이 나타나고 있는 데 대해 **심각한 우려를 표명**하고,

○ 이에 따라 **생산적 투자로 전환**할 수 있도록 **추가적인 조치가 불가피한 상황**이라고 판단, 다음과 같은 대응방침을 논의함

Internet regulation, Capital market regulation and Blockchain

금융위원회가 바라본 금융시장의 문제점
(혁신성장과 일자리 창출을 위한 자본시장 혁신과제 2018. 11. 1.)

- 우리나라 기업금융시장에서 자본시장 역할은 대출위주의 시장임. 특히 중소기업의 경우 직접금융의 해택을 받지 못하고 공공자금에 의존할 수 밖에 없는 상황
- 비상장기업의 경우 증권신고서 때문에 일반공모를 통한 자본시장을 이용하지 못함
- 소액공모, 크라우드펀딩, 사모 방식은 조달금액이 적음(크라우드 펀딩 7억원, 소액공모 10억원)
- 중소기업의 자산유동화가 필요
- 개인 전문투자자군이 형성되지 못함(금융시장 잔고 5억원 이상, 자산 10억원 이상 및 등록)
- IPO 과정에서 지나친 규제로 주관사의 유인이 부족

Internet regulation, Capital market regulation and Blockchain

자유로운 가치이전은 개인의 자유이고 본질임 - 그에 수반하는 의무를 다하면 족함
(예, 세금 부과를 위해 익명성 자체를 손상?)

금융시장규제의 문제점

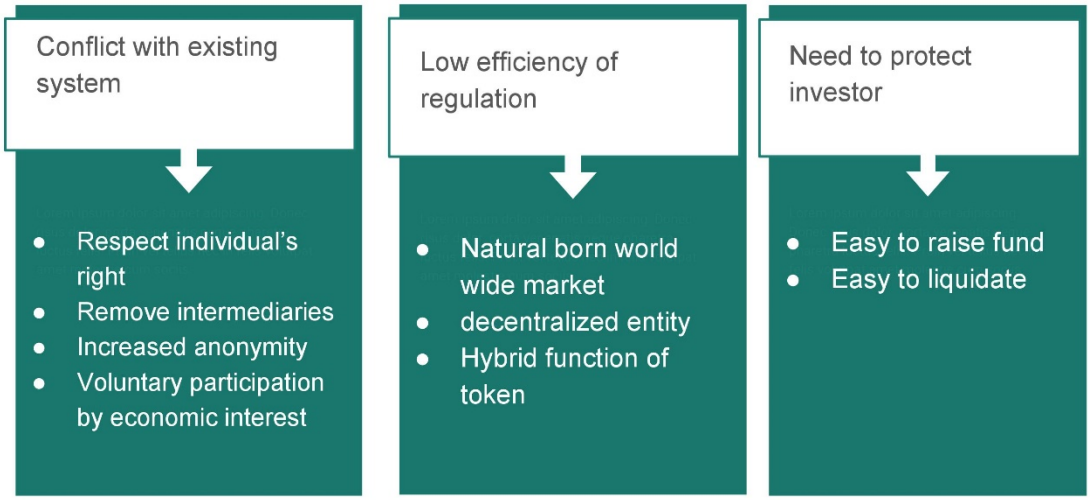
- 금융시스템 위험관리가 주된 목표(기술혁신, 소비자 보호는 뒷전?)
- 사전 규제 위주 - 혁신하려는 개발자들이 줄어들어 실제로 혁신을 가로막을 수 있음
- 기존의 틀 관철 시도 - 새롭게 발전하는 기술이 위법인지 아닌지 불분명한 상태가 계속됨
- 블록체인의 다른 장점을 규제하게 되는 결과가 될 우려
- 금융시장규제는 금융기관을 압박하여 컴플라이언스를 얻어내는 형태 - 기술발전에 유연하게 대처하기 어려움. 블록체인 규제방안으로 실효성에 문제가 있어 과도한 제재로 돌아설 우려

Internet regulation, Capital market regulation and Blockchain

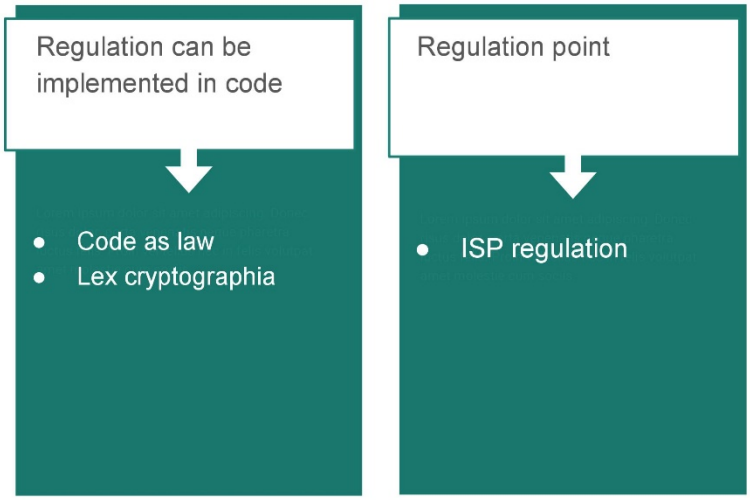
처음에는 형사처벌 + 캠패인 + 거래소 규제 + 프로토콜 규제로 이어질 가능성 -
자유로운 가치이전 보호방안은?

How to regulate

How to regulate



How to regulate



How to regulate

Need more consistent channel to discuss with developers, entrepreneurs, government.

Need to find working principle which civil society can understand.

Conclusion

Blockchain as a human right

Regulation should respect constitution

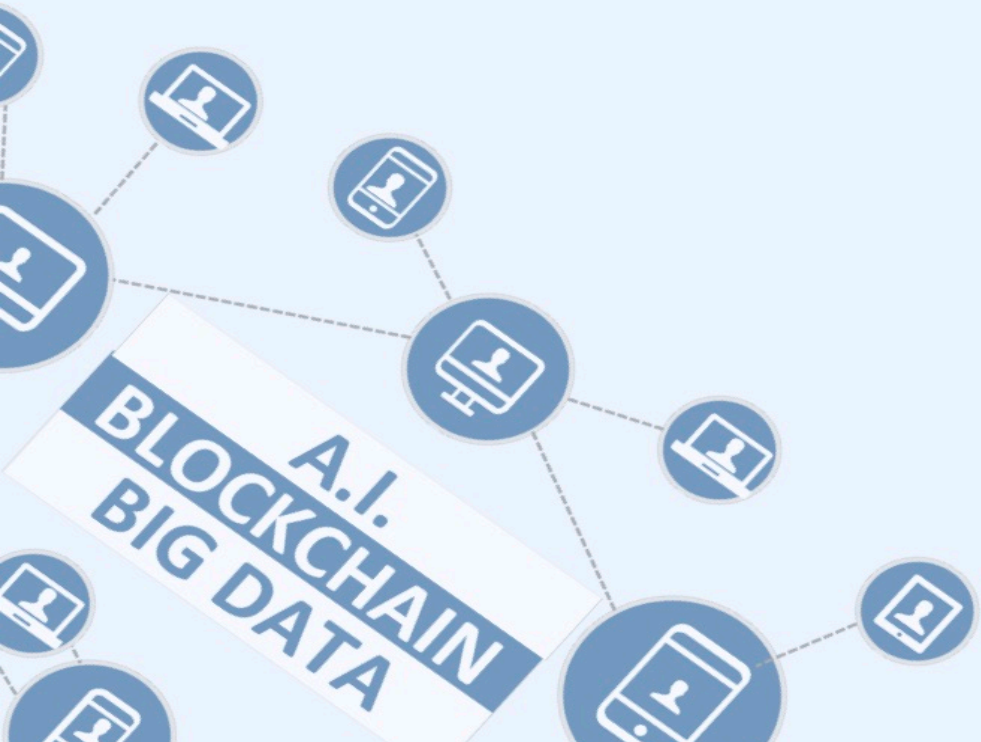
freewiki.net

2강

Blockchain and Smart City

김 보 규 본부장

(주식회사 글로스퍼)



강의 동영상 URL

1 부: https://youtu.be/O-FJapiboFc

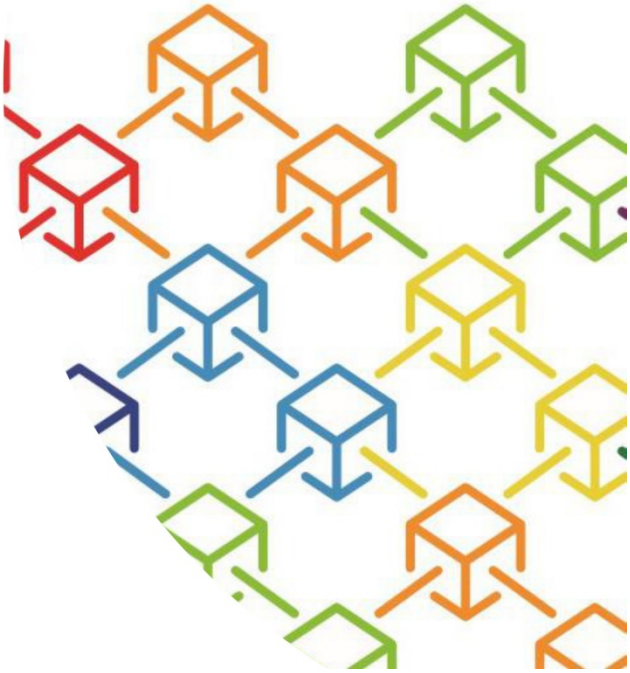
2 부: https://youtu.be/jEOA57ln34Q

- Questions are always welcomed
- Prefer to having real issue talk and conversation
- Before closing, let's have a quick drill

BEFORE WE GO

Introduction
Blockchain and industry

WHAT IS BLOCKCHAIN ?

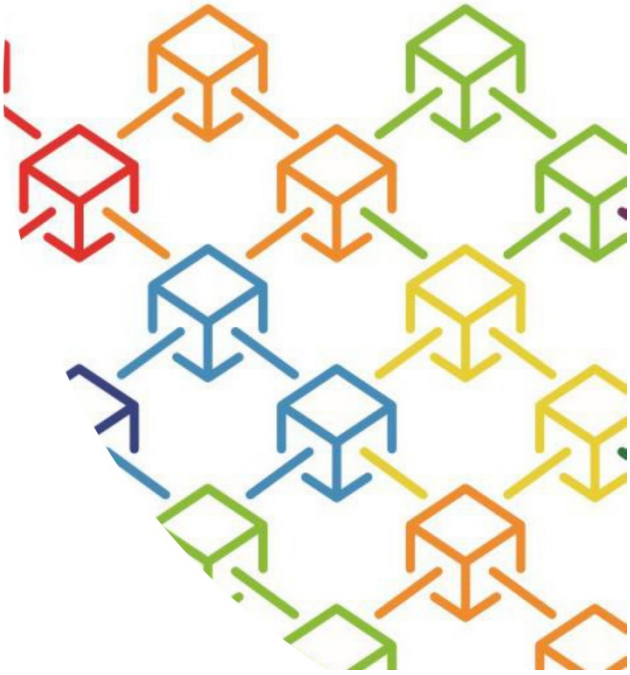


- **A blockchain is a growing list of records, called blocks, which are linked using cryptography.** Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).

- By design, **a blockchain is resistant to modification of the data**. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"... **Once recorded, the data in any given block cannot be altered** retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

<source: Wikipedia>

THEN, WHY BLOCKCHAIN ?



Security
- Data cannot be altered or removed

Transparency
- Secured data is accessible to all participated members

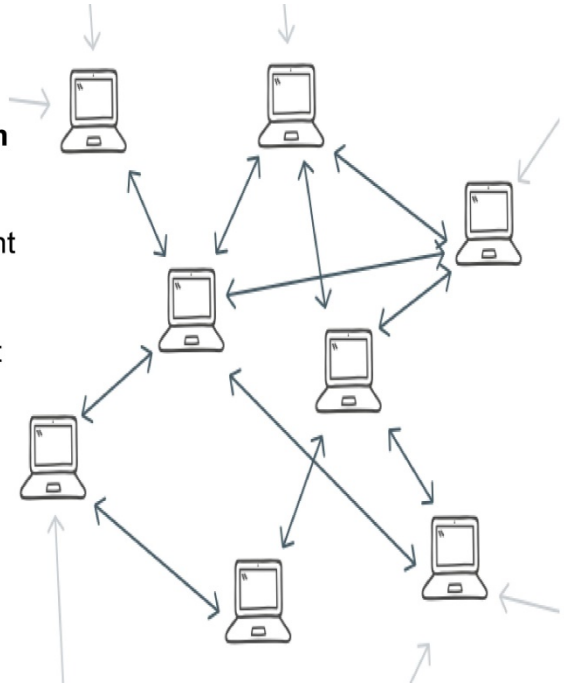
BITCOIN(฿)

- **A proof to show security and transparency**
- Cryptocurrency
- Deposit/Withdraw/Wallet based on public blockchain network
- Decentralized digital currency and ledger without a central bank

TDMS

Transparent Data Management System

- Secure, transparent data management system for Enterprise, Government
- Decentralized digital currency without a central bank
- A way of proof to show security and transparency



Major business sector

FINTECH

- Currency
- Payment
- Investment
- Remittance

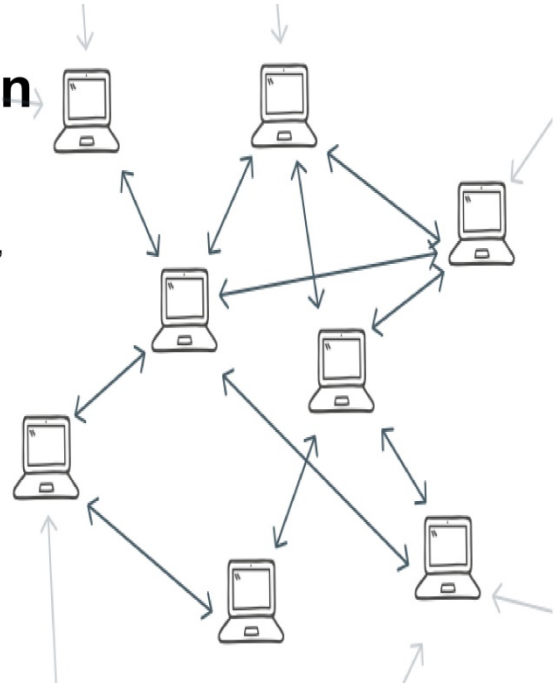
Enterprise/Government

- Transparency
- Fair evaluation
- Digital documents
- Certificates

Enterprise Blockchain

for Enterprise and Government

- Enterprise/Government requires robust, reliable and support-ready solutions
- Most of blockchain solutions in the market does not meet the requirement
- 'The enterprise blockchain' meets the requirement and fits for Enterprise/Government use.



Enterprise Blockchain

Cost vs. DBMS with security

100

Enterprise Blockchain

132

DBMS + Security solution
to support Ent. Blockchain

References
Blockchain and industry

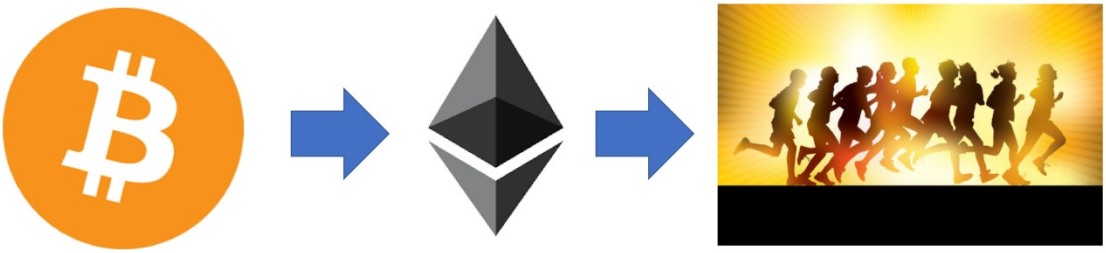
Local Cryptocurrency
지역화폐 노원
2차 사업 진행 중
지역화폐 플랫폼 특허 출원
보유 금액
15,000 원

Busan Port Authority
컨테이너 부두간 발출입증 통합 발급 시스템
환적 컨테이너 반・출입 프로세스에 블록체인 기술을 활용한 E-Slip 통합 발급 시스템

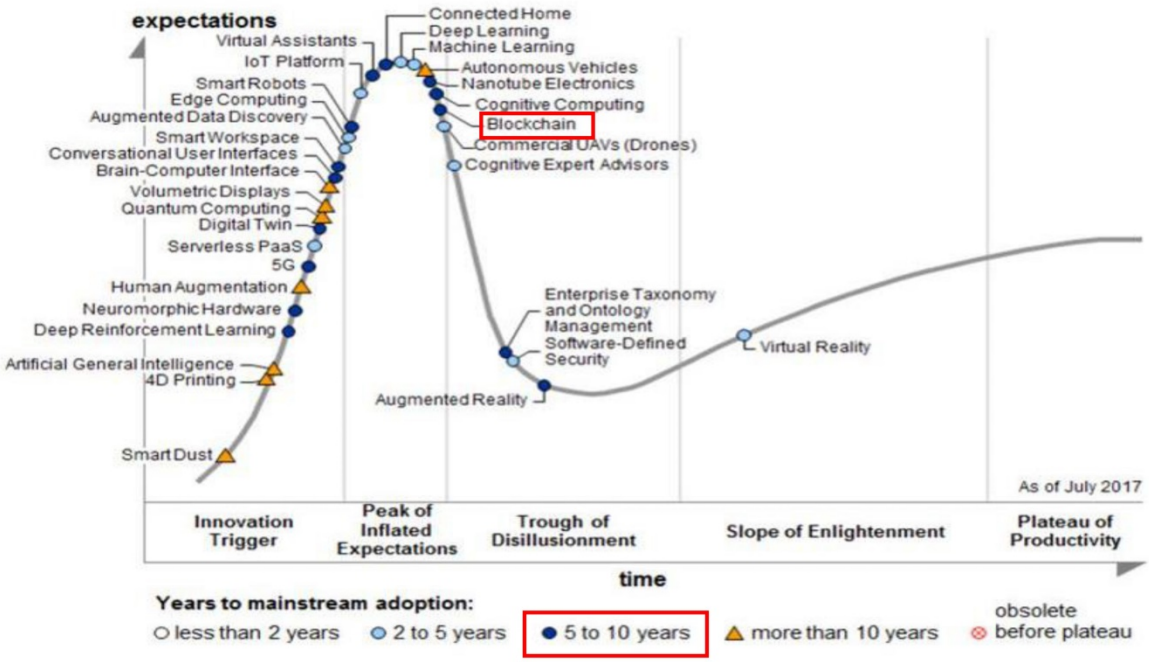
UPMusic
음원 등록, 인증, 유통, 사용료 분배, 정산 프로세스의 신뢰성을 보장할 수 있는
블록체인 기반 뮤직 플랫폼

Blockchain technology
Present and outlook

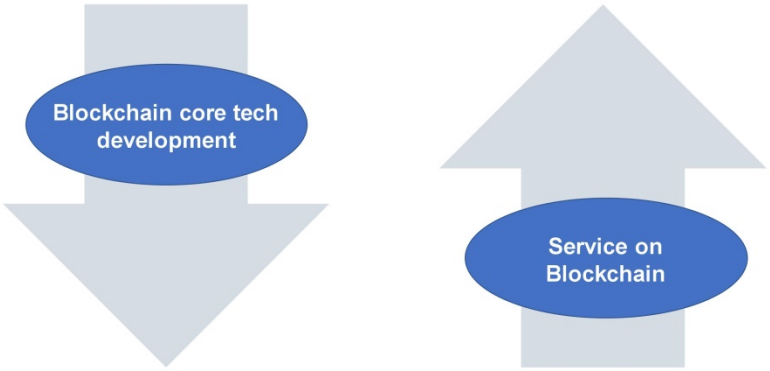
Generations of Blockchain technologies



BITCOIN	ETHEREUM	Future generation
• Pure-coin purpose	• Smart Contract • dApp support	• Smart Contract • dApp support • Faster speed and more



Future of blockchain industry

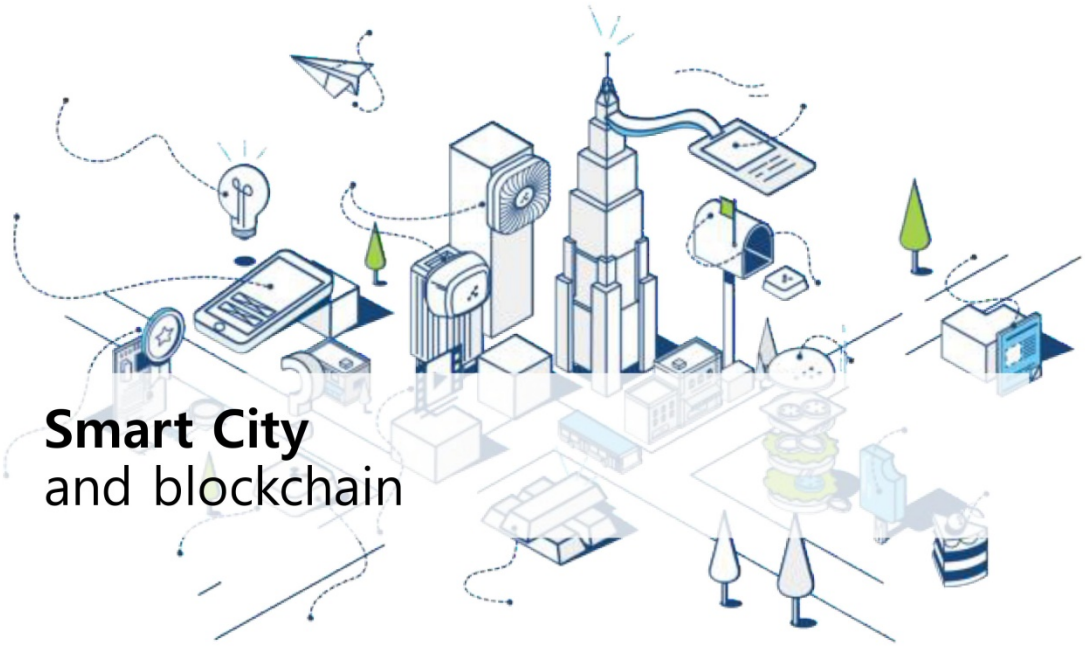


What market wants

Performance:
Fast enough speed for massive transactions

Proven transparency:
to ensure safe transaction and store

Expandability:
Expandable to support growing transactions



Smart City
and blockchain

What is Smart City?

A smart city is an urban area that uses different types of electronic data collection sensors to supply information which is used to manage assets and resources efficiently. This includes data collected from citizens, devices, and assets that is processed and analyzed to monitor and manage traffic and transportation systems, power plants, water supply networks, waste management, law enforcement, information systems, schools, libraries, hospitals, and other community services.
<Source: Wikipedia>

Simply saying,
'A city with ICT technology that helps to upgrade peoples' satisfaction and operation efficiency'

Smart City case study - Korea

Better Security

- Anyang city - crime data analysis
- Crime rate down 18.5%
- Arrest rate up 25.3%

Smart traffic

- Namyangju city – Traffic control
- 7.2km/h speed up
- 30% citizen satisfaction level up

Green energy

- Pangyo smart city - Heat/Power plant control
- Real time communication with incinerator, Water treatment system

Smart City with blockchain

Up to now, Smart City has been all about 'sensor', 'metering' and 'data'.

Blockchain can add features like:

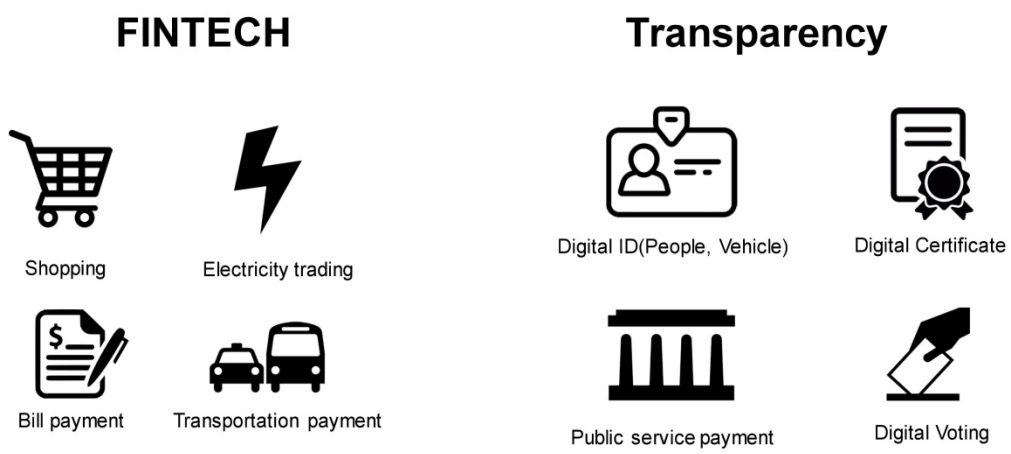
FINTECH

- Digital Currency
- Digital payment

Transparency

- Transparent evaluation
- Related Gov't service

Smart City with blockchain



Can we try quick Smart City planning?

How about Smart ‘Campus’?

Steps of finding solutions

- Step 1. Find issues
- Step 2. What's the answers to the issues?
- Step 3. With what technology we can support the answers?

Case #1

Issue:
Campus needs support from students for certain purpose. Let's say high-performance students award.

Answer:
A voucher valid in a campus for various purpose can be awarded for high-performed students, it can stimulate students to earn higher-grade.

Technology:
Campus currency(Blockchain-based cryptocurrency valid in a campus) can support the answer above.

Case #2

Issue:
Document-based graduate certificate is required for many purpose. But it cannot be validated online easily.

Answer:
Online-based certificate, which requires no additional validation, would help.

Technology:
Blockchain-based certificate support online certificate which requires no additional validation.

Case #3

Issue:
Low participation of students and online voting is considered. However, many people doubt transparency issue of online voting.

Answer:
Secure and transparent online voting system is the answer. If students can get additional benefits(like campus voucher) when they join the voting, it'll boost voting rate.

Technology:
Blockchain-based online voting system is secure and can present real-time voting result.

What is your issues in GIST?

What could be the answers?

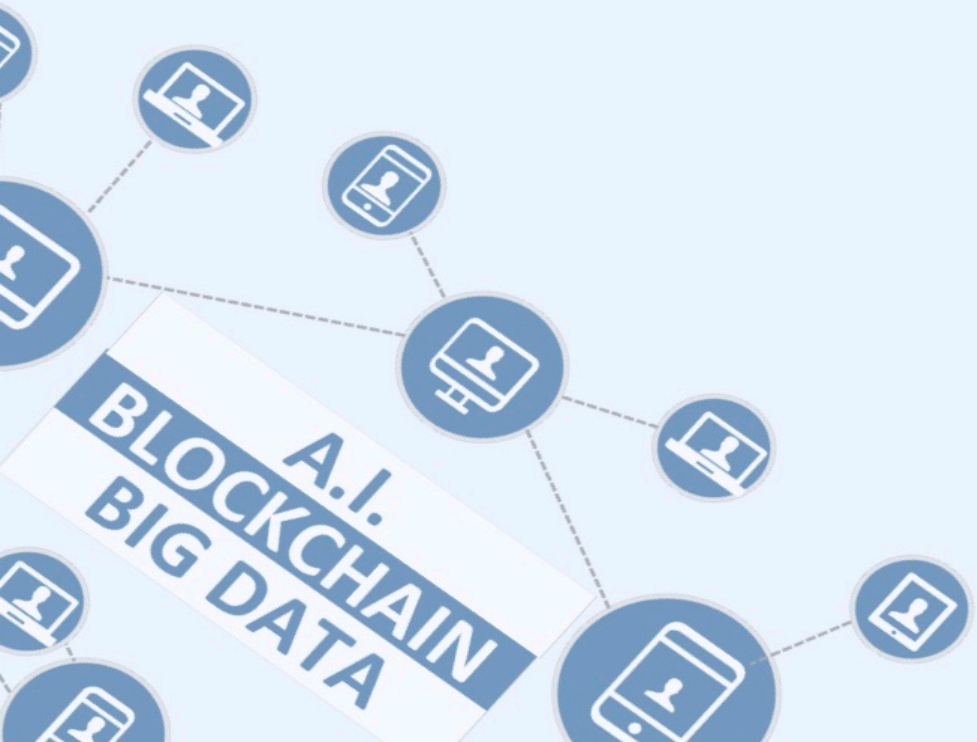
Blockchain meets your requirements?

3강

Trilemma of Blockchain & Cryptocurrency Governance

박 창 기 대표

(주식회사 팍스데이터테크)



강의 동영상 URL

1 부: https://youtu.be/hB8tuoLbbSI

2 부: https://youtu.be/3YvDWjs-PVI

Trilemma of Blockchain & Cryptocurrency Governance

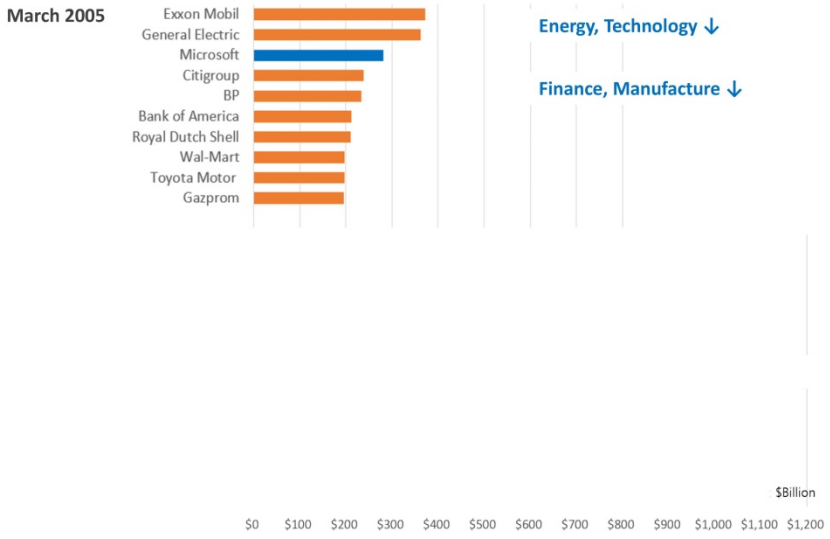
@GIST

March 21, 2019

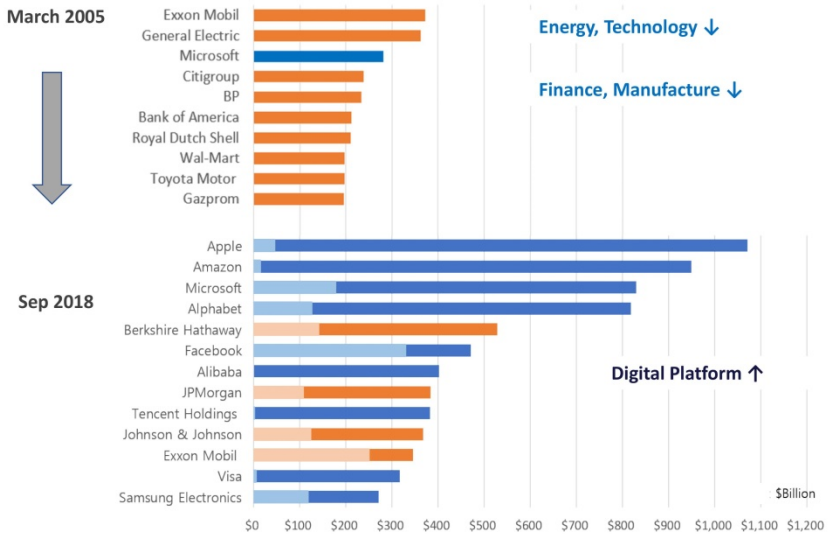
color

Changki Park
/ CEO

Market Capitalization Change



Market Capitalization Change



The Nobel Prize for Economics

Nobel Prize 2014

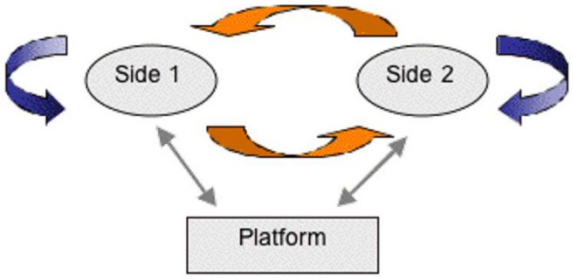
French university professor Jean Tirole becomes a laureate for his **"analysis of market power and regulation"**

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



Founding Father of Platform Economics Wins Nobel Prize

By **Nicholas L. Johnson** on October 16, 2014

2014 Novel Prize

Economics

[Game Theory]

[Analysis of]

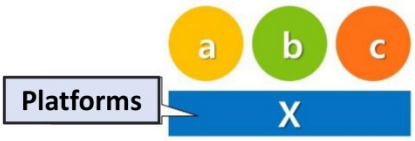
[market power and regulation]

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



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

X | 기차역, win OS, **공통역량**
a,b,c | 노선, 응용프로그램, **핵심역량**

Online Platforms

Offline Platforms

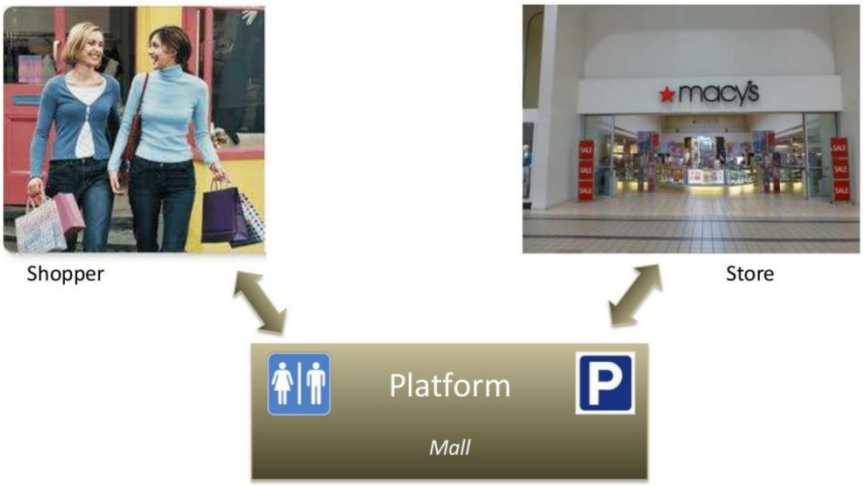
Platforms credit cards

Card holder

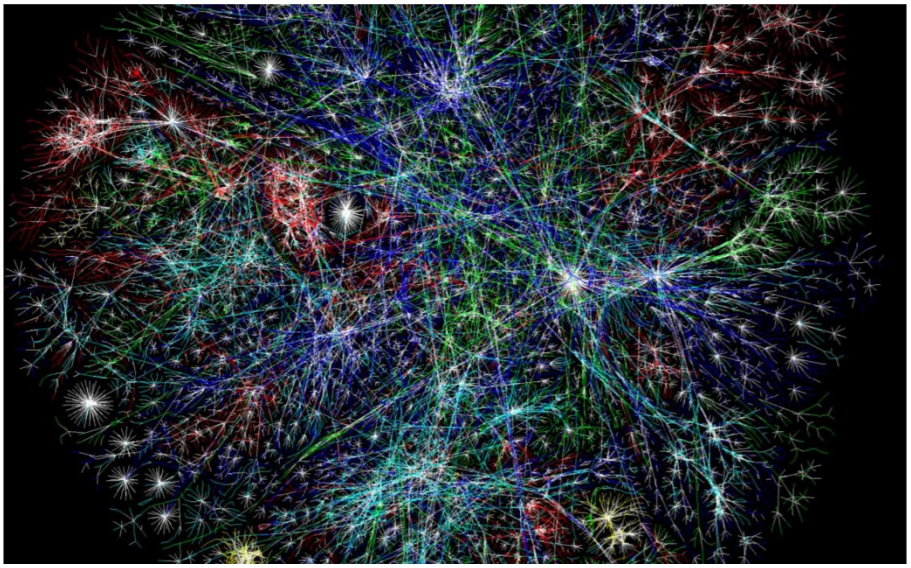
Vendor

Bank

Platforms: Shopping Mall

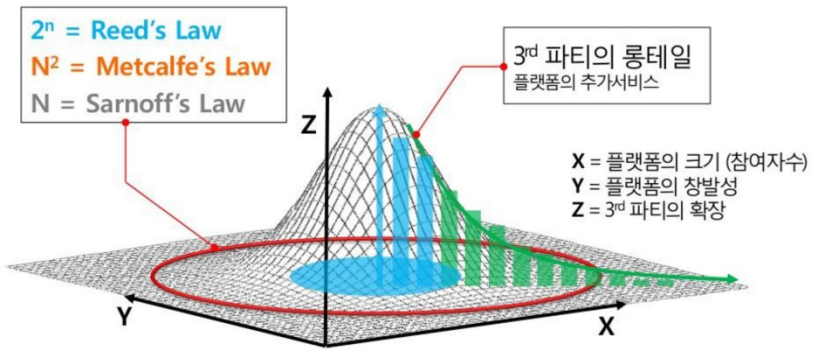


Internet Platform



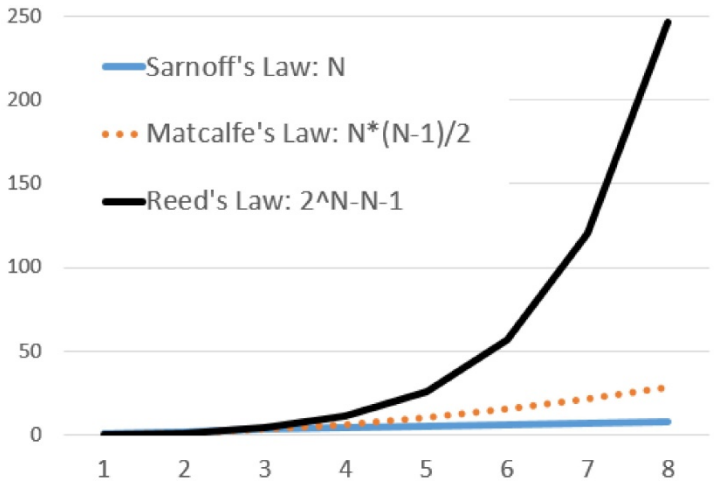
Value of Platform

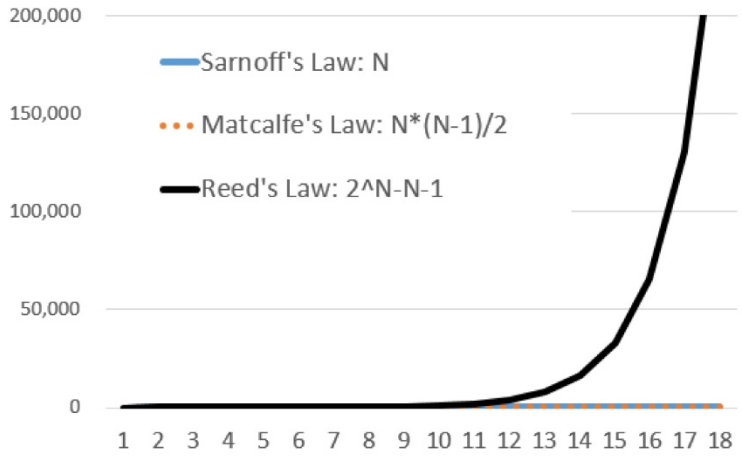
Value of Platform = # of Nodes x Stickiness x 3rd Party



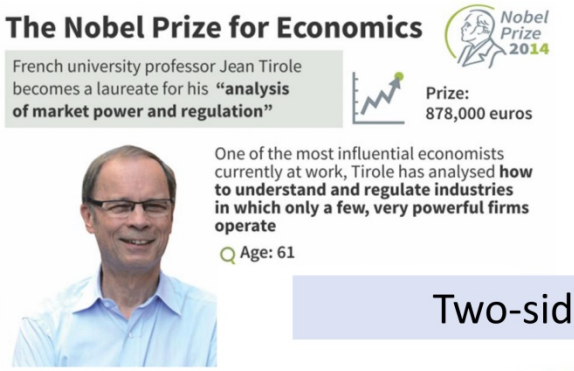
All rights reserved by Korea Creative Economy Research Network

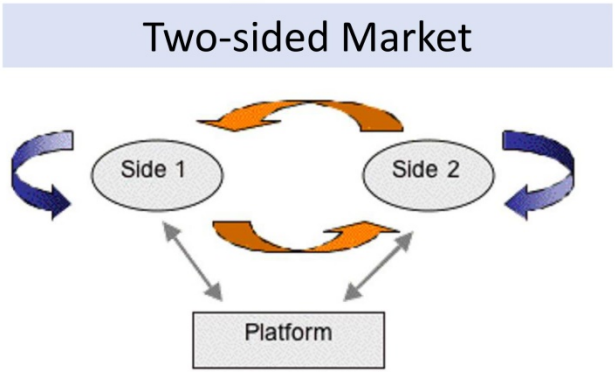
창조경제연구회





2-sided Market



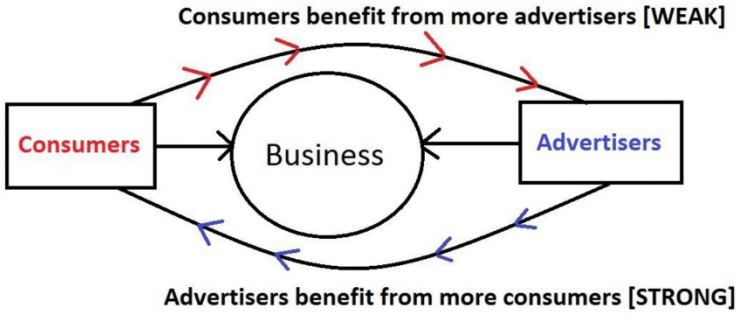


Two-sided Market

Two-sided Market

Two-sided Market

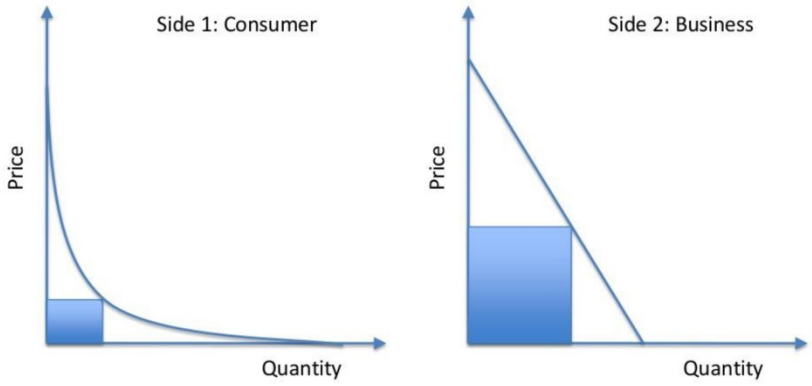
Two-Sided Market



Facebook, YouTube :
Content Provider vs Advertiser

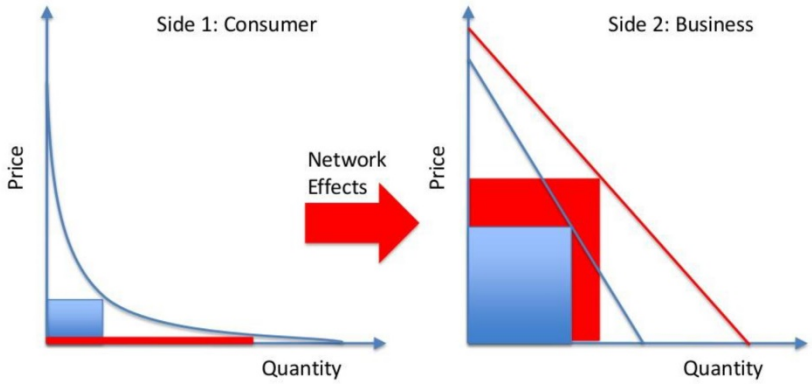
Apple:
App Store revenue is 30%
App Developer vs Paid App users

Independently maximize each market



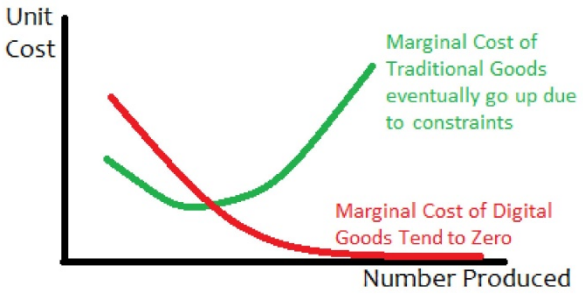
Neglects critical network effects

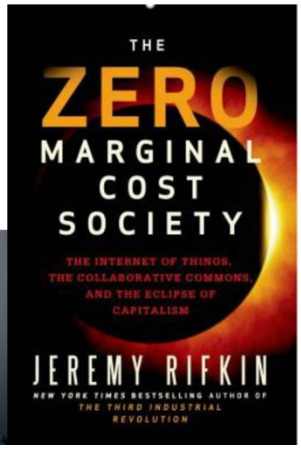
Collectively maximize both markets



Total of red boxes must exceed blue

Leverage network effects



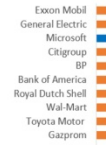


2 View points on Network Effect

Natural monopoly **Externality** **Market Failure**	Need regulation
Productivity up **Consumer utility** **Zero-marginal cost**	Minimum regulation

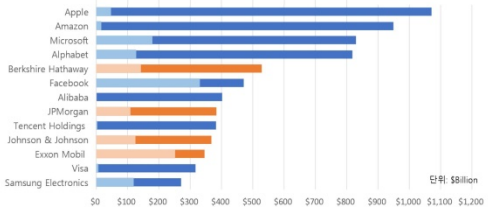
Market Capitalization Change

2005



Capitalism → **1-sided market**

2018



Digital Platform → **2-sided market**

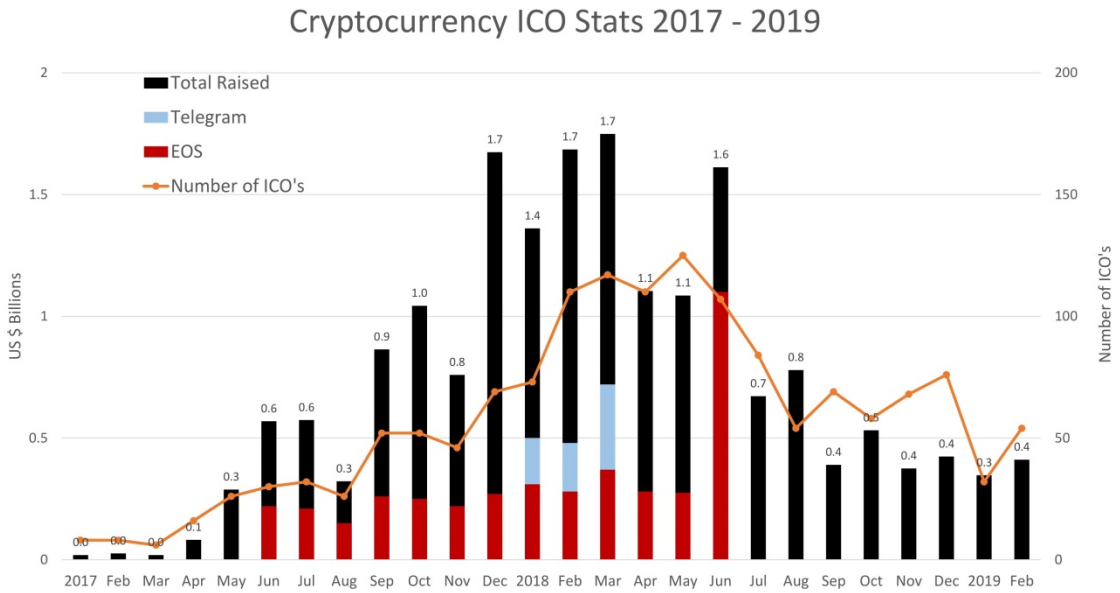
2020

?

Crypto Platform → **3-sided market**

Bitcoin Charts
Linear Scale
Log Scale
Zoom 1d 7d 1m 3m 1y YTD ALL
From Dec 28, 2016 To Mar 20, 2019
$320B
$240B
$160B
$80B
$0
Market Cap
$20,000.00
$15,000.00
$10,000.00
$5,000.00
$0
Price (USD)
24h Vol
60B
0
Mar '17
Jun '17
Sep '17
Dec '17
Mar '18
Jun '18
Sep '18
Dec '18
Mar '19

Ethereum Charts
Linear Scale
Log Scale
Zoom 1d 7d 1m 3m 1y YTD ALL
From Dec 27, 2016 To Mar 20, 2019
$120B
$90B
$60B
$30B
$0
Market Cap
$1,200.00
$900.00
$600.00
$300.00
$0
Price (USD)
24h Vol
6B
0
Jan '17
Apr '17
Jul '17
Oct '17
Jan '18
Apr '18
Jul '18
Oct '18
Jan '19


Cryptocurrency ICO Stats 2017 - 2019
Total Raised
Telegram
EOS
Number of ICO's
US $ Billions
Number of ICO's
2
1.5
1
0.5
0
200
150
100
50
0
0.0 0.0 0.0 0.1 0.3 0.6 0.6 0.3 0.9 1.0 0.8 1.7 1.4 1.7 1.7 1.1 1.1 1.6 0.7 0.8 0.4 0.5 0.4 0.4 0.3 0.4
2017 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2018 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2019 Feb

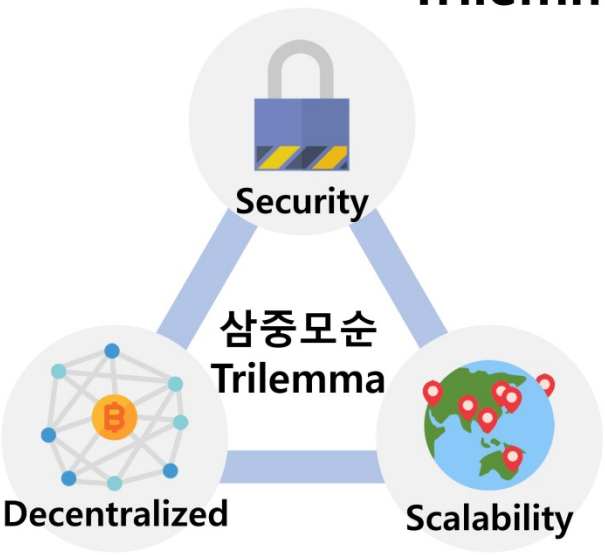
Smsung
Galaxy S10
Blockchain
KeyStore
55°

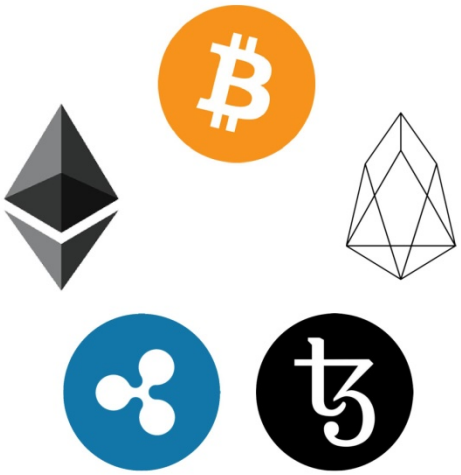
Samsung Blockchain
Keystore 사용을
환영합니다!
지갑 설정
기존 지갑 가져오기
새 지갑 만들기

20 ETH
2 ETH
0.00042 ETH
0.00023 ETH
0.00008 ETH
2.00042 ETH
다음
블록체인 키를 사용하는
그 순간에 안전하게 보호됩니다.
PIN 사용

Samsung Galaxy S10 will have
Built in Crypto Wallet
12
45
12
45
SAMSUNG
E-Wallet

Trilemma





$20,000 → $4,000

$1,300 → $100

Slow

Expensive

Dangerous

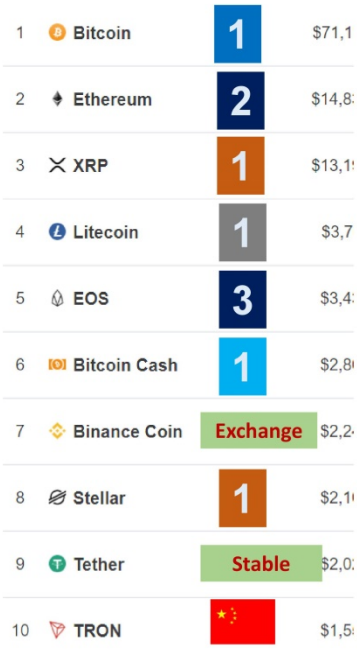
& Re-centralized

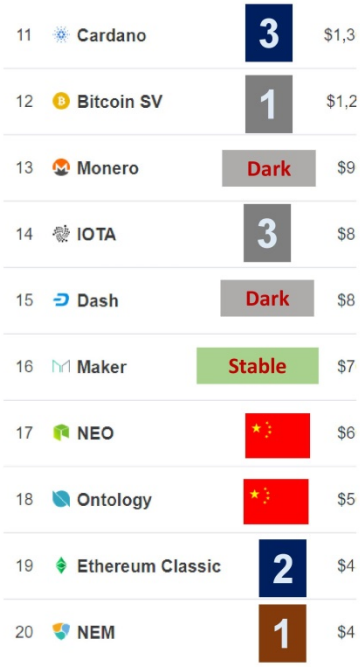
Bitcoin: centralized

Bitcoin Cash: hard fork War

Ethereum: PoW → PoS Transit Delayed

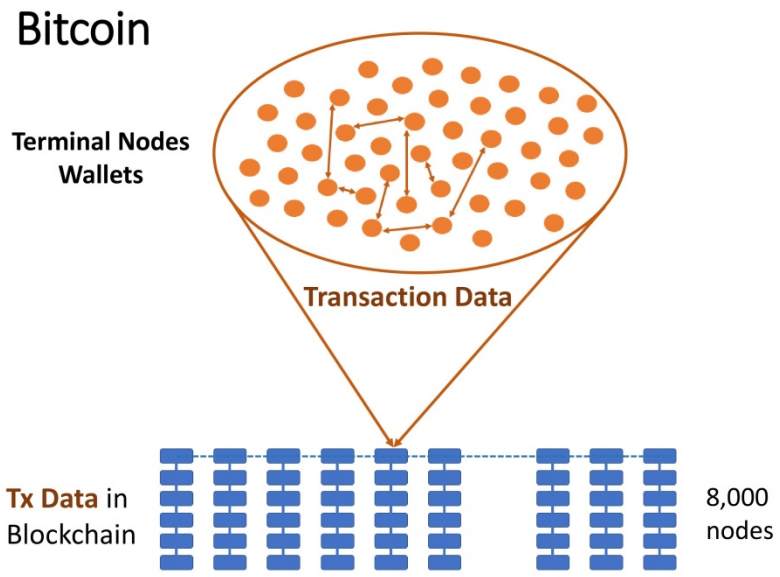
2,000 ICO – Mostly failed

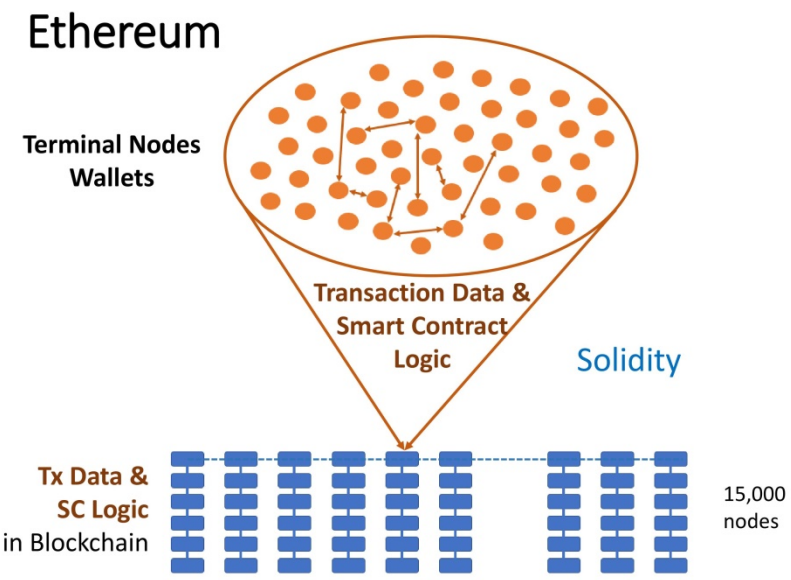


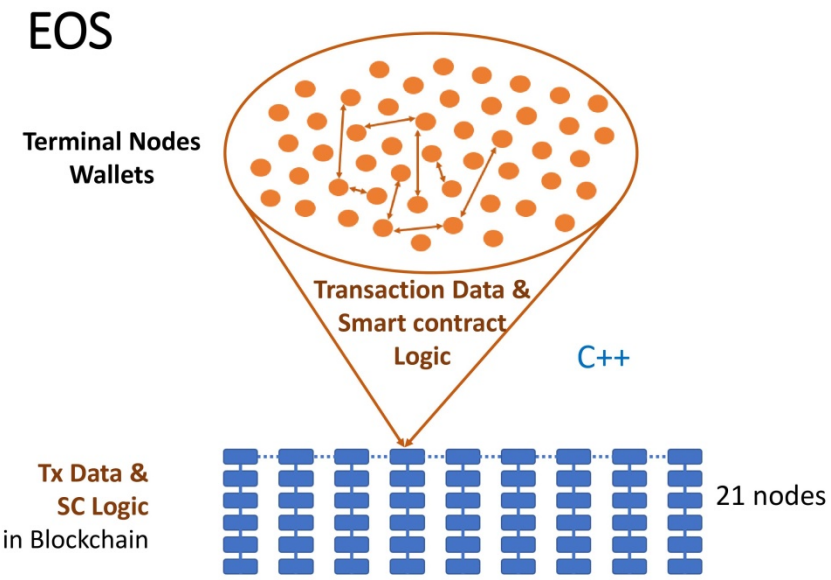


Blockchain Performance

color

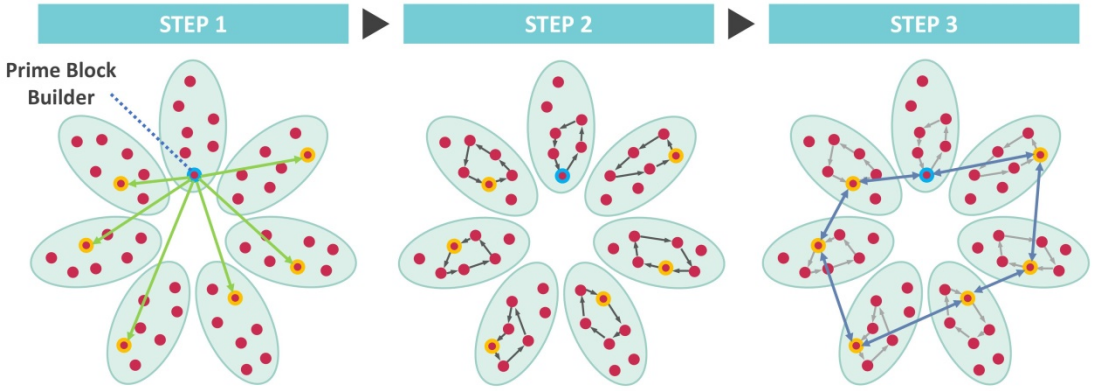



Ethereum
Terminal Nodes
Wallets
Transaction Data &
Smart Contract
Logic
Solidity
Tx Data &
SC Logic
in Blockchain
15,000
nodes


EOS
Terminal Nodes
Wallets
Transaction Data &
Smart contract
Logic
C++
Tx Data &
SC Logic
in Blockchain
21 nodes

Prism

Prism is a DPoS consensus method that utilizes **parallel BFT** (Byzantine Fault Tolerance) to provide faster consensus and settlement speed, structured in leagues with governance meant to curtail cartels.



Step	EOS	Color Prism
Producing Block	10ms	10ms
Sending/Receiving Block	To 20 BPs - 200 ms	To 6 LBB's in 6 Leagues - 150 ms
Sending/Rec Second Block	n/a	To 6 BB inner league 50ms
Consensus Confirm	Among 21 BP 700ms	Inner League 100 ms
Consensus Second Confirm	n/a	Among League 100 ms
Total:	910 ms	410 ms

[Figure 3 - Confirmation Speed Comparison Chart]

PoW **Proof of Work** **BTC**

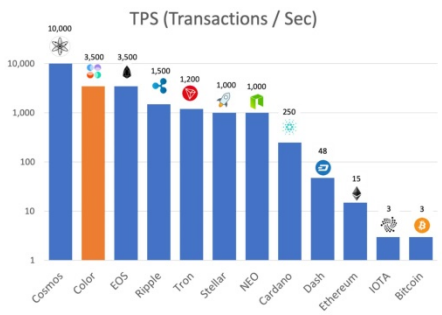
PoS **Proof of Stake** **EOS**

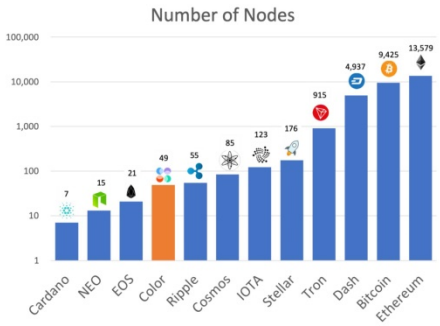
PoC **Proof of contribution** **CLR**

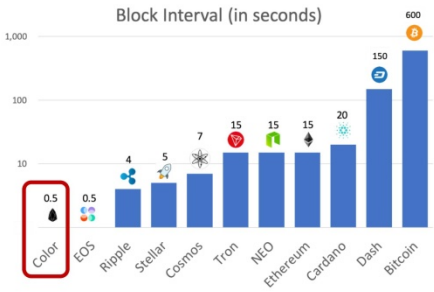
Staked coin

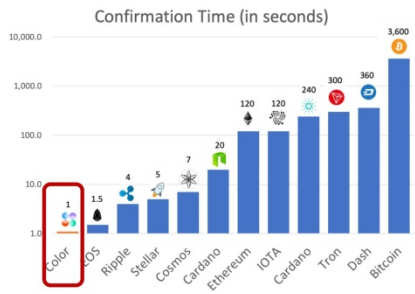
Performance of Hardware

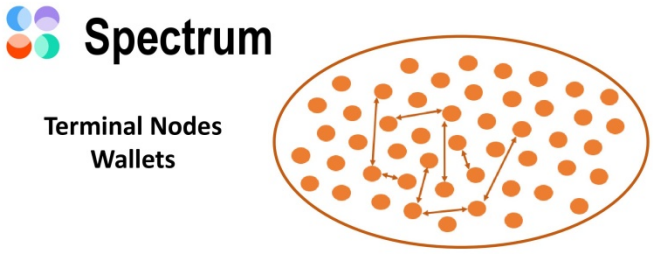
Reputation

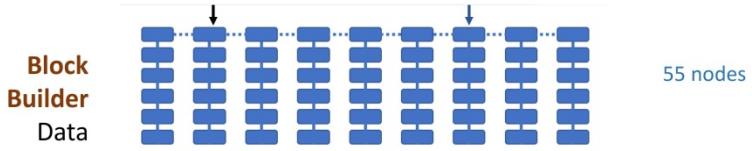


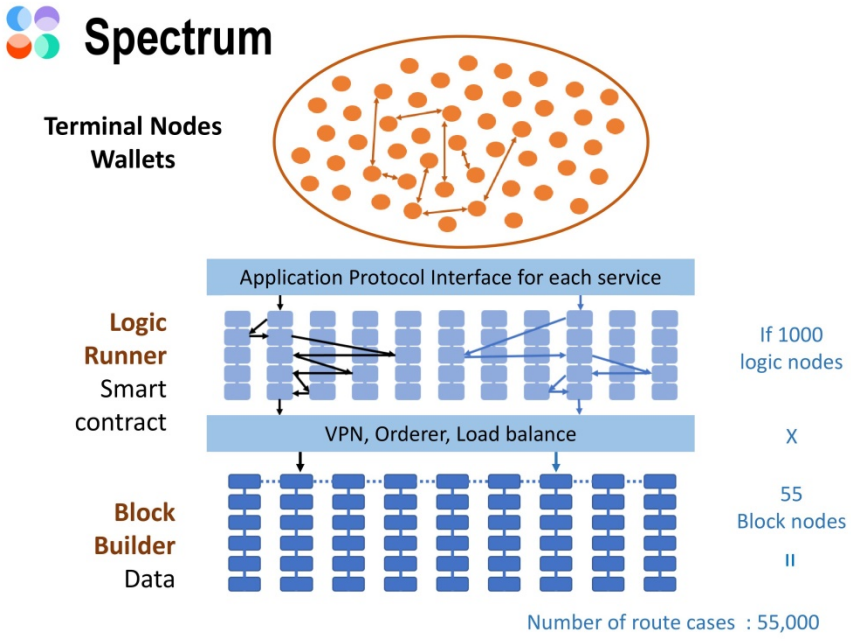


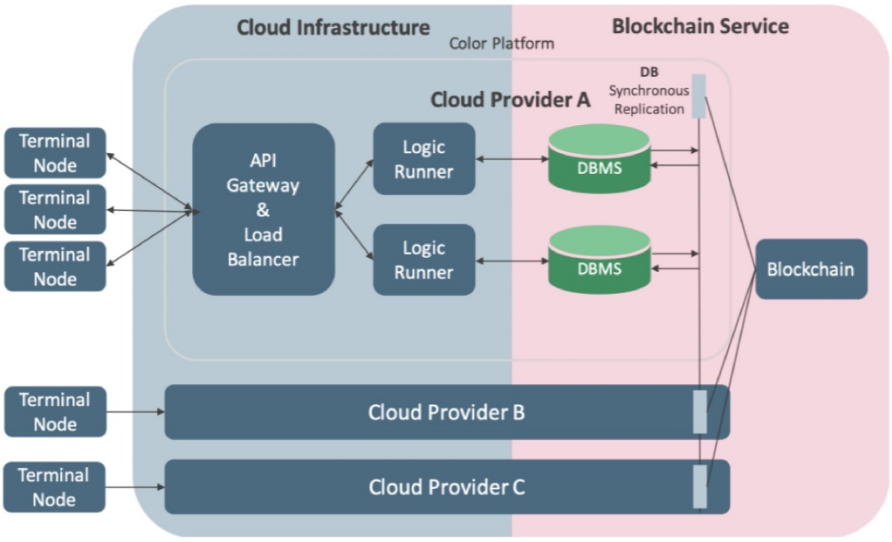





Spectrum
Terminal Nodes
Wallets


Block
Builder
Data
55 nodes

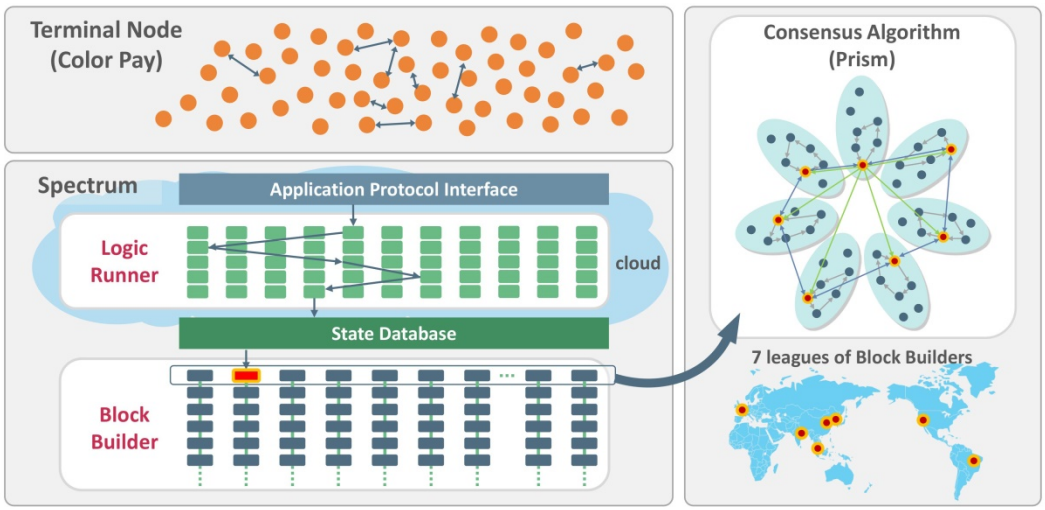

Spectrum
Terminal Nodes
Wallets
Application Protocol Interface for each service
Logic
Runner
Smart
contract
If 1000
logic nodes
VPN, Orderer, Load balance
X
Block
Builder
Data
55
Block nodes
II
Number of route cases : 55,000



[Figure 5 - Cloud in Color Spectrum]

Color Spectrum

Color Spectrum is the engine and core technology for productive and efficient dApp ecosystem.



Slow → Fast confirm

Expensive → Low energy

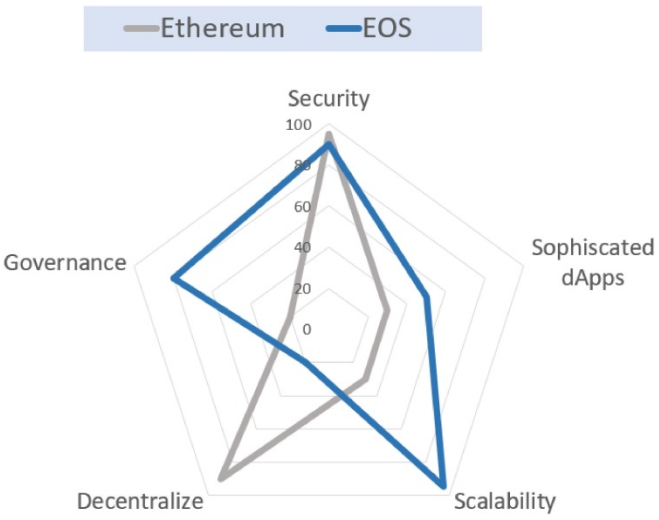
Dangerous → easy to use

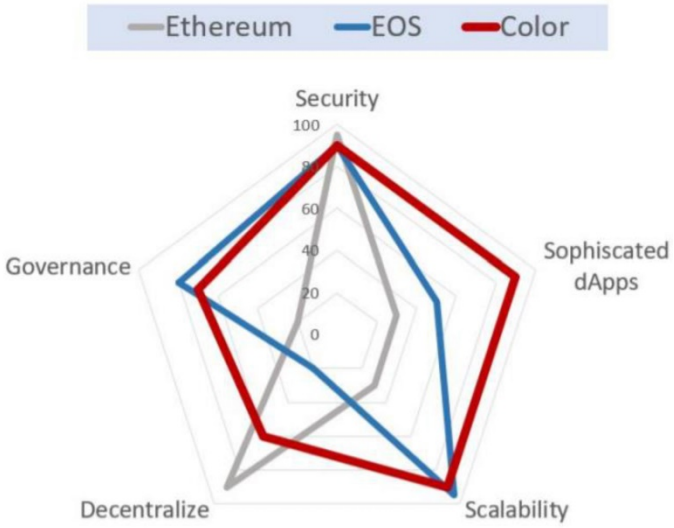
Re-centralized → Ostrom Governance

Wealth polarization → Pixel Program

Decentralized for Daily Life

Solving Blockchain Trilemma





[Figure 1 - Blockchain challenges Diagram]

Fully

Decentralized

Autonomous

Organization

→ Proved Impossible

Requirements for Full Decentralization

1: Nodes with any resource power can earn net profit

2: Delegate resources to others ≤ Run the nodes themselves

3: One player to run multiple nodes ≤ Player runs one node

4: No “the rich richer, the poor poorer”

Mathematically proved that it is impossible.

By Prof. Kim yong dae’team /KAIST

Analysis on Platforms

Platform	Condition 1	Condition 2	Condition 3	Condition 4	# of Nodes
BTC, ETH					10,000
EOS					21
Tron					27
Steem					20
S.O.F					1,000 (22)
Color					49

Condition 1: Nodes with any resource power can earn net profit
Condition 2: Delegate resources to others ≤ Run the nodes themselves
Condition 3: One player to run multiple nodes ≤ Player runs one node
Condition 4: The resource power ratio among nodes should even out over time.

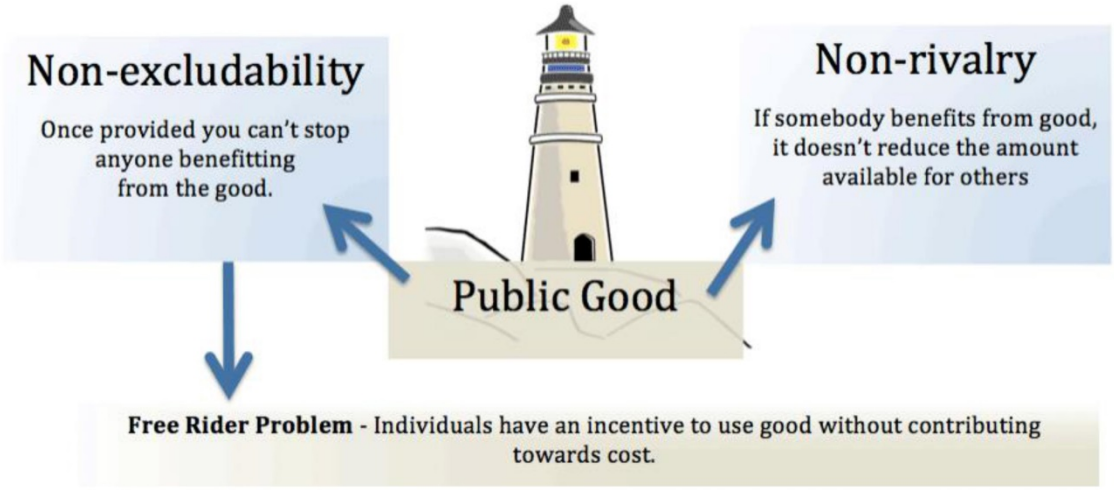
Why DAO is impossible?

Common (Public) Goods

vs

Personal Economic Incentive

Public Goods: Non-excludability & Non-rivalry



Cryptocurrency
is a Common Goods

No-excludability
No-rivaly

Overcome Tragedy of the Commons

Prisoner's Dilemma
(John Nash)

Rational ignorance, Free rider
(Mancur Olsen)

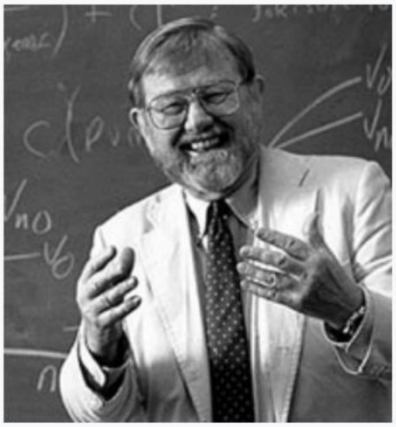
→ State Government or Market economy

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

Institutional Economics

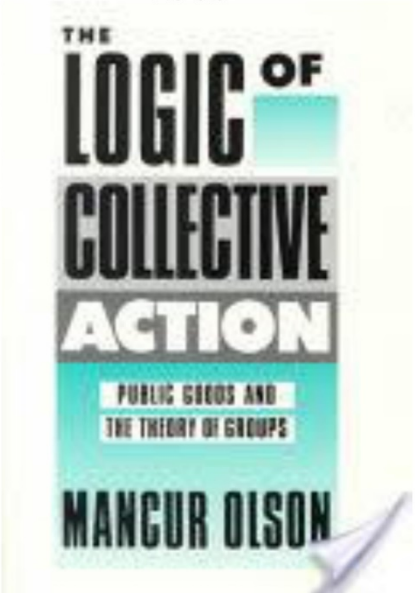
Public goods
Collective action
Economic development

Mancur Olson

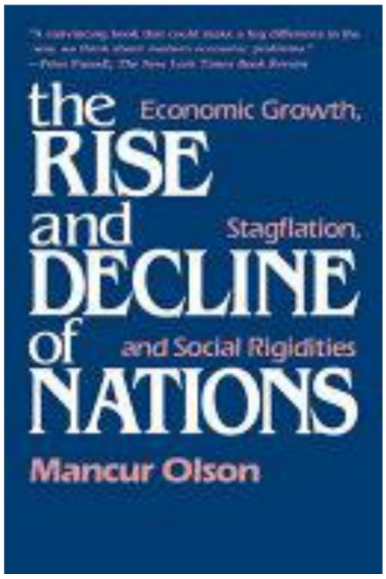


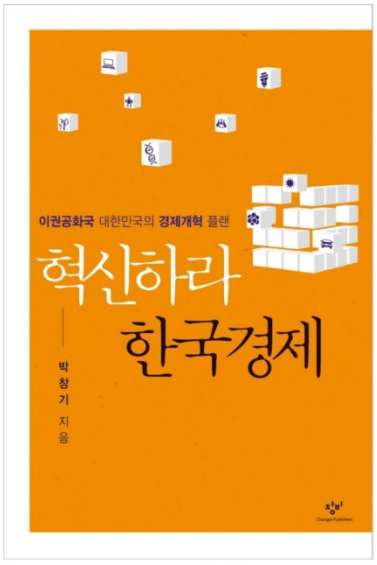
Born	January 22, 1932 Grand Forks, North Dakota
Died	February 19, 1998 (aged 66) College Park, Maryland[1]
Nationality	United States

1965



1982





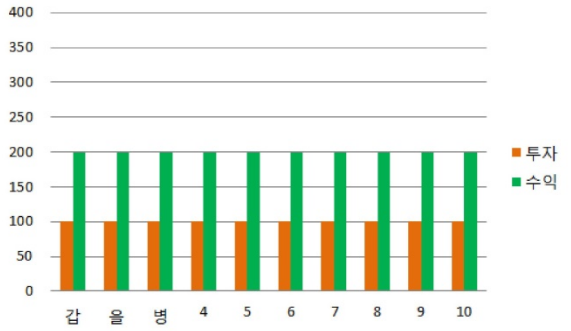
2012년

2013년

가설 1.

Model A

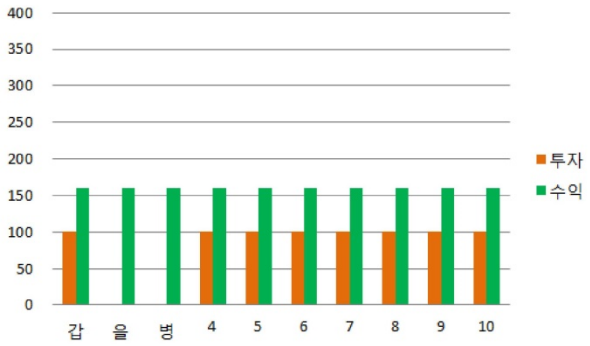
	투자	수익
갑	100	200
을	100	200
병	100	200
4	100	200
5	100	200
6	100	200
7	100	200
8	100	200
9	100	200
10	100	200
합계	1,000	2,000



명제 1

Model B

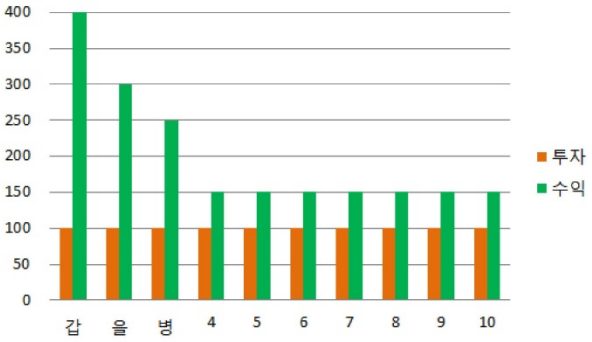
	투자	수익
갑	100	160
을	0	160
병	0	160
4	100	160
5	100	160
6	100	160
7	100	160
8	100	160
9	100	160
10	100	160
합계	800	1,600



명제 2

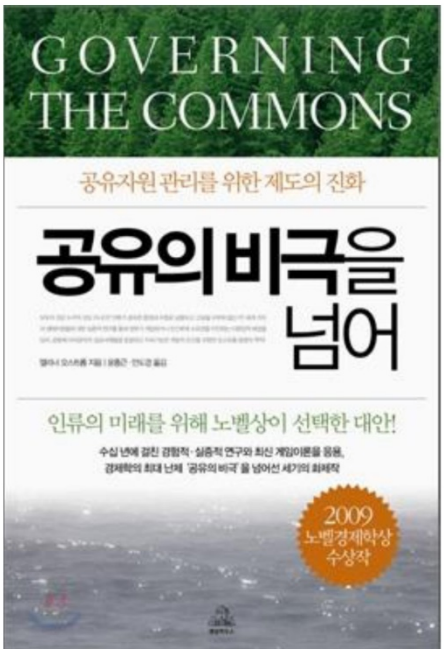
Model C

	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



Elinor Ostrom
1933~2012

2009년
Novel Prize
Economist



Ostrom's Eight Design Principles 1

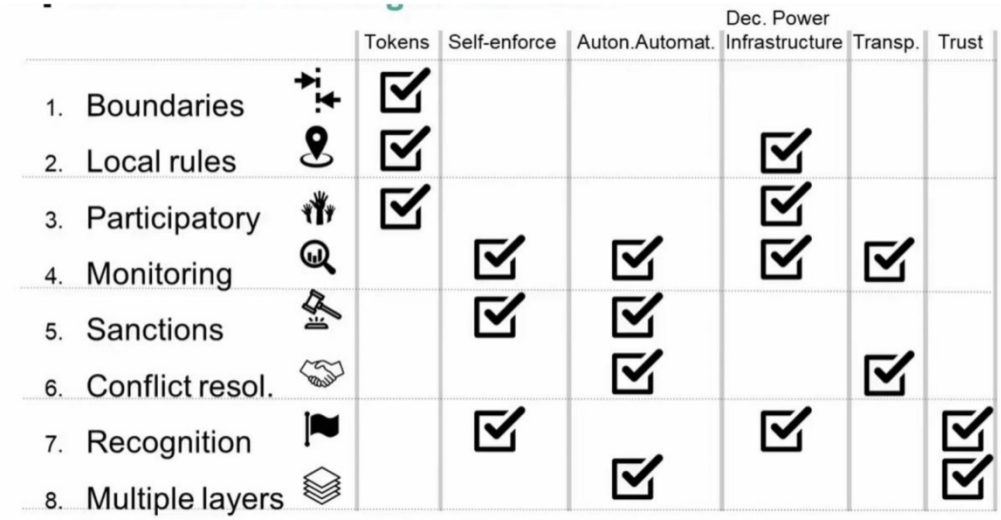
	Ostrom's design principles	Blockchain cryptocurrency design
1	Define clear group boundaries	Token based membership
2	Match rules governing use of common goods to local needs and conditions	Rule determined via blockchain governance
3	Ensure that those effected by rules can participate in modifying rules	Proposal system for members
4	Develop a system, carried out by community members, for monitoring members' behavior	Machine learning and monitoring

https://medium.com/@daviddao/decentralized-sustainability-9a53223d3001
https://wiki.p2pfoundation.net/Ostrom_Contracts

Ostrom's Eight Design Principles 2

	Ostrom's design principles	Blockchain cryptocurrency design
5	Use graduated sanctions for rule violators	Graduate stakes for rule violation
6	Provide accessible, low cost means for dispute resolution	Challenge response game for dispute resolution
7	Make sure rule-making rights for community members are respected by outside authorities	Censorship resistance through decentralization
8	Build responsibility for governing the common resources in nested tiers from lowest level up to the entire interconnected system	Hierarchical nested contracts

Blockchain Facilitating the Commons



	Tokens	Self-enforce	Auton.Automat.	Dec. Power Infrastructure	Transp.	Trust
1. Boundaries	☑					
2. Local rules	☑			☑		
3. Participatory	☑			☑		
4. Monitoring		☑	☑	☑	☑	
5. Sanctions		☑	☑			
6. Conflict resol.			☑		☑	
7. Recognition		☑		☑		☑
8. Multiple layers			☑			☑

9 Council members - Government
5 Arbitration members - Judiciary
1,000 Council members – Congress

49 Block builders
hundreds logic runners

color

Written Constitution
Self – evolving mechanism

Economic incentives Comparison

	Bicoin	Ethereum	EOS	Dash	Color
Mining Servers	O	O	O	O	O
Treasury	X	X	O	O	O
Voters	X	X	X	O	O
New members	X	X	X	X	O Pixel
Tx fee	Miner	Miner	X	Server Treasury Voter	Server Treasury Voter

Color Economic Incentives

	Pixel	Treasury	System Support	Council
New Issue /week*	200,000	100,000	100,000	100,000
Transaction Fee**		30%	40%	30%
Beneficiaries	New Members	Commons budget	Logic runner :70% Block builder :30%	Council Member/ minimum stake

* Decline 5% every 52 week for 50 years
** 0.05% of value with minimum U$ 0.005

Treasury Budget

color

Open Proposal for Spending

Monthly Voting by the Council

Quadratic Differential Voting

color

Quadratic Differential Voting

More money more vote? → Quadratic Voting

$\sqrt{n}$

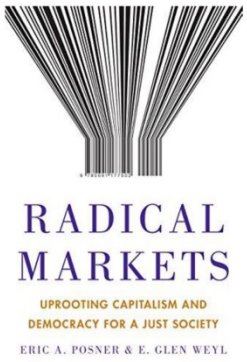
Majority vote? → Differential Voting

Normal #P – #N > 10% then Pass

Important #P – #N > 20% then Pass

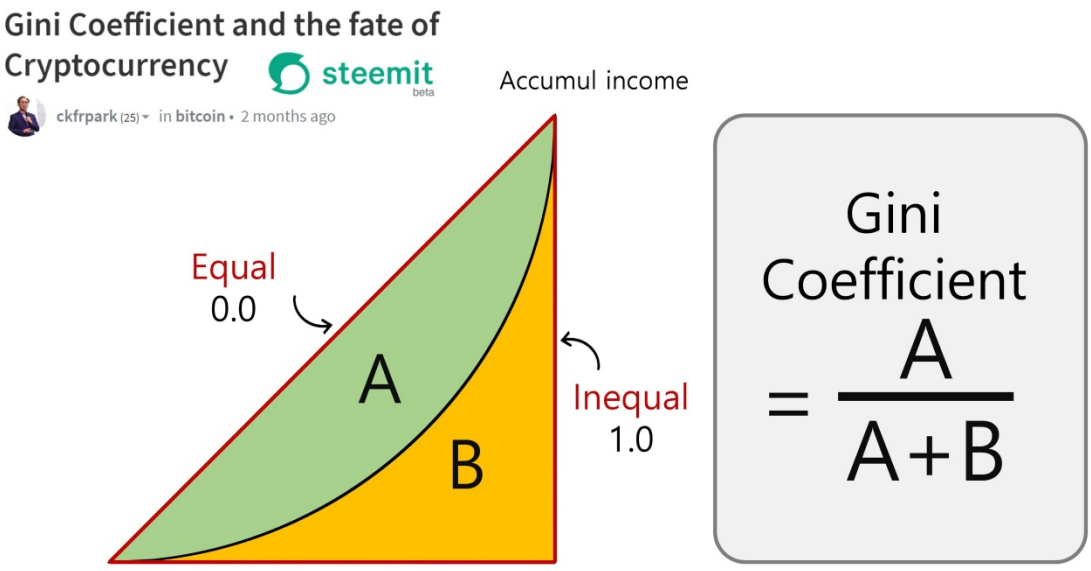
#P Number of positive voting

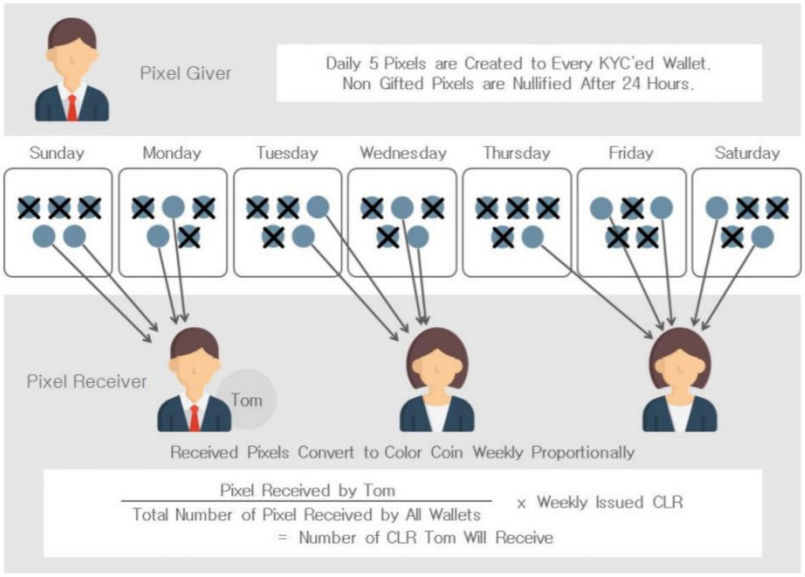
#N Number of negative voting



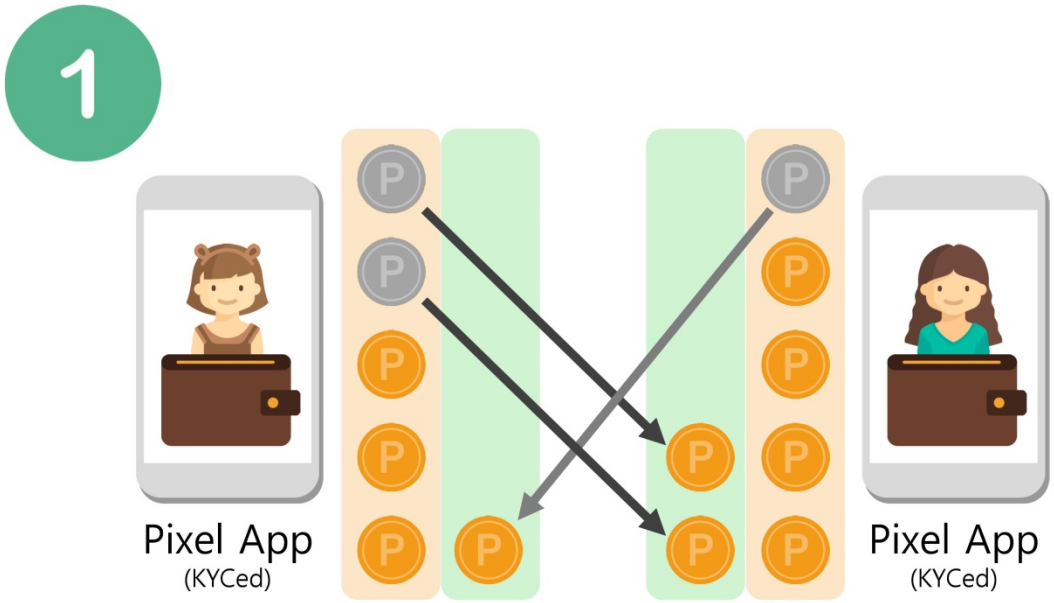
Cryptocurrency Governance
→ Designing the New Civilization
Game Theory → Mechanism Design

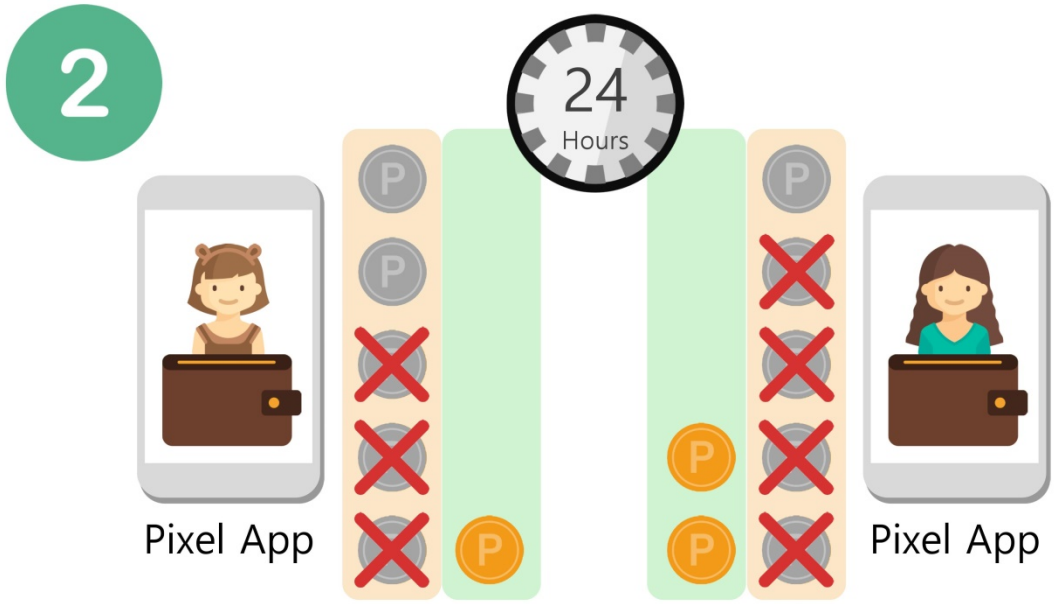
Smart contract →
Low cost Ostrom Governance
Mechanism design easily

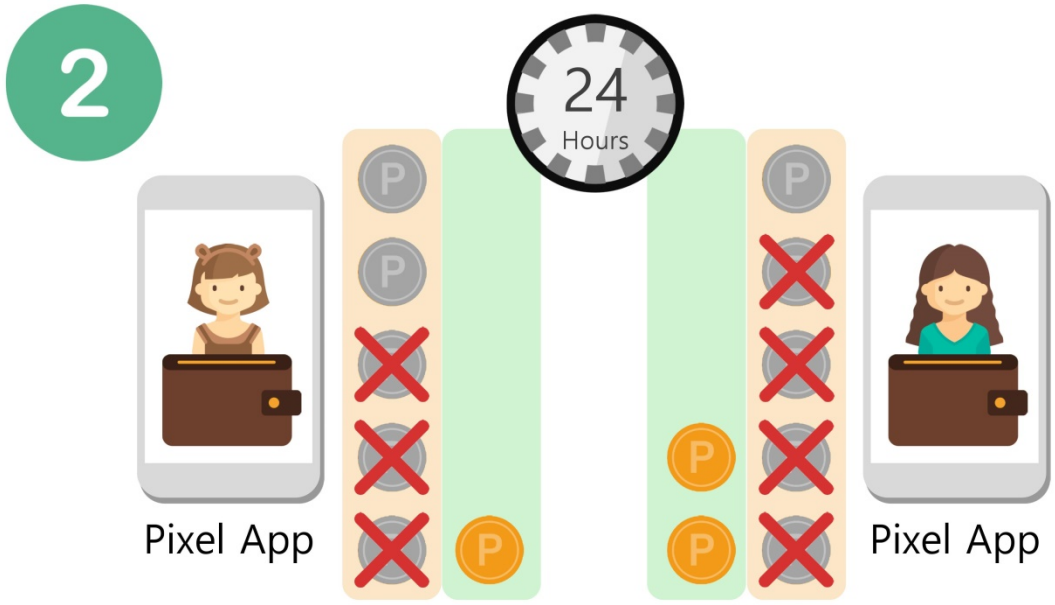


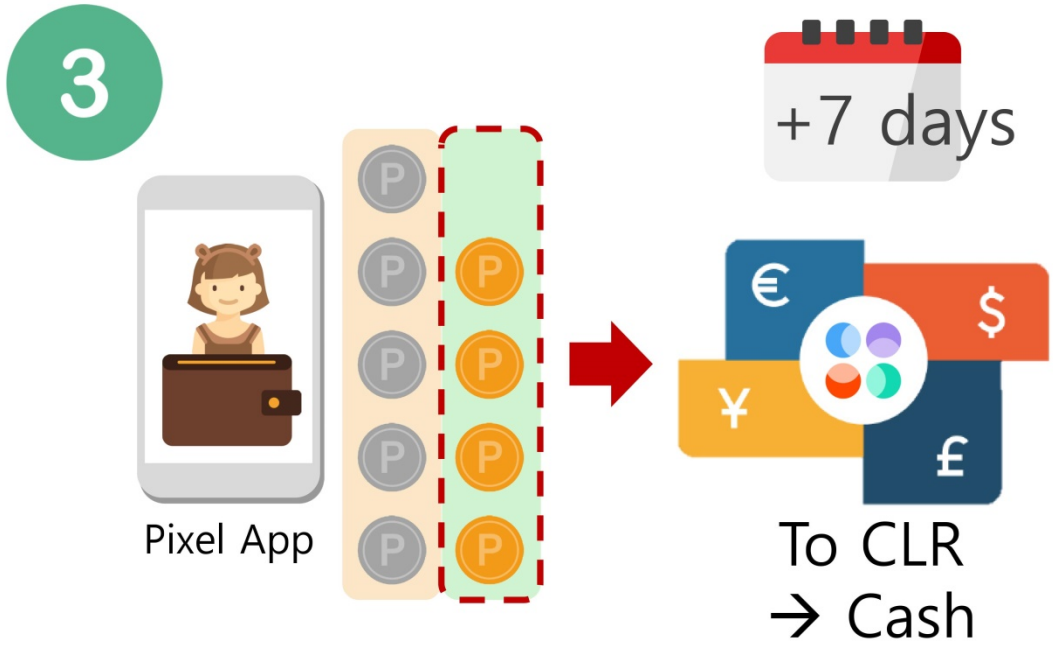


[Figure 7 - Pixel Program Process]




2
24
Hours
Pixel App
Pixel App

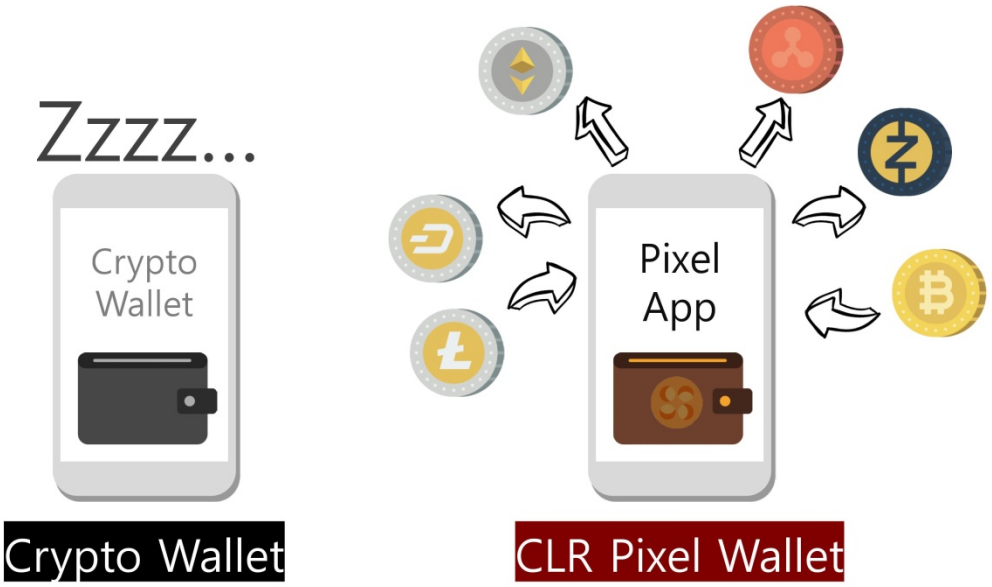

2
24
Hours
Pixel App
Pixel App

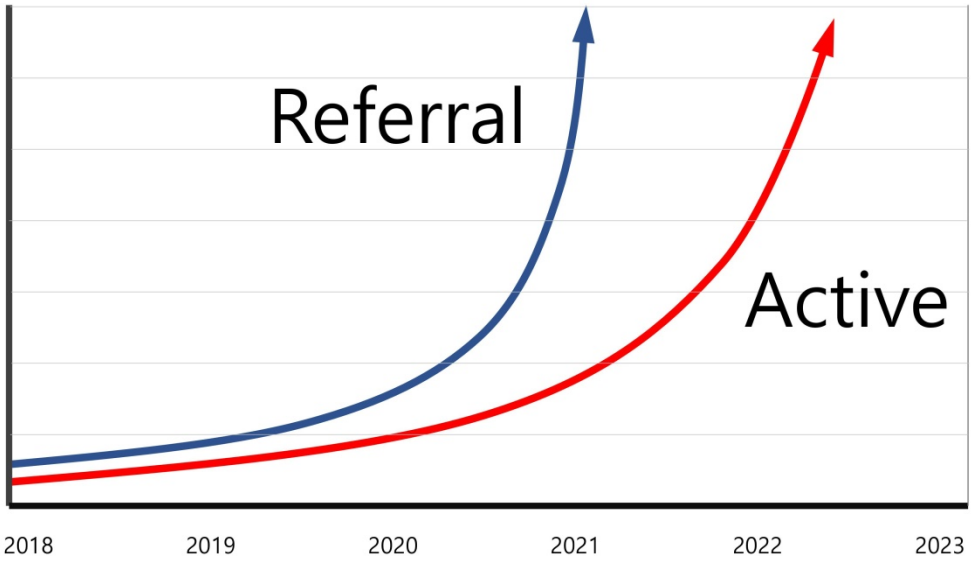

3
+7 days
Pixel App
To CLR
→ Cash

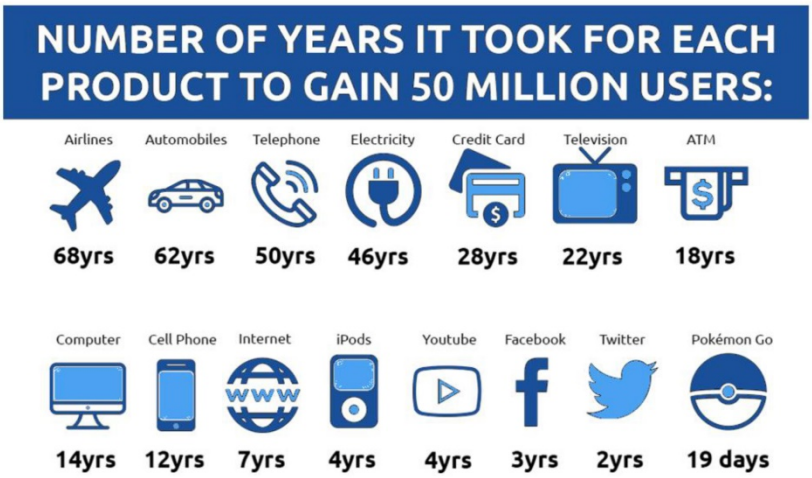
KOREAN AIR
라오스 재난 지역
구호물품 긴급지원
KOREAN AIR

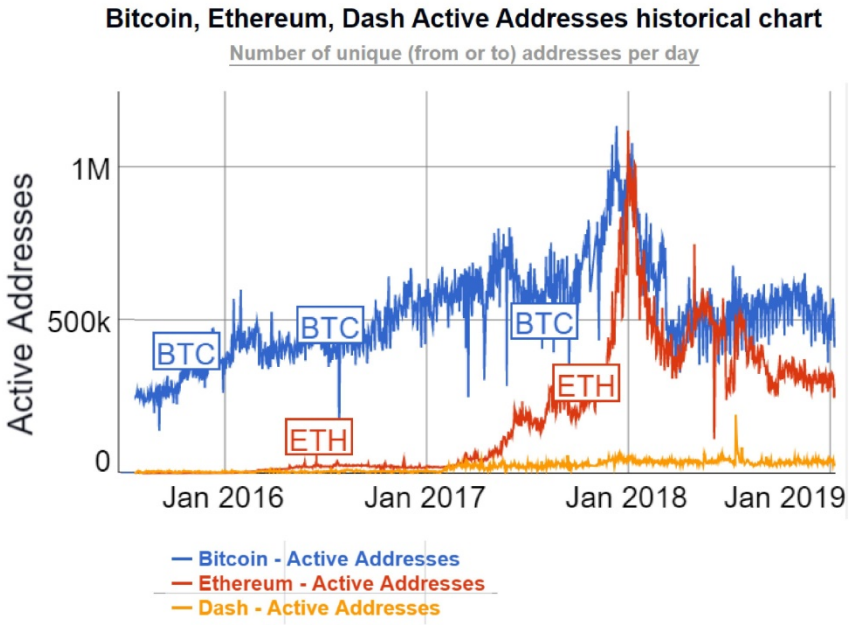
unicef
LOVE MYSELF
#ENDviolence
#BTSLoveMyself
BTS (방탄소년단)
A.R.M.Y

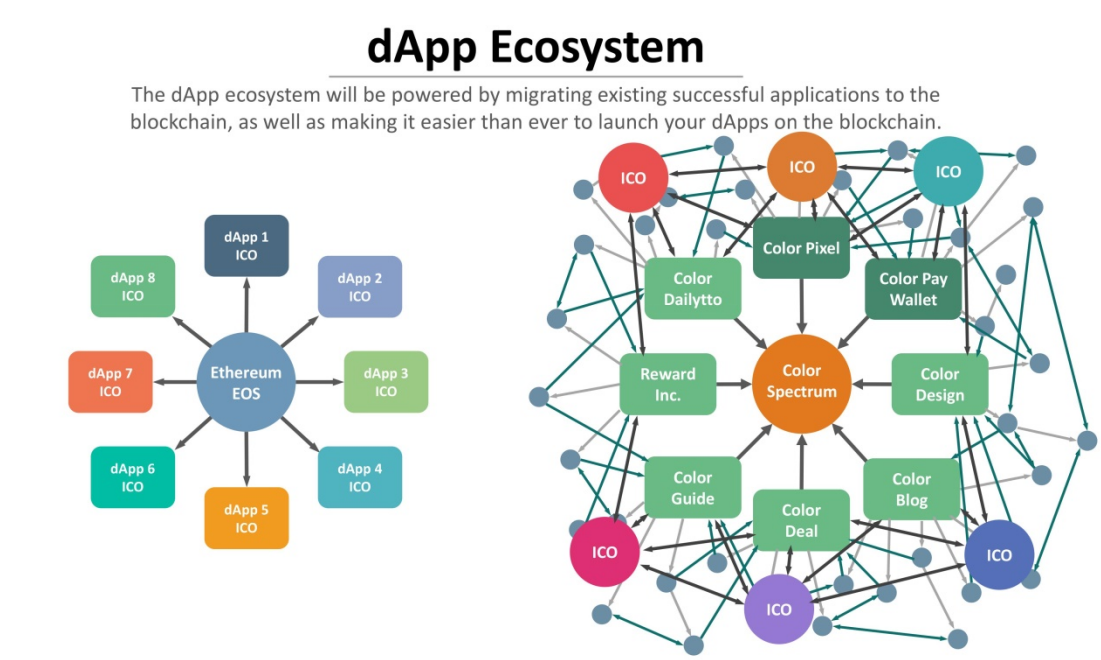
BLACKPINK IN YOUR AREA
BLACKPINK
in your area
2018 TOUR IN SEOUL
우리가 영원히 간직하고 기억할 순간
꽃길만 걸어요
대한태국연합 TEAM LISA
BLACKPINK 2018 TOUR IN YOUR AREA
눈높인 꼭대기 블핑콘 만난 블리잉크
블랙핑크 UNION LATINO, 젠슈리짱 파이팅
LISANATIONS
블랙핑크 리사 100kg
응원드리米
TEAM LISA
블랙핑크 리사 327kg
응원드리米


Zzzz...
Crypto Wallet
Crypto Wallet
Pixel App
CLR Pixel Wallet

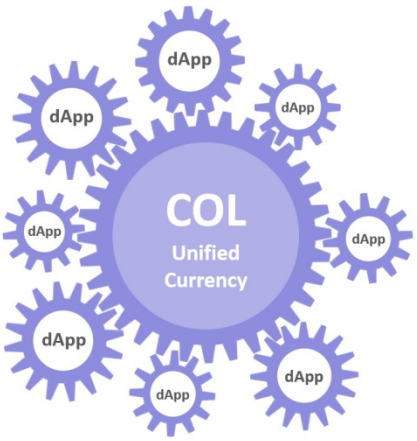

Referral
Active
2018
2019
2020
2021
2022
2023


NUMBER OF YEARS IT TOOK FOR EACH PRODUCT TO GAIN 50 MILLION USERS:
Airlines
68yrs
Automobiles
62yrs
Telephone
50yrs
Electricity
46yrs
Credit Card
28yrs
Television
22yrs
ATM
18yrs
Computer
14yrs
Cell Phone
12yrs
Internet
7yrs
iPods
4yrs
Youtube
4yrs
Facebook
3yrs
Twitter
2yrs
Pokémon Go
19 days

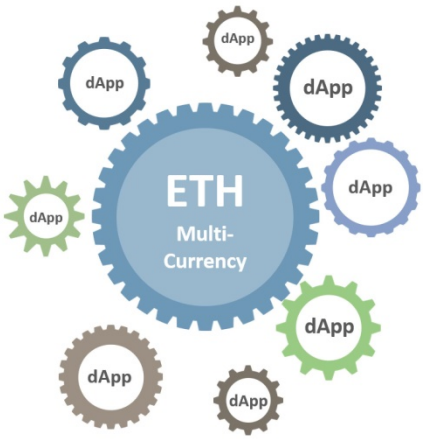

Bitcoin, Ethereum, Dash Active Addresses historical chart
Number of unique (from or to) addresses per day
Active Addresses
1M
500k
0
BTC
BTC
BTC
ETH
ETH
Jan 2016
Jan 2017
Jan 2018
Jan 2019
Bitcoin - Active Addresses
Ethereum - Active Addresses
Dash - Active Addresses


dApp Ecosystem
The dApp ecosystem will be powered by migrating existing successful applications to the blockchain, as well as making it easier than ever to launch your dApps on the blockchain.
dApp 1 ICO
dApp 2 ICO
dApp 3 ICO
dApp 4 ICO
dApp 5 ICO
dApp 6 ICO
dApp 7 ICO
dApp 8 ICO
Ethereum EOS
ICO
ICO
ICO
Color Pixel
Color Dailytto
Color Pay Wallet
Reward Inc.
Color Spectrum
Color Design
Color Guide
Color Deal
Color Blog
ICO
ICO
ICO

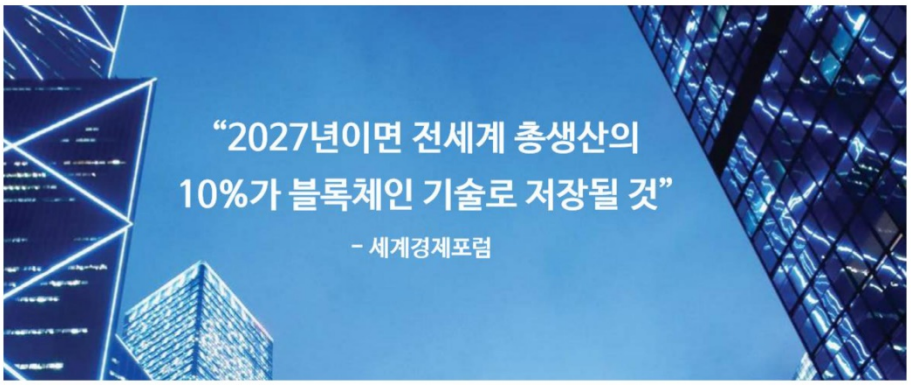
Color Coin



Color Platform



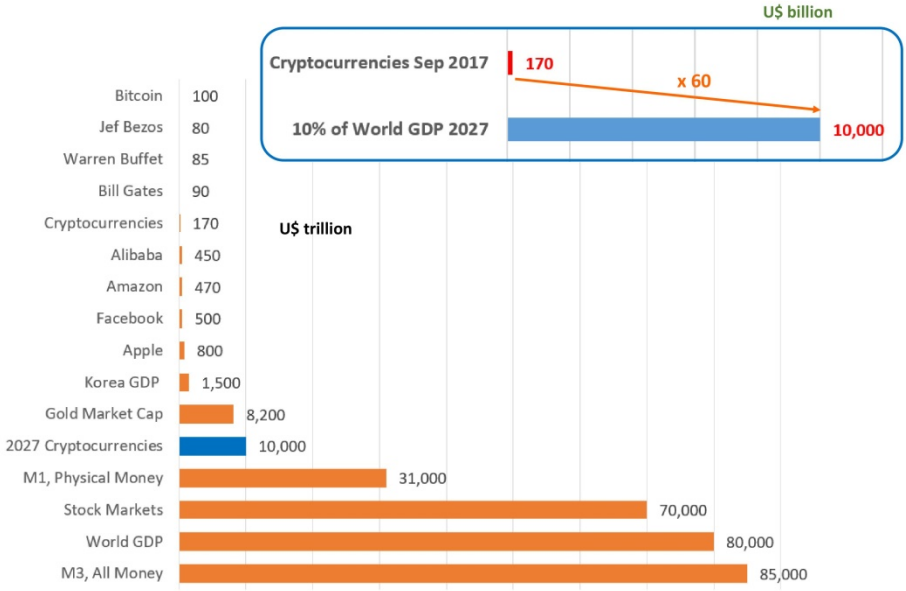
Ethereum

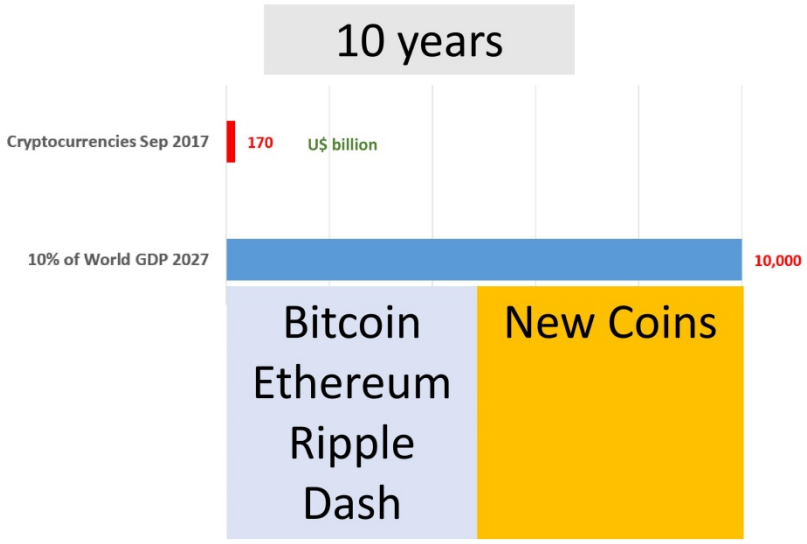


WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Global Agenda Council on the Future of Software & Society

Deep Shift
Technology Tipping Points
and Societal Impact


U$ billion
Cryptocurrencies Sep 2017
170
x 60
10% of World GDP 2027
10,000
U$ trillion
Bitcoin 100
Jef Bezos 80
Warren Buffet 85
Bill Gates 90
Cryptocurrencies 170
Alibaba 450
Amazon 470
Facebook 500
Apple 800
Korea GDP 1,500
Gold Market Cap 8,200
2027 Cryptocurrencies 10,000
M1, Physical Money 31,000
Stock Markets 70,000
World GDP 80,000
M3, All Money 85,000


10 years
Cryptocurrencies Sep 2017
170
U$ billion
10% of World GDP 2027
10,000
Bitcoin
Ethereum
Ripple
Dash
New Coins

Seigniorage

right of the lord (*seigneur*)

to mint money

The greatest business in history

貨幣 鑄造 差益

Seigniorage

Vehicle Currency 基軸通貨

1850~

1930~

2000~

1993~

1985~

2017~

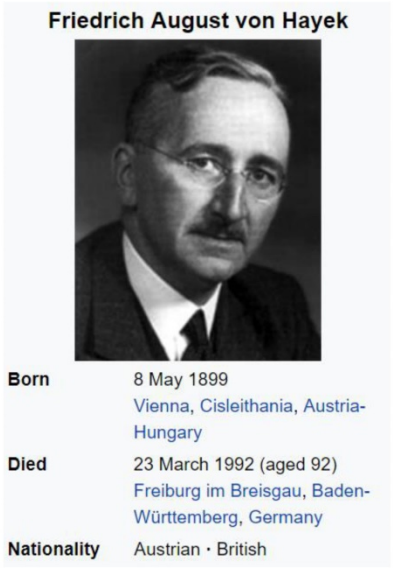
Bank of China

HSBC

Standard Chartered Bank

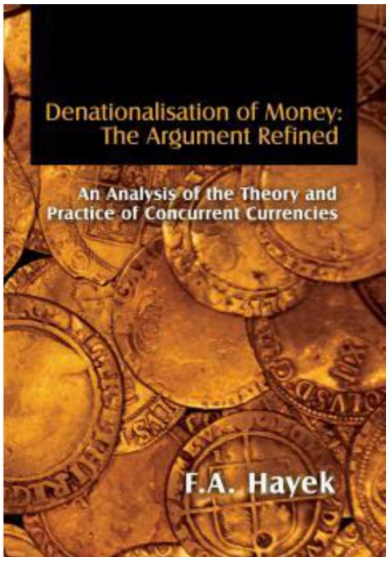
Friedrich Hayek
Libertarian

1974
Nobel Prize,
Economics



The Denationalization of Money

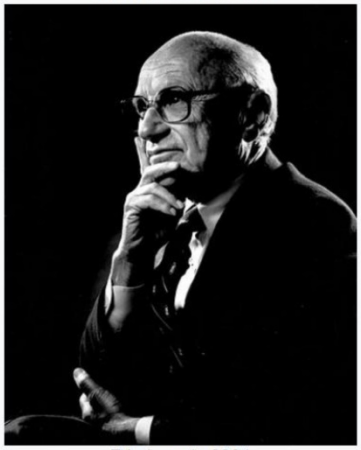
1976



Quantity Theory of Money

貨幣數量說

Milton Friedman



Friedman in 2004

Born	July 31, 1912 Brooklyn, New York, U.S.
Died	November 16, 2006 (aged 94) San Francisco, California, U.S.
Nationality	American

Milton Friedman

1976 Novel Prize

Economics

Chicago School

Monetarist

Libertarian

Quantity theory of money

Fisher's equation of exchange

$$M \cdot V_T = \sum_i (p_i \cdot q_i) = \mathbf{p}^{\mathrm{T}} \mathbf{q}$$

M is the total amount of money in circulation on average in an economy during the period, say a year.
V_T is the transactions velocity of money, that is the average frequency across all transactions with which a unit of money is spent. This reflects availability of financial institutions, economic variables, and choices made as to how fast people turn over their money.
p_i and q_i are the price and quantity of the i-th transaction.
$\mathbf{p}$ is a column vector of the p_i, and the superscript $^{\mathrm{T}}$ is the transpose operator.
$\mathbf{q}$ is a column vector of the q_i.

Mainstream economics accepts a simplification, the equation of exchange:

$$M \cdot V_T = P_T \cdot T$$

where

P_T is the price level associated with transactions for the economy during the period
T is an index of the real value of aggregate transactions.

$$MV = PT$$

Value of Money; $\frac{1}{P} = \frac{T}{MV}$

$$\frac{1}{P} = \frac{T}{MV}$$

To increase Coin price

T up → user expansion via Apps

M down → Limit minting

V reduce → Freezing reward, PoS

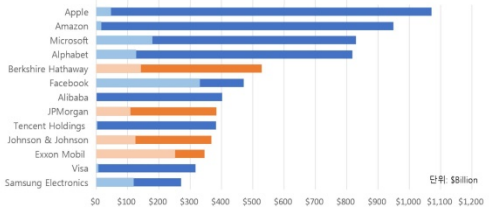
Market Capitalization Change

2005

Capitalism

1-sided market

2018



Digital Platform

2-sided market

2020

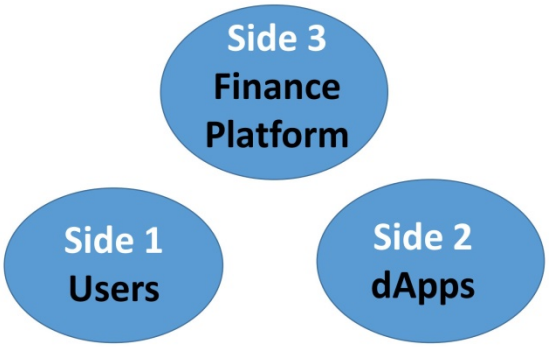
?

Crypto Platform

3-sided market

3-sided Market

2-sided Market → 3-sided Market



WeChat Pay

Alipay™

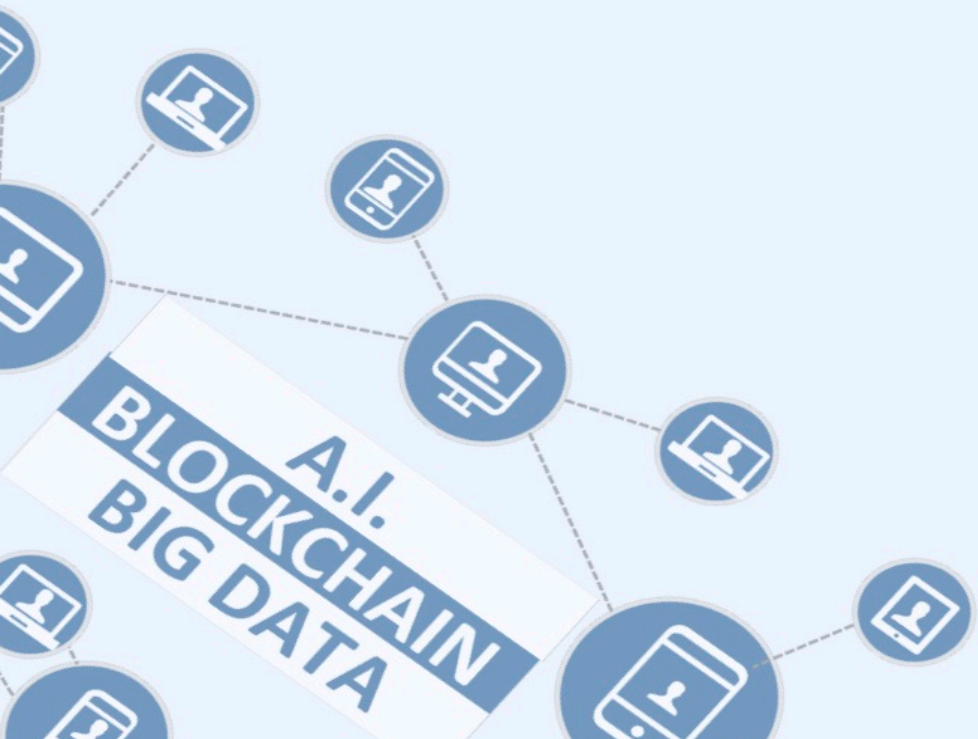
Decentralized for Daily Life

4강

Consensus Algorithm and Tokeneconomy

이 영 환 대표

(주식회사 딜라이트)



강의 동영상 URL

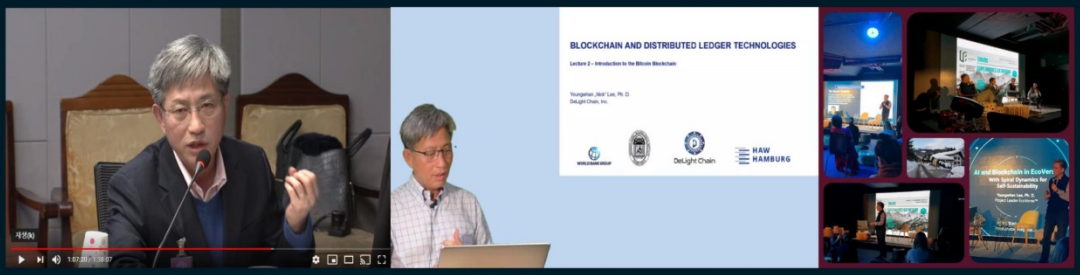
1 부: https://youtu.be/DNyK7vtiRMM

2 부: https://youtu.be/JCbaopwt8I4

Consensus Algorithm and Tokeneconomy

Youngwhan Lee, Ph. D.
Project Leader EcoVerse™

Email:nicklee@delightchain.io
https://ecoverseglobal.io



About me

- Project Leader, EcoVerse
- CEO, DeLight Chain, Inc.
- Former University Professor
- Invited Speaker at Blockbase in Davos, Switzerland
- Invited Lecturer at Hamburg HAW University
- Founder and Chairman, W3C Blockchain Community Group

1 PoW 설명

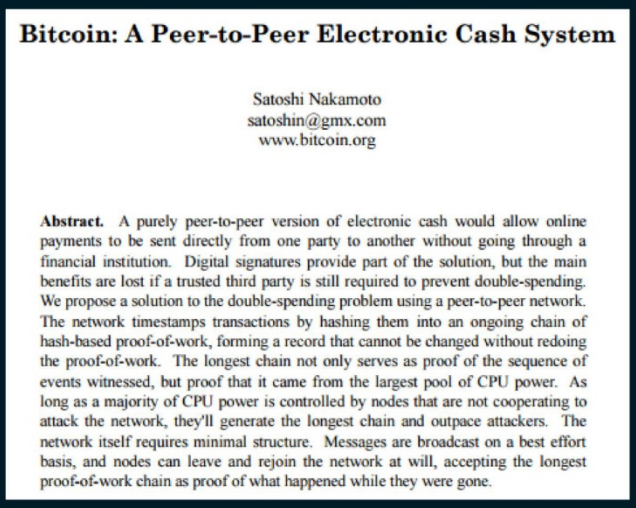
Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

Do you trust these people?

The Beginning

2008년 세계 금융위기 이후
금융시스템에 대한 신뢰가
떨어지면서 사토시 나카모토라는
가명을 쓰는 발명자가 비트코인
이라는 암호화폐를 고안함.

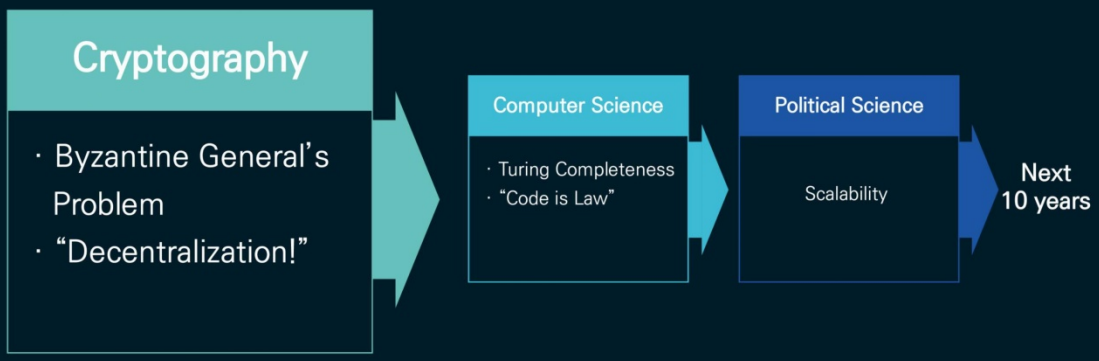


Bitcoin: A Peer-to-Peer Electronic Cash System

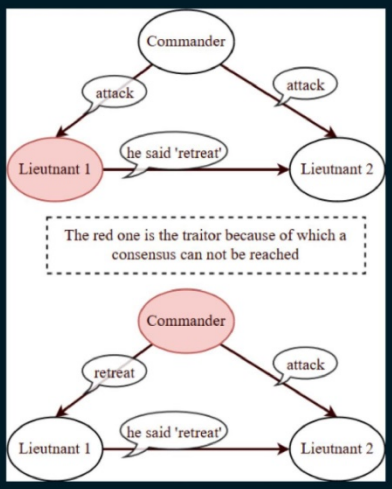
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

암호화폐, 지난 10년 역사



Byzantine generals problem (비잔틴 장군 문제)



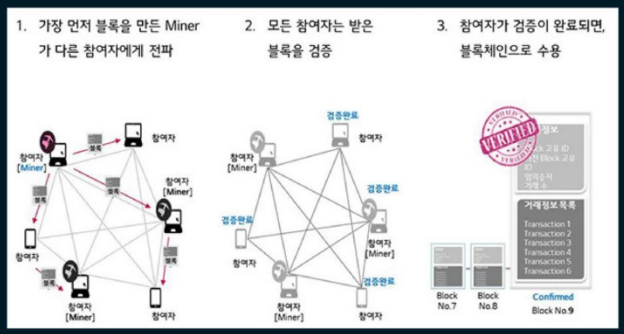
비잔틴 장군 문제 :
· 수학적으로 해결 불가능

사토시 나카모토의 해결책 :
· Nonce찾기 + 인센티브

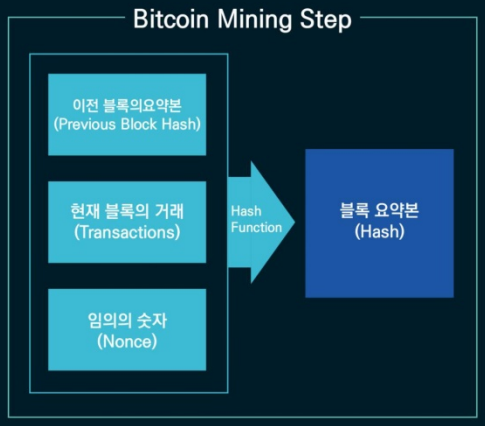
작업증명(Proof-of-Work) 메커니즘

· 일정한 시간이 걸리는 작업을 수행하여 문제를 풀고 난 후, 이를 증명하는 것이 작업증명(PoW: Proof of Work)

· 문제풀이 한 노드가 그 이전에 발생한 거래기록을 블록으로 묶어 시간 순서에 따라 연결하고 이를 공유하면 네트워크 참가 노드(마이너) 과반수 이상이 검증하고 합의하면 공식적으로 장부에 기록함



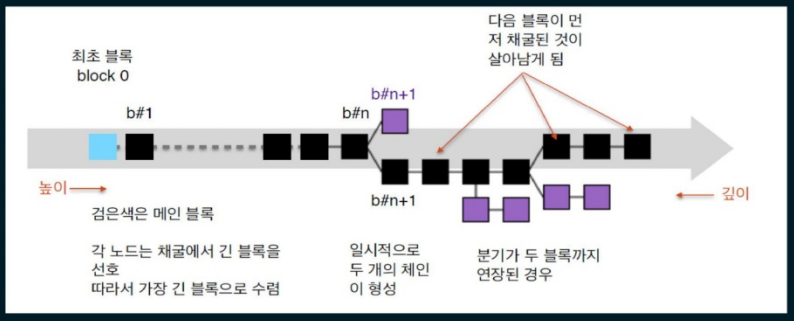
한 사람만 블록을 만들도록 함: 임의의 숫자(Nonce) 찾기



- 블록의 요약본은 이전 블록의 요약본에 현재 블록의 모든 거래를 덧붙이고 여기에 임의의 숫자 X를 덧붙인 문서를 hashing하여 만든다.
- 조건을 만족하는 X를 찾는 것은 모든 경우의 수를 대입해 보는 방법(brute force)밖에 없다.
- 이렇게 조건을 만족하는 임의의 수를 찾아 만든 현재 블록의 요약본을 이웃 채굴자에게 알리고 이를 다른 채굴자들이 맞는 것으로 받아들이게 되면 이를 블록의 해를 구했다고 하거나 블록을 찾았다고 한다

최장 체인 룰 (Lonest Chain Rule)

블록체인의 원본은 모든 노드들이 가지고 있는 데 여러 가지 이유로 일시적으로 서로 다른 원본을 가지고 있을 수 있다(이를 분기되었다(forked)고 한다). 이 때 가장 긴 가지를 메인으로 간주.



PoW의 문제점

· 이중지불 등의 다양한 공격에 취약
· 마이닝에 대대적인 장비 투자 필요
· 불필요한 전기 소비 필요
· 초당 평균 3개 (최대 7개) 거래 허용

마이닝풀

Mining pools allow individual miners to combine, or 'pool', their computational power together

- Reduces variance in mining rewards
- Run by **pool managers** or **pool operators**
- Pool manager usually takes a cut of the mining rewards

Pros

- Allows individual miners to participate
  - Democratizing
- Easy to upgrade the network
  - Pool manager upgrades on behalf of pool participants

Cons

- Pool manager must be trusted
- Centralized
- Enables a whole series of attacks

Mining Pools Computation

Suppose you want to start mining today.

- Antminer S9: Costs $2400, **14 TH/s**

When do you get your money?

- Today's network hashrate: **3,352,427 TH/s**
- **% of network hashrate** = (14 TH/s) / (3352427 TH/s) = **0.000417607%**
- Mining Reward / yr = (1 yr / 10 mins) * 12.5 = **657k BTC / yr**

Expected Annual Reward

- 0.000417% * 657k /yr
  = 2.743 BTC / yr = **$3368.404/yr**

Solo mining

- 1 block mined per 239460 blocks
  = 12.5 BTC every 1663 days
  = **$8059 once every 4 years 6 months**

Mining with mining pool (assuming pool has 1/6th of network hashrate):

- 1/6th hashrate
  => Pool finds every 6th block = 6 per hour
- $3368 / (8760 hrs/yr)
  = **$0.38 once every hour**

Paradox: The more secure Bitcoin gets, the more we need mining pools

BLOCKCHAIN AT BERKELEY

Mining Pool Hashrate Distribution

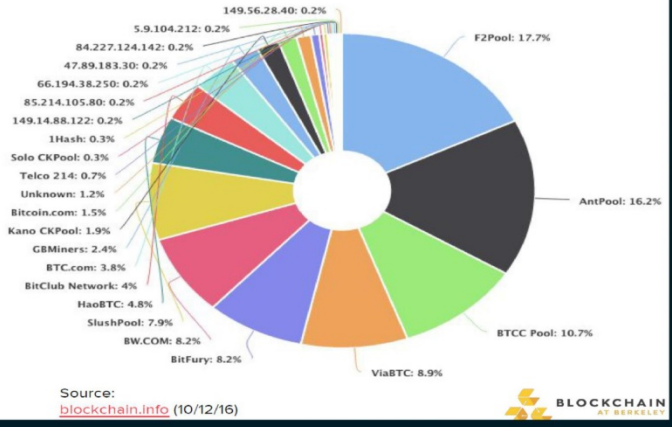
MINING POOL HASHRATE DISTRIBUTION

Community exhibits backlash against large mining pools

- Ex: GHash.io in 2014

Single entity might be be participating in multiple pools

- Called "**Laundering hashes**"
- Actual concentration of control over mining hardware **is unknown**



Source:
blockchain.info (10/12/16)

BLOCKCHAIN AT BERKELEY

Pool Wars

You have 30% of the hashrate. Assume 1 BTC block reward. All of the following numbers are expected value.

- 30% HR (hashrate)
  = 30% MR (Mining Reward) = 0.3 BTC

You buy more mining equipment, worth 1% of current network hashrate

Standard mining strategy

- Add 1% HR => 31/101 = 30.69% HR = .3069 BTC
  - Revenue gain = **0.0069 BTC for 1% hashrate added**

Cannibalizing Pools - Distribute your 1% equally among all other pools, withhold valid blocks.

- Rewards will still be received
- Undetectable unless statistically significant

Other pool hashrate breakdown:

- (70/71 honest, 1/71 dishonest)
  = 70% honest hashrate = .7 BTC
- You own (1/71) of other pools, so expected value of mining there is
  (1/71) * .7 = **0.0098 BTC**
- **0.0098 (cheat) > 0.0069 (honest)**

More profitable to cannibalize pools than mine honestly

2 PoW 공격

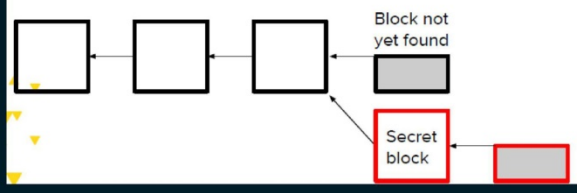
- 이기적 마이닝
- 이중지불
- 검열
- 시간차 공격
- DoS (Denial of Service) 공격
- 트랜잭션 늘리기 해킹
- 51% 공격
- Sybill 공격

이기적 마이닝

You are a miner; suppose you have just found a block.

- Instead of announcing block to the network and receiving reward, keep it secret
- Try to find two blocks in a row before the network finds the next one

This is called **selfish mining** or **block-withholding**

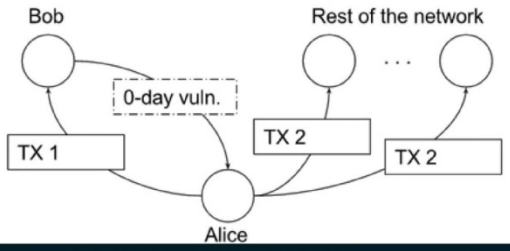


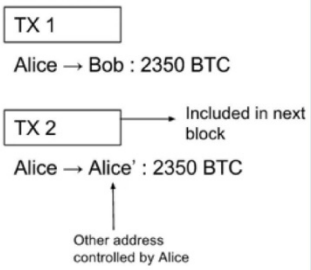
Note: "block-withholding" is also sometimes used in the context of mining pools - submitting shares but withholding valid blocks

이중 지불: 0-Confirmations Bob

Suppose Bob doesn't wait for **any** confirmations on Alice's transaction. He simply checks that the transaction is valid and **immediately** sends Alice the exploit.

Bob is vulnerable to a **Race Attack**!

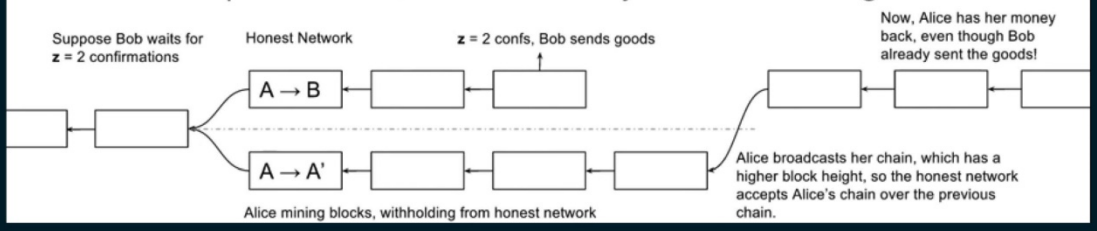




이중 지불: z–Confirmations Bob

Clearly not secure if Bob doesn't wait for any confirmations... What if Bob waits for **z** confirmations?

[A → B] transaction needs **z** confirmations before Bob sends the goods. In order to double spend Bob, Alice needs to mine on her private chain, mine **z** blocks on top of her block, then broadcast *after* Bob sends the goods.



이중 지불로부터 안전하려면???

Double Spend - Security cont.

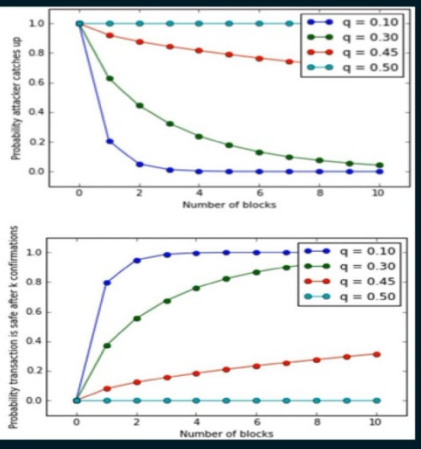
To avoid infinite tail, discrete summation, we look at the inverse probability that Alice **can't** catch up to the chain **j** blocks ahead

$$= 1 - \Sigma^{\infty}_{k=0} (\lambda^k e^{-\lambda})/(k!) \begin{cases} 0 & \text{if } k > z \\ 1 - (q/p)^{z-k} & \text{if } k \le z \end{cases}$$

$$= 1 - \Sigma^{z}_{k=0} (\lambda^k e^{-\lambda})/(k!) \cdot (1 - (q/p)^{z-k})$$

So... how many confirmations should Bob wait for, before sending Alice the goods?

Depends on how much hash power we assume Alice to control.



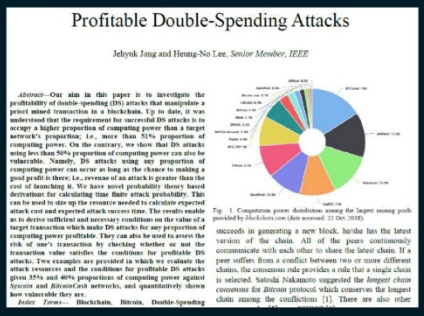
Less than 51% Attacks Profitable

What if the attacker set a "cut time"?

Theorem-1. For all attacker's fractions of computing power p_A (1%~99%), DS attacks are profitable if the value V of target transaction is greater than

$$V_{Suf.}(p_A; N_{BC}) = \gamma'(p_A)\frac{\lambda_H p_A \mathrm{E}[T_{AS}]}{(1-p_A)\mathbb{P}_{AS}(p_A, t_{cut}; N_{BC})}.$$

Theorem-2. A DS attack using p_A less than 50% are profitable only if a finite cut time $t_{cut} < \infty$ is given.



Profitable Double-Spending Attacks

Jehyuk Jang and Heung-No Lee, *Senior Member, IEEE*

Abstract—Our aim in this paper is to investigate the profitability of double-spending (DS) attacks that manipulate a priori mined transaction in a blockchain. Up to date, it was understood that the requirement for successful DS attacks is to occupy a higher proportion of computing power than a target network's proportion; i.e., more than 51% proportion of computing power. On the contrary, we show that DS attacks using less than 50% proportion of computing power can also be vulnerable. Namely, DS attacks using any proportion of computing power can occur as long as the chance to making a good profit is there; i.e., revenue of an attack is greater than the cost of launching it. We have novel probability theory based derivations for calculating time finite attack probability. This can be used to size up the resource needed to calculate expected attack cost and expected attack success time. The results enable us to derive sufficient and necessary conditions on the value of a target transaction which make DS attacks for any proportion of computing power profitable. They can also be used to assess the risk of one's transaction by checking whether or not the transaction value satisfies the conditions for profitable DS attacks. Two examples are provided in which we evaluate the attack resources and the conditions for profitable DS attacks given 35% and 40% proportions of computing power against *Syscoin* and *BitcoinCash* networks, and quantitatively shown how vulnerable they are.

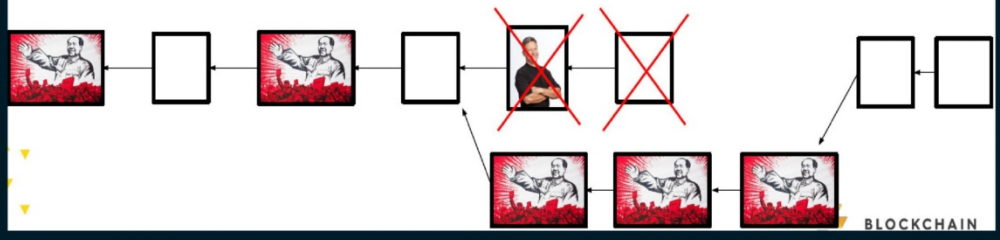
Index Terms— Blockchain, Bitcoin, Double-Spending

Fig. 1. Computation power distribution among the largest mining pools provided by *blockchain.com* (date accessed: 22 Oct. 2018).

succeeds in generating a new block, he/she has the latest version of the chain. All of the peers continuously communicate with each other to share the latest chain. If a peer suffers from a conflict between two or more different chains, the consensus rule provides a rule that a single chain is selected. Satoshi Nakamoto suggested the *longest chain* consensus for *Bitcoin* protocol which conserves the longest chain among the conflictions [1]. There are also other

Blacklisting by Punitive Forking

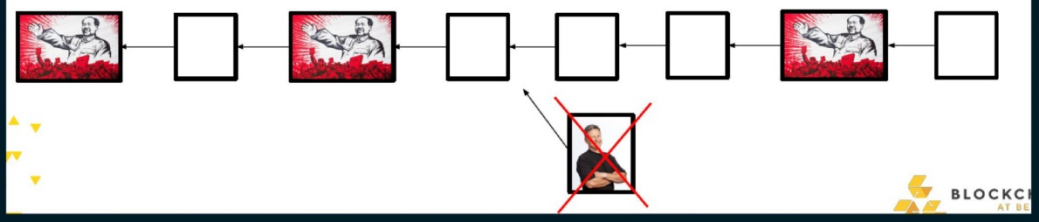
- If non-Chinese miners include a transaction from Johnson in a block, China will fork and create a longer proof of work chain
- Block containing Johnson's transaction now invalidated, can never be published



Blacklisting by Punitive Forking

- Non-Chinese miners eventually stop trying to include Johnson's transactions when mining blocks, since they know that their block will be invalidated by Chinese miners when they do

We have now shown how a 51% majority can prevent anyone from accessing their funds. This is called **punitive forking.**



Youngwhan Lee, Ph. D.

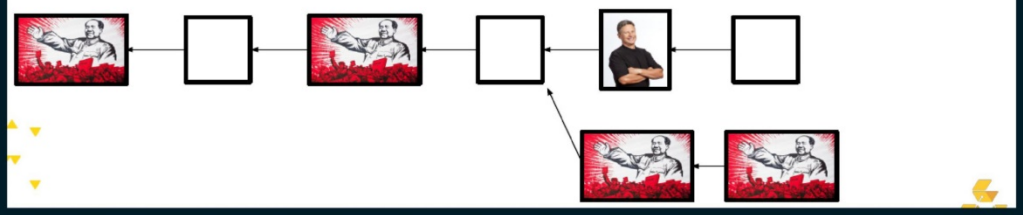
EcoVerse™ DeLight Chain

Blacklisting by Feather Forking

Let **q** equal the proportion of mining power you have, $0 < q < 1$
Let **k** = 1: You will give up after 1 confirmation (one additional block)

- Chance of successfully orphaning (invalidating) the Johnson block = q^2

If **q** = **.2**, then q^2 = **4%** chance of orphaning block. Not very good



Youngwhan Lee, Ph. D.

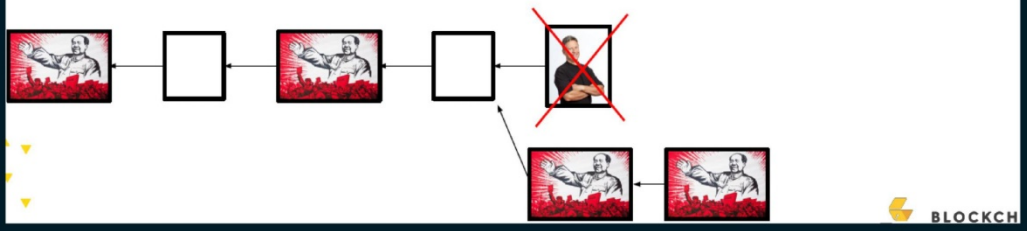
EcoVerse™ DeLight Chain

Blacklisting by Punitive Forking

But other miners are now aware that their block has a q^2 chance of being orphaned. They must now decide whether they should include Johnson's tx in their block

EV(include) = (1 - q^2) * BlockReward + Johnson's tx fee

EV(don't include) = BlockReward



TRANSACTION MALLEABILITY

Transaction Malleability:

Nodes relaying a fresh transaction can tweak certain fields to make a version of the transaction with a different hash image, yet the *digital signature still verifies!*

For example: in ECDSA, the following signature pairs are equivalent:
(r, s (mod N)) and (r, −s (mod N))
Both validate the same transaction data, but now the hash image changes.
Additionally, the **scriptSig** field can (sometimes) have extraneous script ops tacked on the end.

Timejacking

Background: Bitcoin nodes are exchanging monetary transactions over vast distances and time zones; every node needs to be in synch with the other nodes on the network.

Nodes maintain an internal clock time that is computed as the median clock time of its peers.

If the median time differs by more than 70 minutes from the system time, the node reverts its internal clock time to the system time.

As a precaution, nodes reject new blocks with timestamps that are more than 2 hours ahead of its internal clock.

Attack: Attacker launches a **sybil attack** against the target node and *every other node*.

For the **target node**, the attacker aims to set the internal clock 70 minutes *behind* the wall clock.

For **every other node**, the attacker wants to set the internal clocks 70 minutes *ahead* of the wall clock.

DOS Attack – Malicious miners

Malicious miners can **timejack competing miners**, effectively taking the competing miners out of the network and increasing the malicous miner's effective hash power!

In fact, this works for any **denial of service attack** (DoS Attack).

Miners with access to a distributed Botnet have a competitive advantage.

51% attack (1/2)

· Computational power requires electricity, which requires money Equilibrium reached, if miners are breaking even or profitable
Mining Reward = Mining Cost

· If you are roughly breaking even with the capital you invest, there is little to no marginal cost to getting more hashrate. You need more capital to attain 51%!
Cost of acquiring 51% ≈ 0 〈 Mining cost

51% Attack (2/2)

What profit do you get from owning more than 51% of the hashrate?

You can effectively get 100% of the mining reward
· Only mine on your own blocks
Can prevent anyone else from mining – you always produce longest PoW chain

Value of 51% attack 〉Mining Reward

Generalization of vulnerabilities

Bitcoin mining is zero sum

- In general, to increase earnings, someone else needs to be excluded

Members-only Mining

- Let hashrate join a collusion until 80% of the network is in, then exclude the rest
- No incentive not to join
  - Attack succeeds, get increased reward
  - Attack would not fail: conduct attack in such a way that it would not start until the threshold is reached

Example:

- 3 pools collude and then own more than 51% and ignore every 10th block of another pool
- Undetectable!

➡ More profitable than honest strategy!

Post-block Reward Bitcoin

Assumption: average Bitcoin user holds $100,000 in Bitcoin, willing to pay $1000 in fees

- (This is when Bitcoin is near 0 block reward)
- Is mining based off transaction fees sustainable?
- Money must move, must be paid in transaction fees so that miners can collect it as mining reward
- Amount of hashpower going into Bitcoin dependent on mining reward

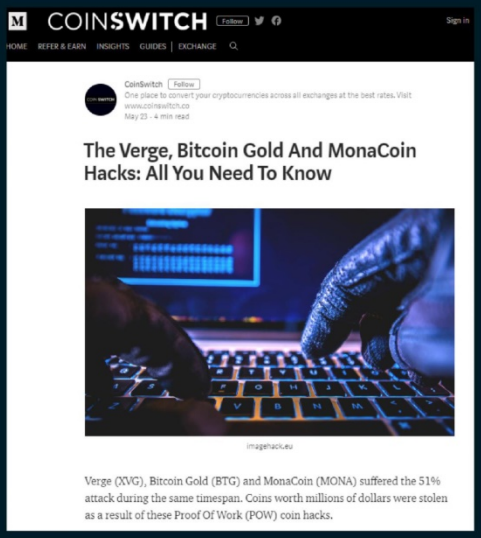
Therefore

- (average fees paid) / (avg holdings) = (cost of attacking) / (market cap)
- In our example, attacker only needs to pay 1% of the market cap of Bitcoin to attack

Post reward Bitcoin must have a high velocity of money to be secure

Many coins are being attacked.

- Verge: exploited a programming error, $1.7M
- Bitcoin Gold: 51% attack, $18.6M
- MonaCoin: Selfish mining attack, $90K
- Ethereum Classic: 51% attack, $1.1M



3 PoS (Proof of Stake)

Proof of Stake: Introduction

Definition
A consensus algorithm in which the member's voting (or mining) power is proportional to **stakes** in the network to select a node to **create** a block and **validate** the one created.

The stakes to select a node to make a block can be vary as follow:
- **the amount of tokens locked up**
- the number of days tokens held (Peercoin)
- random (nxt, Blockcoin)
- round robin (most of DPoS platforms)

Proof of Stake

Simple Minded POS Algorithm 1:
1. Randomly choose a "**block creator**" based on the proportional stake locked-up from the group of already existing validators.
2. The chosen validator, a.k.a. block creator, *creates* a block which points to some previously created block.
3. The chosen validator gets the block reward and the transaction fees

Proof of Stake: Introduction

Simple Minded POS (BFT-style):

1. Randomly choose a validator based on the proportional stake Locked-up from the group of already existing validators.
2. The chosen validator **proposes** a block
3. All the other validators **vote** yes if they think it is a valid block
4. **If ⅔ or more voting power votes yes**, the block is included in the blockchain. Otherwise a new proposer is chosen and we go to 1.
5. The chosen validator gets the block reward and the transaction fees

Proof of Stake: Introduction

Advantages:

1. No electricity wasted
2. Security
3. Reduced risk of centralization

Drawbacks:

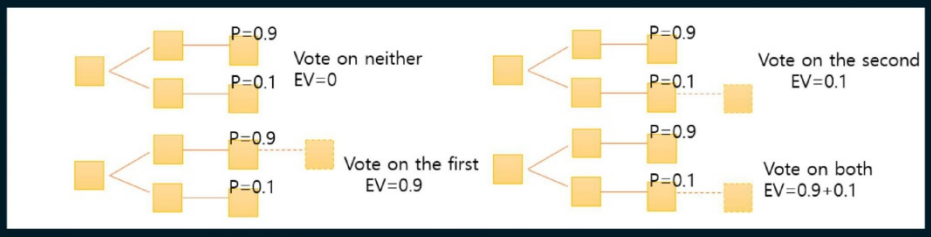
1. Rich get Richer
2. Liquidity problem as funds are locked up
3. Low participation can cause centralization
   - ASICs in PoW can be bought, but stake cannot be accumulated unless a stakeholder sells
4. History of blockchain could be rewritten if malicious attackers acquire stakes

4 PoS 공격

· Nothing at Stake
· 34% 공격
- Censorship Attack
- Stake Grinding Attack
- Data (Un)availability Attack

Attacks: Nothing at Stake

In Simple Minded PoS Algorithm 1, only rewards for creating blocks on multiple competing chains, no penalties.
1.If actors are all economically rational (i.e. pursuing self-interests only), the blockchain never converges in the case of a fork, thus never reaches consensus.
2.Economically rational actors choose both.



Defense: Nothing at Stake

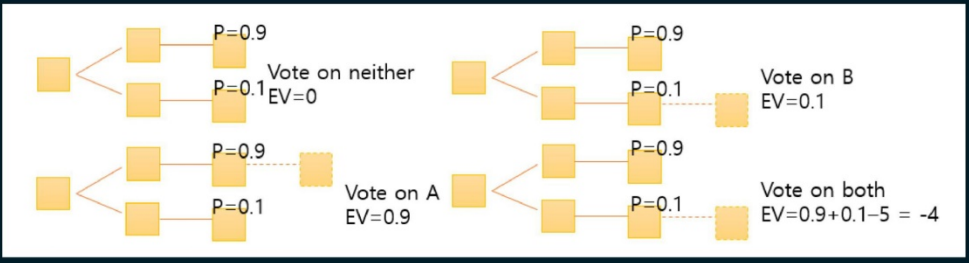
Simultaneous Slasher:

- At every round 64 validators gain signing privileges based on the 2000 block behind the current block.
- The maximum length blockchain is weighted by the signatures of validators.
- If a malicious validator signs on two conflicting chains simultaneously, a future honest validator can include a proof of the double signing in a future block and slash the rewards of the malicious validator, taking 33% of the reward in return for honest behaviour.

Defense: Nothing at Stake

Simultaneous Slasher Drawbacks:

- The selected validators must be online all the time to know if they are given signature privileges.
- Hope validators don't collude ahead of time



34% Attack

Attack on Finality

· Change the history of the blockchain, thus creating two conflicting histories causing a fork in the blockchain.

Defense:

· Freeze the blocks every n blocks
· Community needs to communicate over social media, reddit, etc.

34% Attack

Liveness Denial

· 〉=34% of voting power could ensure that the blockchain never reaches consensus.

Defense:

· Protocol could force rotate the validator set if, after a long period of time, blocks don't get created
· The community could decide a hardfork

Censorship Attack

Censorship

· 〉=34% of voting power could effectively prevent from certain valid transactions to be included in the blockchain
· If the attacker has 〈67% power, the honest nodes can refuse to mine on blocks that they believe were censored, transforming this into a Liveness Denial attack.
· If the attacker 〉=67% voting power, it can workaround above strategy.

Censorship Attack

Problem: it is difficult to differentiate

· A user K attempts to send Transaction T but it got unfairly censored
· A user K attempted to send Transaction T but the transaction fee was very low, not enough, it never got included
· A user K never sent Transaction X at all.

Censorship Attack

Defense: Make censorship costly

- If 100 out of 100 validators sign a block then everyone gets 100% of the rewards.
- If 99 out of 100 validators sign a block, penalize the network i.e. everyone gets 99% of the rewards
- Altruistic validators won't sign a block if they believe transactions are censored
- Penalize everyone if a block is ignored

Censorship Attack

Drawbacks of "Make censorship costly"

- Malicious validators could refuse to sign a valid block, penalizing rest of the network for no reason.
- Assumes some altruists exist.
  - What if no one is altruistic? Validators would avoid including transactions that could cause the block to be censored.

Censorship Attack

Drawbacks of "Make censorship costly"

· Malicious validators could refuse to sign a valid block, penalizing rest of the network for no reason.
· Assumes some altruists exist.
– What if no one is altruistic? Validators would avoid including transactions that could cause the block to be censored.

Censorship Attack

Defense: Timelock Cryptography Algorithm

1.Sender creates transaction t
2.Sender encrypts t using p and q to get c, and sends c and pq to a validator alongside a zero-knowledge proof that the values were produced correctly.

$$d = c^{2^n} \mod pq$$

3.The validator includes c and pq into the blockchain
4.There is a protocol rule that the validator must submit the correct original transaction t into the blockchain within 24 hours.

Censorship Attack

Drawbacks of "Timelock Cryptography Algorithm"

Honest validators would be open to using this scheme

- They don't know what they are including in the block until 24 hours later
- Can penalize validators if t is not revealed in time by slashing a large security deposit

Either complete censorship or none at all

- Validators can collude ahead a time and refuse to include transactions without t , p, q, c

Stake Grinding Attack

Problem

In a chain-based ecosystem, need a way to randomly pick the next validator.

- Need to pick an infinite sequence of validators in case the picked validator is offline

Next chosen validator depends on previous block's signature

- The current validator can repeatedly produce (a.k.a. "grind") new signatures to improve his chance of being picked again.
- In NXT, passing up the opportunity of being the validator for the current round gives the user a chance to manipulate randomness for future rounds. This carries an opportunity cost equal to the block reward, but sometimes the new random seed would give the validator an above-average number of blocks over the next few dozen blocks.

Stake Grinding Attack

Defense

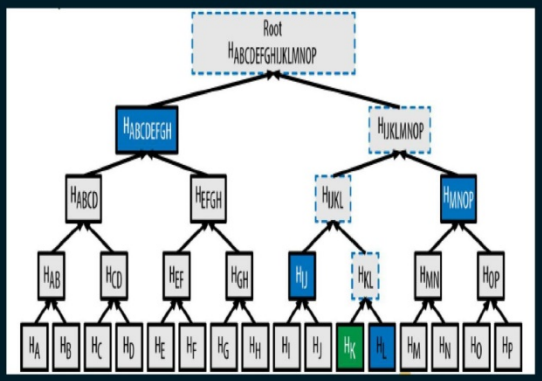
- Not to use information that can be easily manipulated as source data for the randomness
- Require all the validators deposit their stake well in advance
- Use some sort of secret sharing/threshold signature scheme, and have multiple validators collaboratively generate the random value.
  - Unless majority colludes, this is a safe scheme

Data (UN)availability Attack

The Normal Situation

- Attacker makes a block with invalid or malformed transactions, it is possible to construct a proof from the transaction and its corresponding Merkle tree to prove invalidity of the block.

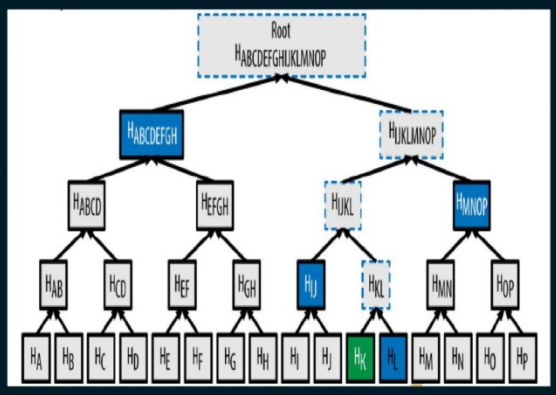
1. If someone submits an invalid fraud proof, their funds get slashed.
2. If the fraud proof is valid, the malicious actor's reward gets slashed, the honest actor gets a share of the reward.



Data (UN)availability Attack

Attack:

· Attacker makes a block with invalid or malformed transactions, but does not include all the relevant data for someone constructing a fraud proof.

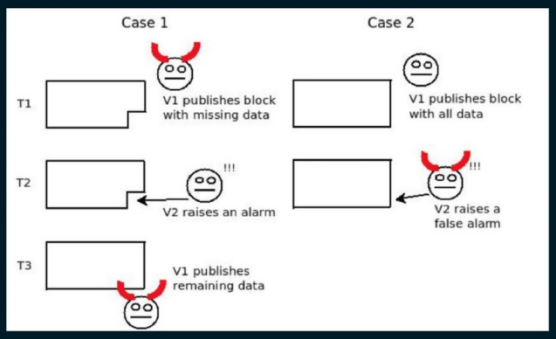


EcoVerse™ DeLight Chain

Data Unavailability Attack

Problem

· Not distinguishable the following two cases



Source: https://bit.ly/2Jh4Loo

EcoVerse™ DeLight Chain

Data Unavailability Attack

Defense

- Require blocks to commit to the Merkle root of this "extended" data (use erasure codes),
- Probabilistically check that the majority of the extended data is available.
- We know that one of three things is true:

1. The entire extended data is available, the erasure code is constructed correctly, and the block is valid.
2. The entire extended data is available, the erasure code is constructed correctly, but the block is invalid.
3. The entire extended data is available, but the erasure code is constructed incorrectly.

5 Delegated Proof of Stake

Delegated PoS: Introduction

Simple Minded DPoS

· Community elects a small number (20) of delegates (often called “witnesses”).
· Delegates take a turn by round-robin rotation. A delegate in turn creates a block and gets a reward. If the delegate in turn fails to produce a valid block, then it is not paid, and may be voted out in the future.

Delegated PoS: Introduction

Pros

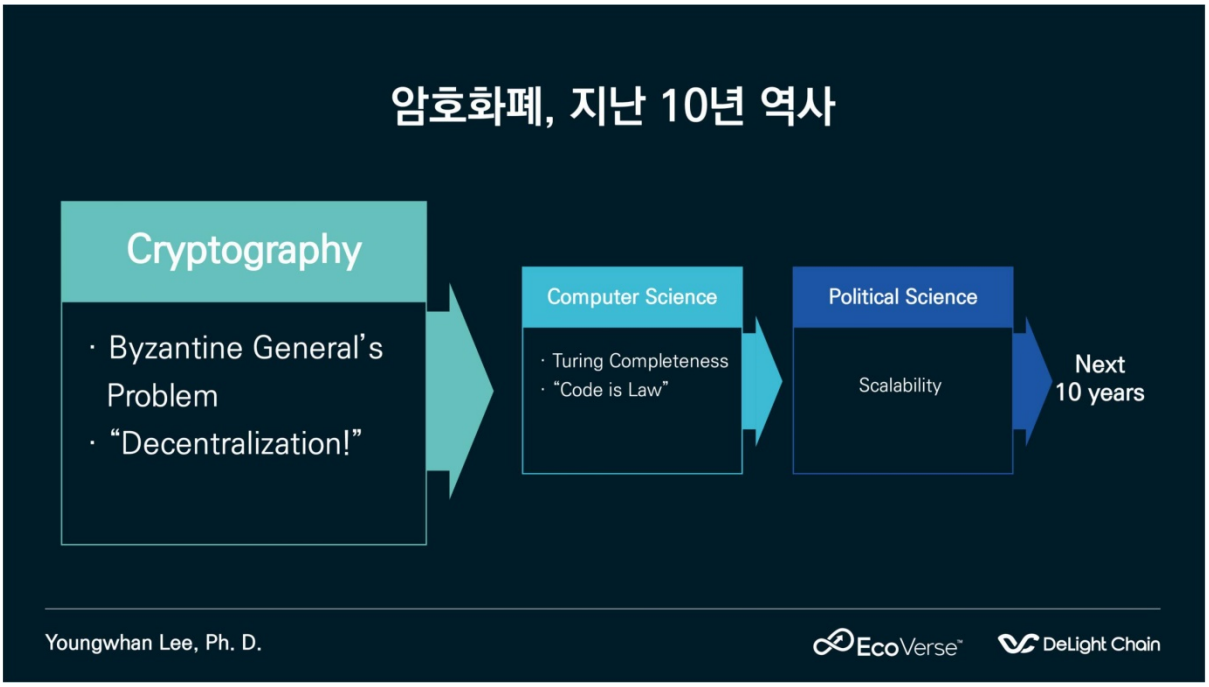
· **Fast**
– Transactions can be confirmed as low as one second
– More than 1000 TPS, adopted as a solution to scalability
· **Efficient**
– Network parameters such as fee schedules, block intervals, transaction sizes can be decided by elected delegates.
· **Used by many recent cryptocurrency platforms**
· **Double spending attack can be difficult**

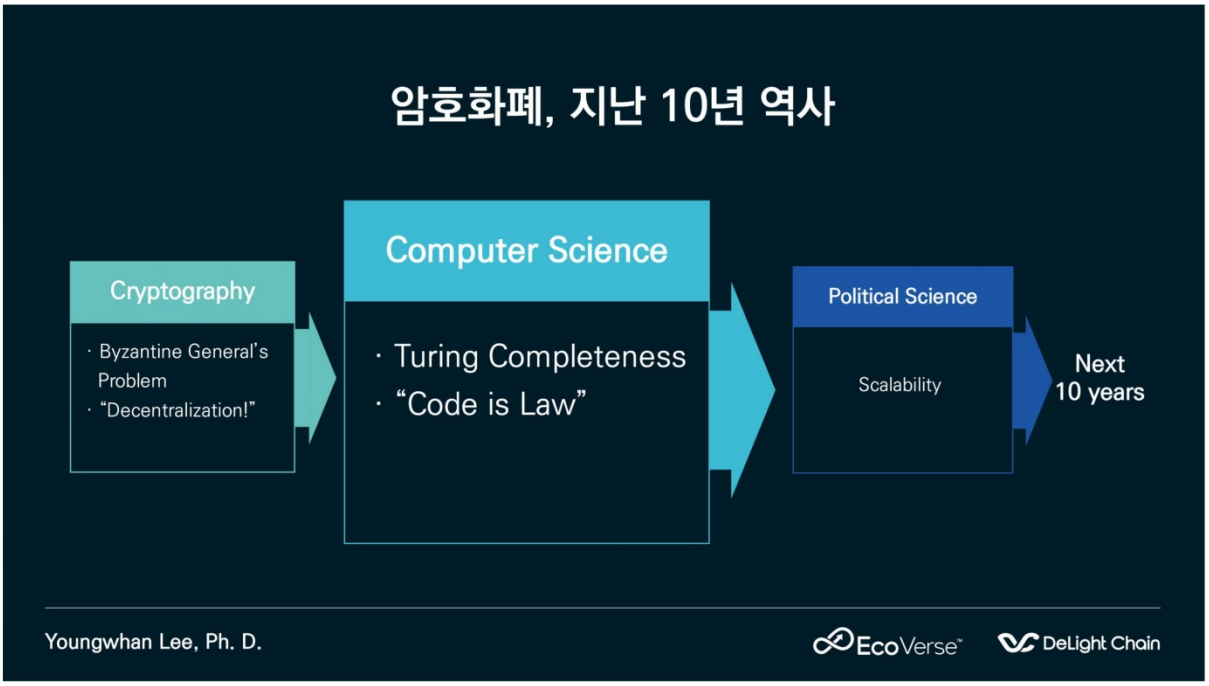
Delegated PoS: Introduction

Cons

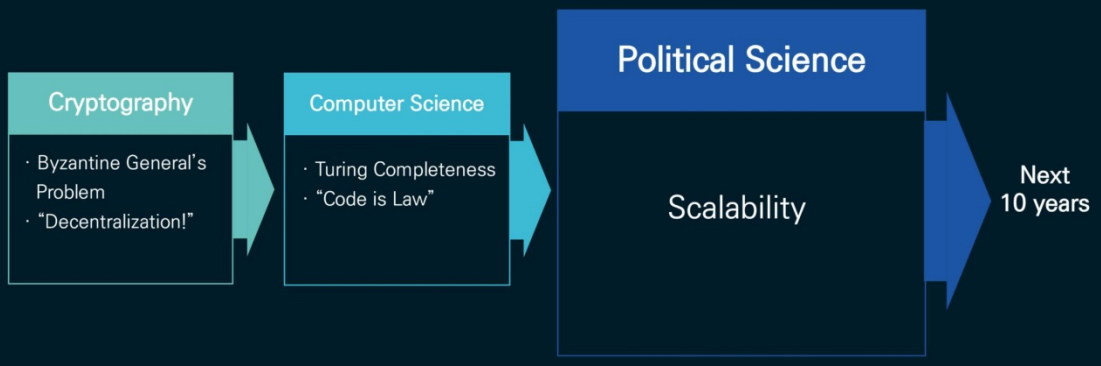
- Centralized
  - Vulnerable to network attacks such as DoS (Denial of Service)
- Delegates require to have high computing power and can not easily replaced by ordinary stake holders
- Delegates can be colluded
  - Supposedly highly accountable

6 암호 화폐 역사


암호화폐, 지난 10년 역사
Cryptography
· Byzantine General's Problem
· "Decentralization!"
Computer Science
· Turing Completeness
· "Code is Law"
Political Science
Scalability
Next 10 years
Youngwhan Lee, Ph. D.
EcoVerse
DeLight Chain


암호화폐, 지난 10년 역사
Cryptography
· Byzantine General's Problem
· "Decentralization!"
Computer Science
· Turing Completeness
· "Code is Law"
Political Science
Scalability
Next 10 years
Youngwhan Lee, Ph. D.
EcoVerse
DeLight Chain

암호화폐, 지난 10년 역사



Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

"Dr. Doom" Roubini

'Dr Doom' Nouriel Roubini attacks cryptocurrencies as 'the mother and father of all scams and bubbles, and labels blockchain 'the most overhyped technology ever'

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

If problems are left untreated

Incentives on cryptos are nullified, and the market will self-destruct.
암호화폐 유입 유인 소멸로 시장 자체가 붕괴

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

A Bit of Artificial Intelligence

인공지능의 기술

룰 기반 기술: 주로 전문가 시스템 위주로 발달
- IBM Watson
- Wolfram Alpha (Siri의 기반기술)

신경망기반 기술

· 1943년 McCIloch and Pitts proposed a computational model for neural networks, similar to human brains.
· 2006년 Hinton proposed deep neural network called restricted Boltzman machine to model each layer.
· AlphaGo has three versions: Lee, Master, Zero
- Zero vs. Lee > 100 wins 0 losses
- Zero vs. Master > 89 wins 11 losses

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

7 Remaining Problems and AI

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

Remaining Problems

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

Self-Sustainability in Mechanism Design

A (crypto-currency) mechanism is self-sustainable if it meets, at any given time, the following two conditions

- voluntary participation, and
- incentive compatibility

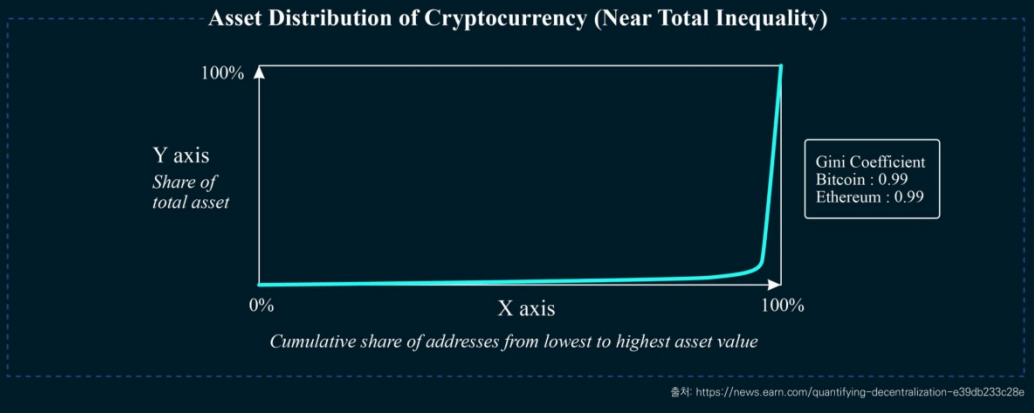
A mechanism is incentive-compatible if every participant can achieve the best outcome to himself/herself just by acting according to his/her true preferences.

EcoVerse™ Definition: Incentive Compatibility

Suppose a cryptocurrency incentive mechanism gives away only one monotonic type of incentive. If such a mechanism is denoted by C, and participant x, and time t, then we can define the incentive compatibility as follows:

$\forall C\ \forall x\ \forall t\ ((\text{incentive-paid } x, t, C) > (\text{incentive-wanted } x, t, C)) \rightarrow (\text{incentive-compatible } C)$

Gini Coeffcient for Cryptocurrency



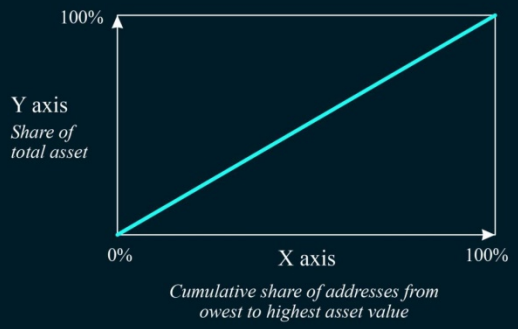
출처: https://news.earn.com/quantifying-decentralization-e39db233c28e

Consensus Algorithm

1.Purposes
- Ledger Synchronization
- Distributing Seigniorage

2.Players
- Block Producers (–〉 Miners)
- Incentive Takers (–〉 Miners)

Employing AI Agents for Block Producing



When AI Agents are employed in Blockchain

1.Advantages
- No incentive to AI > Creative incentive distribution possible.
- Arguably no liars (no greed) 〉No collusions among agents
- Attacks difficult: Censorship attack, Sybil attack, ···

2.Disadvantages
- Conflict resolution mechanism must be implemented > slow
  - When two or more agents may have different worldviews (a.k.a. a fork)

AI Agents Must be

1.Independent from human operators

· Difficult to hack, collude, cheat, and censor

2.Evolving through learning

· Fraud transaction detection: e.g. double spending

· Money laundering detection

Blockchain and AI

			Token	Remarks
Blockchain in AI	AI Marketplaces	Singularity NET	AGI	Services thru Smart contracts
		DeepBrain Chain	DBC	AI hardware computing resources through a network
	Crowdsourced Predictive Models for Hedge Funds	Numerai	NMR	The best performing models can win the weekly prices
	Investment Management	Peculium		Automated machine learning to learn from the analysis of hist. info from crypto market
AI in Blockchain	Smart Contract Replacement	BosCoin 1.0	BCS	Solution to Halting Problem(?), Efficiency, Scalability
		Ontology	ONT	
	Consensus-Block Prod. Consensus-Wealth Dist.	EcoVerse	ECX, ECR	AI-DPoC
	Network Management	EcoVerse	ECX, ECR	Conflict Resolution
	Volume of Coin Printing	EcoVerse	ECR	Monetary Volume Control
	Incentive Diversification	EcoVerse	ECR	AI-ARS

Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

Computing Contribution(C) of a Participant (p)

$$C_p = \sum_{d=1}^{l} \left(W_d \cdot M_d \cdot \sum_{a=1}^{m} W_{d,a} \cdot A_{p,d,a} \right) + \sum_{c=1}^{n} W_c \cdot B_{p,c}$$

Where

C_p : contribution of participant 'p'
W_d: dApp 'd's weight of contribution to the entire network
M_d: MAU (Monthly Active User) of dApp 'd'
$W_{d,\,a}$: participant's weight of activity a on dApp 'd'
$A_{p,\,d,\,a}$: participant 'p's amount of activity a on dApp 'd'
W_c : committee 'c's weight on all committees
$B_{p,\,c}$: participant 'p's amount of activity on committee 'c'

Youngwhan Lee, Ph. D.

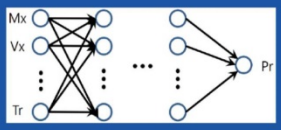
EcoVerse™ DeLight Chain

New Issuance of Coins : Constant Value-Increase Strategy

Quantity Theory of Money

M * V = P * T

Where M is the amount of currency issued, V is the rate of currency circulation, P is the value of the currency, and T is the transaction size.

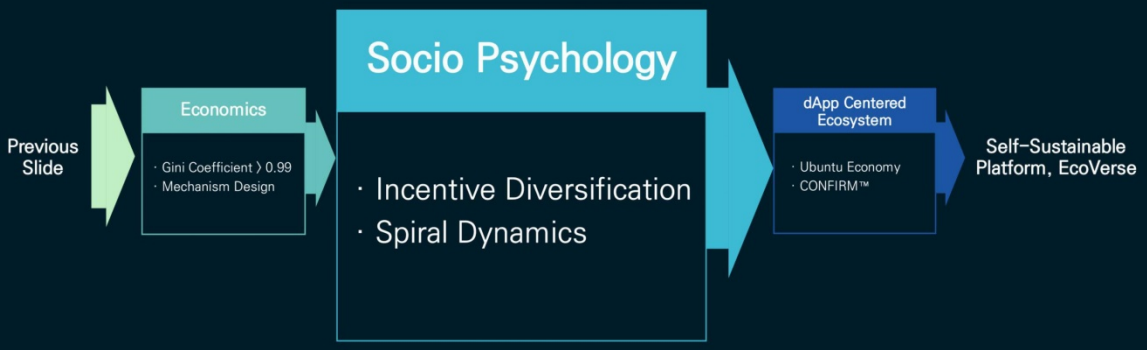


- In EcoVerse™, the appropriate volume of currency, M, for ECR is determined by estimating the future value of P based on M, V, P and T of ECX and ECR.
- The volume of new coin issuance will be limited to make sure that the price will move to the right-upward direction.

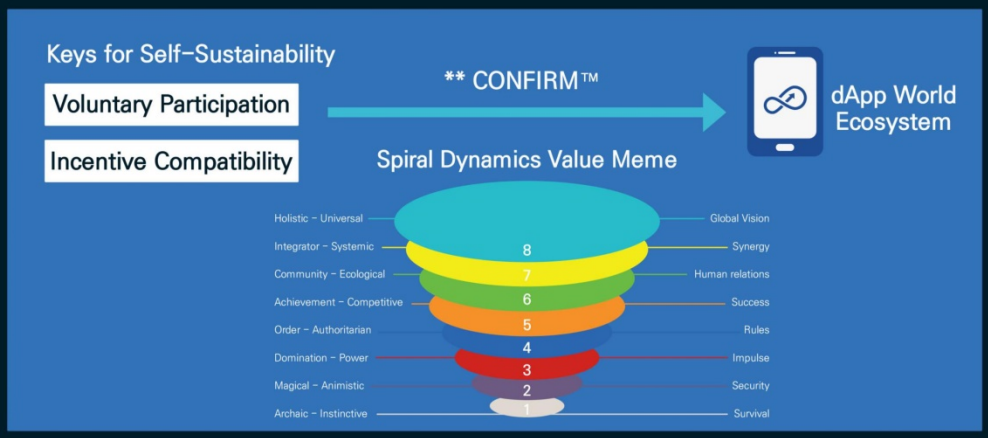
Youngwhan Lee, Ph. D.

EcoVerse™ DeLight Chain

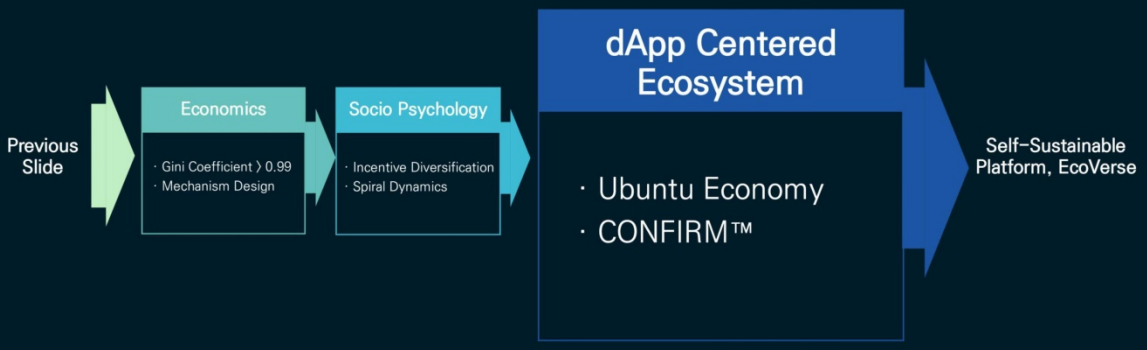
Remaining Problems



Mechanism Design and Socio-Psychology



Remaining Problems



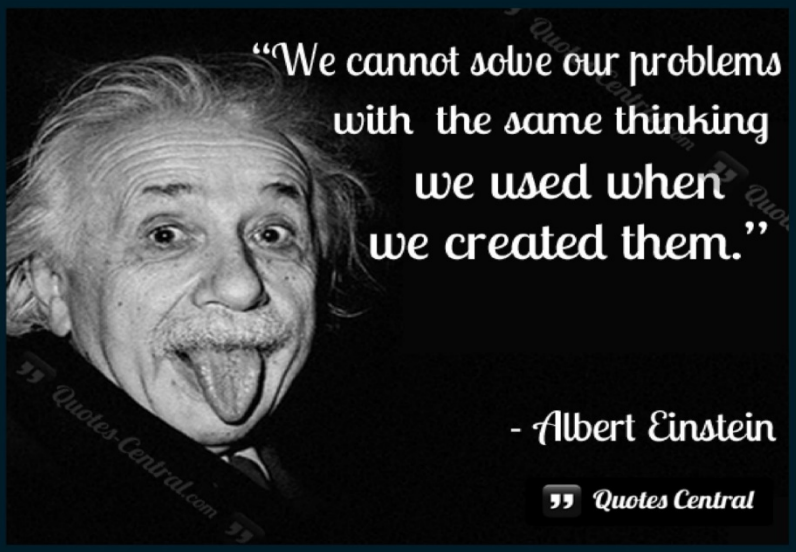
8 Conclusion

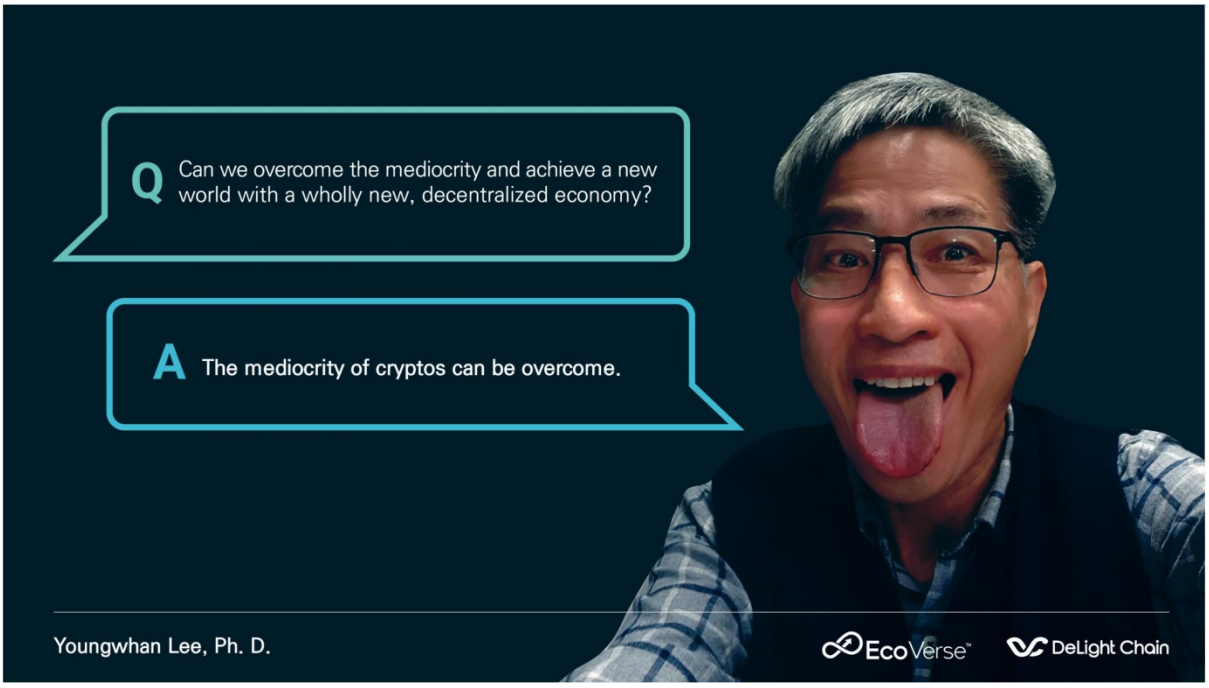
Youngwhan Lee, Ph. D.
EcoVerse™ DeLight Chain

Revisited!

"Dr. Doom" Roubini

'Dr Doom' Nouriel Roubini attacks cryptocurrencies as 'the mother and father of all scams and bubbles, and labels blockchain 'the most overhyped technology ever'




Q Can we overcome the mediocrity and achieve a new world with a wholly new, decentralized economy?
A The mediocrity of cryptos can be overcome.
Youngwhan Lee, Ph. D.
EcoVerse
DeLight Chain

EcoVerse™ Platform is the first-ever
self-sustainable platform
embracing Ubuntu economy
Youngwhan Lee, Ph. D.
EcoVerse
DeLight Chain

References

EcoVerse Manifesto. https://bit.ly/2BncBY2
EcoVerse Whitepaper. https://ecoverseglobal.io/17.
To Integrate Blockchain and AI Part 1.https://link.medium.com/jQJtOhpssT
To Integrate Blockchain and AI Part 2.https://link.medium.com/j4Insn5rsT
To Integrate Blockchain and AI Part 3.https://bit.ly/2R8GGPy
To Integrate Blockchain and AI Part 4.https://bit.ly/2HwR703
Youngwhan Nick Lee. Replanning in Response to Conflicts. University of Illinois Press. Doctoral dissertation.
Requirements for Self-Sustainable Blockchain, Part 1.https://bit.ly/2KDiV0D
Requirements for Self-Sustainable Blockchain, Part 2.https://bit.ly/2RrkXne
Requirements for Self-Sustainable Blockchain, Part 3.https://bit.ly/2PPgZUy.
Requirements for Self-Sustainable Blockchain, Part 4.https://bit.ly/2Pl6tlL.
Requirements for Self-Sustainable Blockchain, Part 5.https://bit.ly/2A75zVs
Requirements for Self-Sustainable Blockchain, Part 6.https://bit.ly/2TwxFlV
Answers to Roubini, “Dr. Doom.” https://bit.ly/2PC7riX
Defending ICON’s Empty Blocks and Other Issues. https://bit.ly/2F4L5lQ
Making a cryptocurrency mechanism to be incentive-compatible. https://bit.ly/2KnTksq
Buterin questions, EcoVerse(tm) answers! https://bit.ly/2Qeb7rc
Are Cryptocurrencies Self-Sustainable? https://bit.ly/2KsaDbS

Thank you

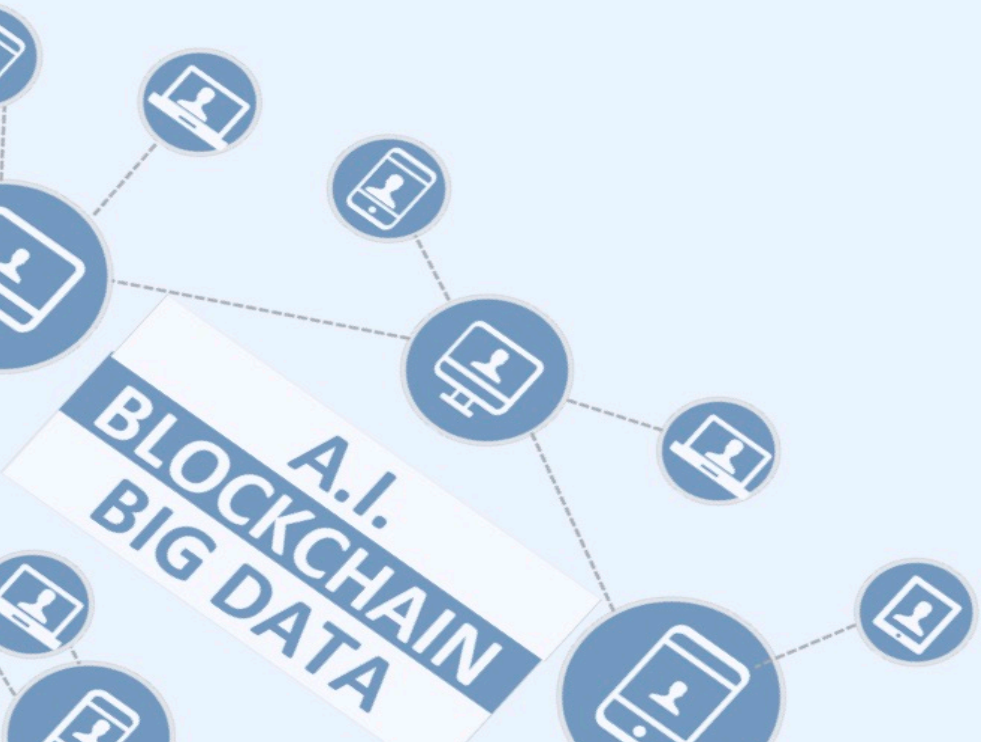
Youngwhan Lee, Ph. D.
EcoVerse™ DeLight Chain

5강

Ethereum Dapp

이 광 열 대표

(주식회사 업라이프)



강의 동영상 URL

비공개

Ethereum Dapp

㈜업라이프 이광열

Contents

1. Ethereum?

2. Ethereum Concepts

3. Tools & Technologies

4. Training

1. Ethereum?

Introduction

- Welcome to the Etherium Basic Course! This course is aimed at developers interested in developing decentralized applications in the EtherBar block chain.

- The goal of this course is to introduce the minimum concepts you need to understand in advance, and to introduce the basic tools you need to start developing decentralized applications.

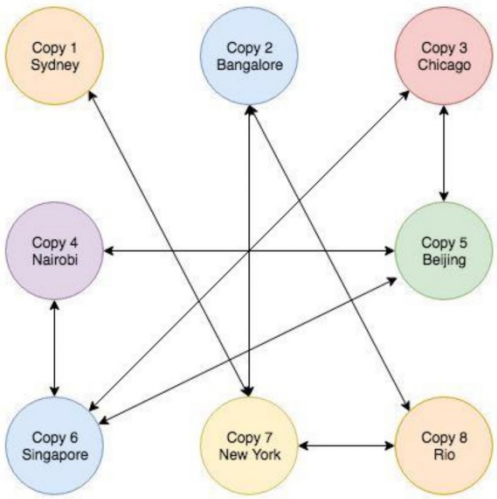
More than payments

Bitcoin blockchain is primarily used for sending money between various parties on the blockchain without the need for a central authority such as a bank. A 19 year old developer by name Vitalik Buterin wanted to apply the idea of decentralization (no central authority) to more than just money transfer. He wanted to build applications that could run globally without any central authority in control. For example, if you are a google user, google as a company owns your data and they have the right to remove your account if they wish. In 10 years, google could shut down in which case all your data could be lost.

- Vitalik proposed to add a scripting language to Bitcoin to be able to build applications. However, after failing to gain agreement from the Bitcoin development team, in January 2014, he officially published the white paper proposing the development of a new platform with a more general scripting language. A team formed shortly and one of the developers, Dr. Gavin Wood soon released the Ethereum yellow paper, which covered the Ethereum Virtual Machine (EVM), the runtime environment that executes all of the smart contracts on the network (You will learn more about EVM and smart contracts in the next sections). The development of the platform was funded through a crowdsale in July–August 2014, with the participants buying the Ethereum value token (ether) with bitcoin.

Global Computer

- Ethereum is a public, blockchain based distributed computing platform. It can be thought of as **one big computer** made up of small computers around the world. You can write applications and run them on this global computer. The platform guarantees that your application will always run without any downtime, censorship, fraud or third-party interference. Apart from running applications, Ethereum blockchain can also transfer money between 2 parties without a central authority.
- All these computers (also called nodes) are connected to one another and have a **full copy of the code and data**. When you deploy your code on to the Ethereum blockchain, the code is **replicated across all the nodes** in the network. When your application stores any data, even that **data is replicated** across all the nodes. There are thousands of nodes in the network and it is almost impossible for anyone to stop all the nodes. This insures your application to be always accessible.

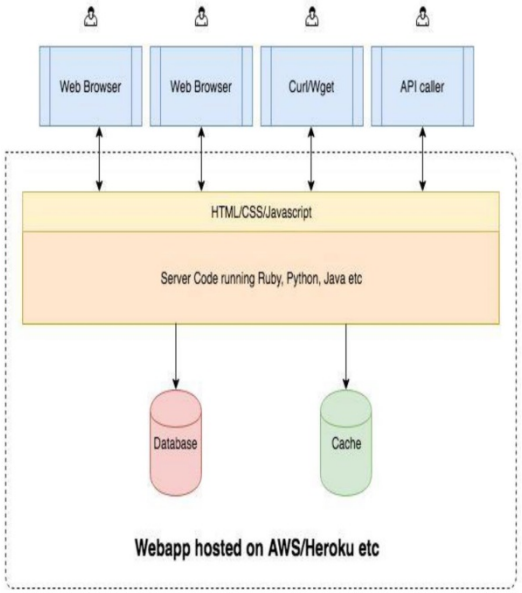


Webapp Architecture

- One of the best ways to understand Ethereum is by comparing it with a **traditional client/server architecture**. If you are a web developer, the diagram on the right should make sense (You can still follow along if you are not aware of the web architecture). It is a high level client/server architecture of a simple web application.

- A typical web application consists of **server side code** which is usually written in a programming language like **Java, C#, Ruby, Python etc**. The frontend code is implemented using HTML/CSS/Javascript. This entire application is then hosted on a hosting provider like **AWS, Microsoft Azure, Google Cloud Platform, Heroku or a VPS.**

- Users interact with the web application using a client such as web browser, curl/wget (command line) or through an API. Note that there is **one web application which is centralized and all the clients interact with this one application**. When a client makes a request to the server, the server processes the request, interacts with the database and/or cache, reads/writes/updates the database and returns a response to the client.

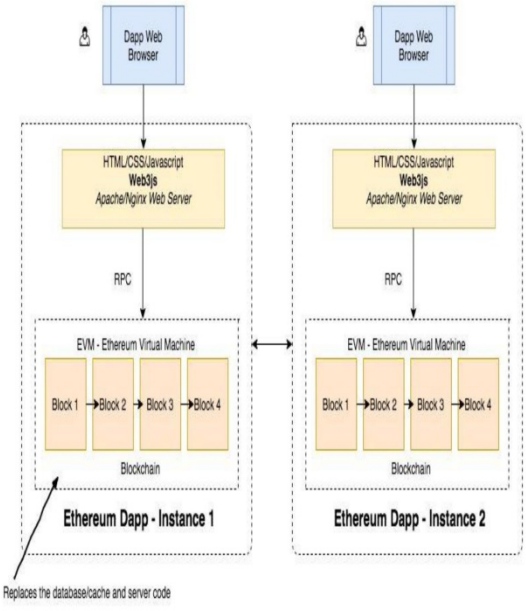


Ethereum Architecture

- If you notice the diagram on the right, every client (browser) communicates with its own instance of the application. There is no central server to which all clients connect to. This means, in an **ideal decentralized world**, every person who wants to interact with a dapp (Decentralized Application) will need a full copy of the blockchain running on their computer/phone etc. That means, before you can use an application, you have to download the entire blockchain and then start using the application.
- We don't live in an ideal world and it is unreasonable to expect everyone to run a blockchain server to use these apps. But the idea behind decentralization is to not rely on a single/centralized server. So, the community has come up with solutions (hosted blockchain servers, metamask etc.) where you don't have to spend lot of your hard disk and RAM downloading and running a full copy of the blockchain but also not compromise on the decentralized aspect. We will evaluate those options in the future lessons.

- Now, what exactly is in the Ethereum blockchain? The blockchain has 2 main components:
- **Database**: Every transaction in the network is stored in the blockchain. When you deploy your application, it is considered as a transaction. If you have for example a Voting application that allows anyone to vote for candidates, a vote for a candidate would be considered a transaction. All these transactions are public and any one can see this and verify. This data can never be tampered with. To make sure all the nodes in the network have same copy of the data and to insure no invalid data gets written to this database, Ethereum uses an algorithm called Proof of Work to secure the network. (http://ethereum.stackexchange.com/questions/14/what-proof-of-work-function-does-ethereum-use)

- **Code**: The database aspect of blockchain just stores the transactions. But where is all the logic to vote for candidate, retrieve the total votes etc. In Ethereum world, you write the logic/application code (called contract) in a language called Solidity. You then use the solidity compiler to compile it to Ethereum Byte Code and then deploy that byte code to the blockchain (There are few other languages you could use to write contracts but solidity is by far the most popular and relatively easier option). So, not only does Ethereum blockchain store the transactions, it also stores and executes the contract code.
- So basically, **the blockchain stores your data, stores the code and also runs the code in the EVM (Ethereum Virtual Machine).** You will learn more about ByteCode and EVM in the future sections.
- To build web based Dapps, Ethereum comes with a handy javascript library called web3.js which connects to your blockchain node. So you can just include this library in your famous js framework like reactjs, angularjs etc and start building.



2. Ethereum Concepts

What are smart contracts?

- we discussed how we can write applications in the Solidity programming language and deploy it on to the Ethereum blockchain. In Ethereum, these applications are called Smart Contracts.
- You must be wondering why these applications are called smart contracts. In general, **contract is a written agreement between two or many parties that is intended to be enforced by law**. If we take this written contract and translate it in to code and deploy on the blockchain, we get digital contracts. But the beauty of this code on the blockchain is that it can enforce the agreement between parties and that is the reason they are called "smart contracts".
- How can this code enforce the agreement? If you remember, once a contract is deployed to the blockchain, it can neither be stopped nor modified. That is how the agreement is enforced. Let's take a look at a simple example to understand this better.

- Let's say we want to build a **Crowdsale application**. There is a creator who wants to raise $10,000 to create a product and there are potential customers who are interested in this product and are willing to pre-pay for it. The agreement is, each customer will contribute anywhere between $10 - $10,000 and **if the goal is met, the money is sent to the creator**. If not, **money is sent back to the contributors**. This is an ideal use case to use smart contract to enforce the agreement between the creator and supporters. It is trivial to implement this logic in a centralized application as well. The advantages of implementing this in a smart contract are
- The money sent by all the contributors is in the smart contract. Neither the contributor nor the creator can take that money.
- The code can be implemented so that the money is sent to the creator as soon as the goal is reached.
- The code can be implemented so anyone can trigger a refund to all the customers if the goal is not reached within a certain time frame.
- This code can not be tampered once it is deployed on to the blockchain.

Ether & Denominations

- Just like in the real world, each country has it's own currency like **USD, INR, RNB, GBP, EUR** etc, each blockchain has it's own currency. In the case of Ethereum blockchain, the native currency is called **Ether**. There are exchanges where you can convert Ether to any other fiat currency like USD or EUR. You can see the current price of Ether here
- In the real world, currencies have various denominations. For example, a US Dollar is equal to 100 cents and it has various denominations such as pennies (1 cent), nickel (5 cents), dime (10 cents), quarter (25 cents). Depending on your country and currency, you probably have various denominations as well.
- **Ether also has various denominations as shown on the right. The only two you should really remember are Ether and Wei. Wei is the lowest denomination and this is the denomination you use in your smart contracts.**

Table 1. Ether Denominations and Unit Names

Value (in wei)	Exponent	Common Name	SI Name
1	1	wei	wei
1,000	10^3	babbage	kilowei or femtoether
1,000,000	10^6	lovelace	megawei or picoether
1,000,000,000	10^9	shannon	gigawei or nanoether
1,000,000,000,000	10^{12}	szabo	microether or micro
1,000,000,000,000,000	10^{15}	finney	milliether or milli
1,000,000,000,000,000,000	*10^{18}*	*ether*	*ether*
1,000,000,000,000,000,000,000	10^{21}	grand	kiloether
1,000,000,000,000,000,000,000,000	10^{24}		megaether

What is an Ethereum address?

- To login to any website like google, you usually use an email/username and password. Your username is your identity in google and you use your username/password to authenticate with google.
- In Ethereum blockchain, address is your identity. An Ethereum address looks like this: **001d3f1ef827552ae1114027bd3ecf1f086ba0f9**. An address has a corresponding private key. You can think of private key as a password that only you know. You need this pair of address+private key to interact with the blockchain. Below are few key things to **memorize** without which it is hard to understand blockchain and Ethereum:
- Ethereum address is public and you can share it with anyone in the world.
- The private key should never ever be shared with anyone.
- The address+private key is not stored in any database. Only you are in control of them.
- In the future sections, you will learn how to manage these addresses and ways to use them.

- How is an Ethereum address generated?
- Below is a quick explanation of how this address ex: **001d3f1ef827552ae1114027bd3ecf1f086ba0f9** is generated. This assumes that you know how public key cryptography works. You can learn more about it here: https://en.wikipedia.org/wiki/Public-key_cryptography.

- **Generate a private key**
- k(private key) = f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315

- **Derive the public key from the private key**
- K(public key) = 6e145ccef1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b83b5c38e5e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32ccd0

- **Calculate the hash of the public key by using keccak256 algorithm**
- Keccak256(K) = 2a5bc342ed616b5ba5732269001d3f1ef827552ae1114027bd3ecf1f086ba0f9**001d3f1ef827552ae1114027bd3ecf1f086ba0f9**

- **Take the last 20 bytes of the generated hash to get the Ethereum address**
- 0x001d3f1ef827552ae1114027bd3ecf1f086ba0f9

What is an Ethereum account?

The combination of Ethereum address and it's private key is referred to as an **account**. Not only that, an account in Ethereum can hold balance (Ether) and can send transactions. Ethereum has 2 types of accounts.

1. Externally owned accounts (EOA): This is the account we mentioned above which is a combination of public address and private key. You can use these accounts to

- Send and receive Ether to/from another account
- Send transactions to smart contracts

2. Contract accounts: These accounts **don't have a corresponding private key**. These accounts are generated when you deploy your contract to the blockchain. You will see them referred to as just contracts in lot of places (instead of contract accounts). Some key features of contract (accounts) are

- They can send and receive ether just like EOA
- They have code associated with them unlike EOA
- Transactions have to be triggered by an EOA or another contract
- It will get a lot more clearer in the future chapters when we create and use these accounts.

What is an Ethereum wallet?

- Ethereum Wallets are software plugins/libraries that are used to store and manage your Ethereum accounts. Wallets allow you to manage multiple accounts, provides functionality to sign transactions, track balances and so on. Wallets can be broadly classified into 2 types:
- **Non-Deterministic Wallet**: This is a type of wallet that uses a random private key and generates a public key from it. You can generate as many public/private key pairs but there is no relation between each pair of keys.
- **Deterministic Wallet**: In this wallet, keys are derived from a single starting point known as a **seed**. The seed allows a user to **easily back up and restore a wallet** without needing any other information and can in some cases **allow the creation of public addresses without the knowledge of the private key**. Seeds are typically serialized into human-readable words in a Mnemonic phrase. If you have used a plugin like metamask, it would have asked you to save the 12 word seed when you first installed it. The Metamask section in the next chapter has a video demo of the deterministic wallet.

Gas, Gas Price and Gas Limit

- **Gas**
- We know that you can deploy contracts on the Ethereum blockchain and execute transactions on it. However, there is a cost associated with each interaction. You have to pay Ether to the miners in the network to execute a transaction on the blockchain.
- Who decides how much Ether to pay for a transaction? This is where it gets interesting and also where lot of developers new to Ethereum get confused. The answer is, the yellow paper has specification on how many units of work a transaction has. For example, if your transaction is to simply add two numbers, that is 3 units of work. If it is multiplication, that would be 5 units of work and so on. **This unit of work is called gas.**

- **Gas Price**
- We now know how much gas each transaction will need. But we still don't know how much Ether we have to pay the miners. That is determined by **Gas Price** and the interesting thing is, you can set whatever gas price you want. For example, you can say "**I am willing to pay 3 Gwei per gas**" for my transaction. If your transaction takes 100000 gas and you set the gas price to 3Gwei, you end up paying 300000 Gwei for your transaction.
- The higher the gas price you set, the sooner your transaction gets mined. This is because, most of the miners sort the transactions in the descending order of gas price and pick the transactions with higher gas price to include in the block. If you set the price low, your transaction will eventually get included in the block but you might have to wait for a bit.

- **Gas Limit**
- It is very difficult to know exactly how much gas your transaction will take. As a developer, you don't want to blindly execute a transaction and realize your transaction took hundreds of dollars worth of Ether. To avoid this situation, you can specify a **gas limit** which indicates the maximum amount of gas you are willing to buy to execute your transaction.

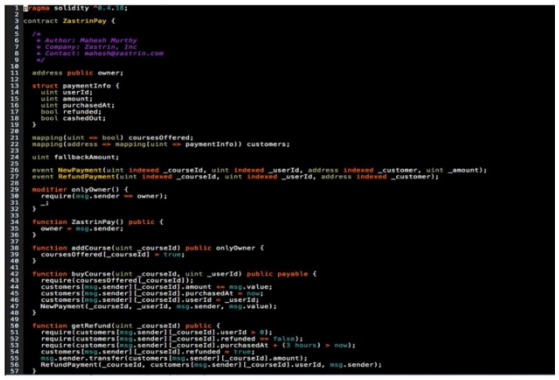
- *Don't confuse this with Block gas limit. Block gas limit is the maximum cap applied to each block in Ethereum. Currently, a block can only include transactions whose total sum of gas is less than 8 million. The reason you have a limit for each block is to prevent someone from just writing an infinite loop in which case the transaction wouldn't complete it's execution resulting in block not getting mined.*

Byte Code

- Smart contract code is usually written in a high level programming language such as **Solidity**. This code gets compiled to something called the **EVM bytecode** which gets deployed to the Ethereum blockchain. This is very similar to a programming language like Java where the code gets converted to JVM Byte code. The Ethereum runtime environment only understands and can execute the bytecode.

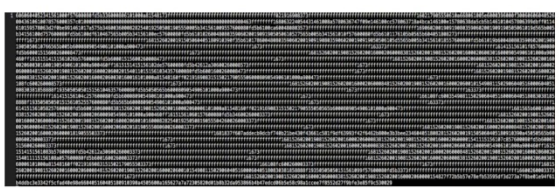
- One of the benefits of this design is that it gives developers option to use other programming languages to implement smart contracts. Currently, there are a handful of languages like **Vyper** (similar to Python) that compiles down to the EVM bytecode. If you are a language designer, you can just refer to the Ethereum yellow paper and implement your own programming language for Ethereum!

- **Sample Solidity Code**



```
pragma solidity ^0.4.18;

contract ZastrinPay {

  /*
   * Author: Mahesh Murthy
   * Company: Zastrin, Inc
   * Contact: mahesh@zastrin.com
   */

  address public owner;

  struct paymentInfo {
    uint userId;
    uint amount;
    uint purchasedAt;
    bool refunded;
    bool cashedOut;
  }

  mapping(uint => bool) coursesOffered;
  mapping(address => mapping(uint => paymentInfo)) customers;

  uint fallbackAmount;

  event NewPayment(uint indexed _courseId, uint indexed _userId, address indexed _customer, uint _amount);
  event RefundPayment(uint indexed _courseId, uint indexed _userId, address indexed _customer);

  modifier onlyOwner() {
    require(msg.sender == owner);
    _;
  }

  function ZastrinPay() public {
    owner = msg.sender;
  }

  function addCourse(uint _courseId) public onlyOwner {
    coursesOffered[_courseId] = true;
  }

  function buyCourse(uint _courseId, uint _userId) public payable {
    require(coursesOffered[_courseId]);
    customers[msg.sender][_courseId].amount += msg.value;
    customers[msg.sender][_courseId].purchasedAt = now;
    customers[msg.sender][_courseId].userId = _userId;
    NewPayment(_courseId, _userId, msg.sender, msg.value);
  }

  function getRefund(uint _courseId) public {
    require(customers[msg.sender][_courseId].userId > 0);
    require(customers[msg.sender][_courseId].refunded == false);
    require(customers[msg.sender][_courseId].purchasedAt + (3 hours) > now);
    customers[msg.sender][_courseId].refunded = true;
    msg.sender.transfer(customers[msg.sender][_courseId].amount);
    RefundPayment(_courseId, customers[msg.sender][_courseId].userId, msg.sender);
  }
```

- **Corresponding ByteCode**



What is EVM?

- The Ethereum Virtual Machine (EVM) is a simple but powerful, Turing complete 256bit Virtual Machine that allows anyone to execute arbitrary EVM Byte Code. The EVM is part of the Ethereum Protocol and plays a crucial role in the consensus engine of the Ethereum system. It allows anyone to execute arbitrary code in a trust-less environment in which the outcome of an execution can be guaranteed and is fully deterministic.

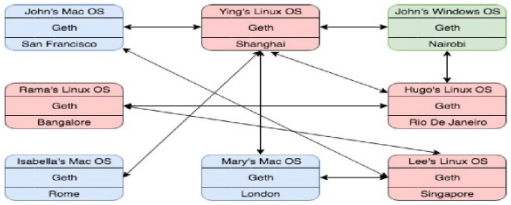
- When you install and start the geth, parity or any other client, the EVM is started and it starts syncing, validating and executing transactions.

3. Tools & Technologies

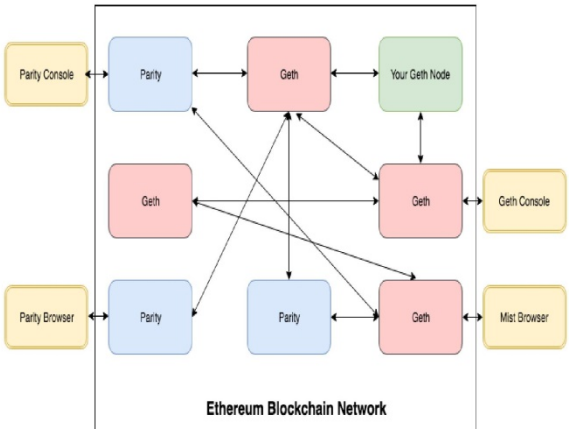
Geth/Parity Clients

- Let's see what tools are available to build applications on the Ethereum blockchain.

- **Geth**
- Geth is the official client software provided by the **Ethereum Foundation**. It is written in the Go programming language. When you start geth, it connects to other Ethereum clients (also called nodes) in the network and downloads a copy of the blockchain. It will constantly communicate with other nodes to keep it's **copy of the blockchain up to date**. It also has the ability to **mine blocks** and add transactions to the blockchain, **validate** the transactions in the block and also **execute the transactions**. It also acts as a server by exposing APIs you can interact with through RPC.
- It also comes with a **javascript client** (geth console) that can be used to connect to the blockchain.



- **Parity**
- Parity is another good implementation of the Ethereum protocol and is written in the **Rust programming language**. It is maintained by a company called Parity Inc.
- Any one can implement the client software and join the Ethereum network. There are clients written in C++ and Python and other languages. You can follow the specs in the yellow paper to implement your own client if you like!



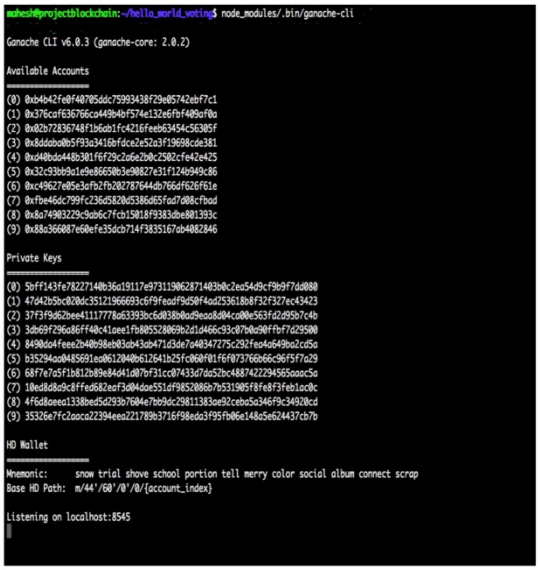
Web3JS/Truffle

- **Web3JS**
- This is a very popular javascript library that is used to interact with the Ethereum blockchain. You can use this javascript library in any frontend framework to build a **user facing decentralized application**. Here is a demo voting application we have created using web3js https://www.zastrin.com/simple-ethereum-voting-dapp.html

- **Truffle**
- Just like you have frameworks for web application development such as Ruby on Rails, Python/Django etc, Truffle is one of the most popular frameworks used to develop dapps. They **abstract away lot of the complexities of compiling and deploying** your contract on the blockchain. It also has an in-built **testing framework** you can use to test your contracts. You can find more details about the truffle framework here: http://truffleframework.com/. **All our courses are based on the Truffle framework**.

Ganache

- Using a client like geth or parity for development can slow you down because it takes 15 seconds to execute each transaction. In order to get around this issue, developers usually use an in-memory blockchain called **ganache** for development purposes. You can either install a command line version called ganache-cli or the GUI version. Another nice thing about ganache is that you get **10 test accounts loaded with 100 Ether for your testing**.

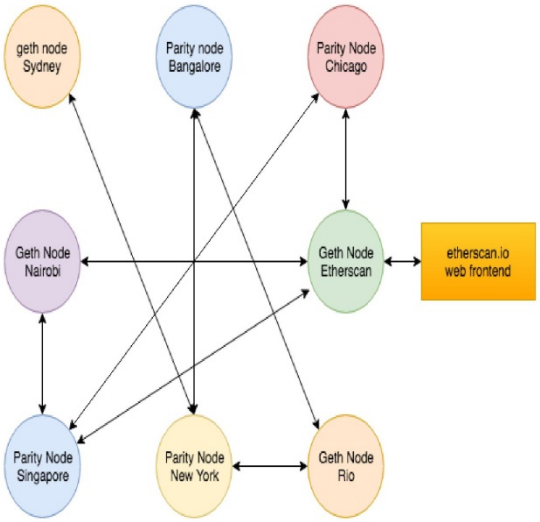


Metamask

- If you remember, we discussed about Wallets in the previous chapter. Metamask is one of the popular wallets everyone in the Ethereum community use. You can install it as a chrome plugin from their website. We created a video showing how to install metamask and also some of the concepts of deterministic wallets and seed phrases we discussed in the previous chapter.

Etherscan

- Etherscan is a handy frontend application offered as a free service by the company called Etherscan to explore the Ethereum blockchain. If you interact with the public Ethereum blockchain, all the addresses, transactions, block details etc can be viewed on that website. You can see on the right, the visualization of the Ethereum network and how Etherscan fits in the network.
-
- You can find links to Etherscan frontend for various public networks below:
- Mainnet: https://etherscan.io/
- Ropsten: https://ropsten.etherscan.io/
- Rinkeby: https://rinkeby.etherscan.io/
- Kovan: https://kovan.etherscan.io/



Remix

- Remix is a browser IDE you can use to code your smart contracts. Not only can you use it to as an editor but it can be used to compile and deploy your contracts to various networks and interact with them directly from the IDE. It has many features to select various compiler versions, debug your contracts and so on. You can access the IDE here: https://remix.ethereum.org.
- In our opinion, remix is good to quickly test out small contracts but we recommend using an editor like **Vim, Atom, Visual Studio or Sublime** for development and use truffle framework for compiling and deploying your contracts.

4. **Training**

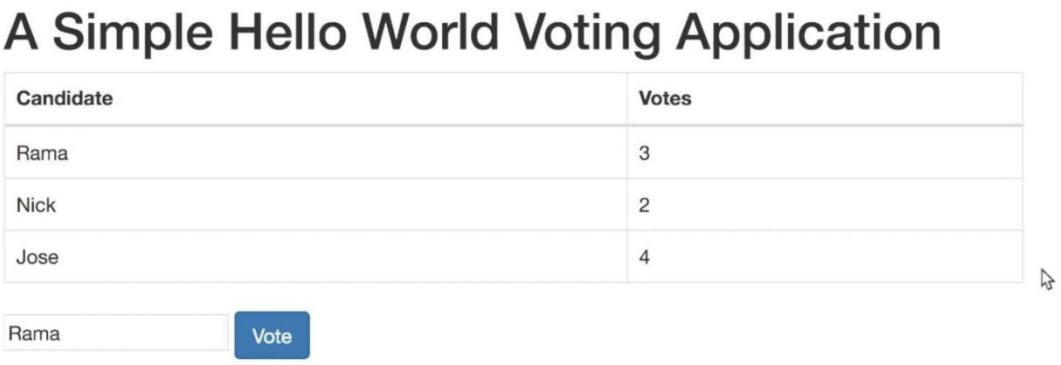
Windows installation instructions

- Windows
- Install Visual Studio Community Edition. If you choose a custom installation, the bare minimum items that need to be checked are all pertaining to Visual C++ (Current version is VS 2017)
- Install the Windows SDK for Windows
- Install Python 2.7 if not already installed, and make sure to add its install location to your PATH
- Install git if you don't have it and add it to your PATH
- Install OpenSSL from here. Make sure to choose the right package for your architecture, and only install the full package (not the light version). You must install OpenSSL at its recommended location — do not change the install path
- Download and install node v8.1.2. Version v6.11.0 is not recommended with VS2017
- Execute the command npm install ganache-cli web3@1.0.0-beta.37 solc@0.5.3
- To start ganache, run node_modules/.bin/ganache-cli

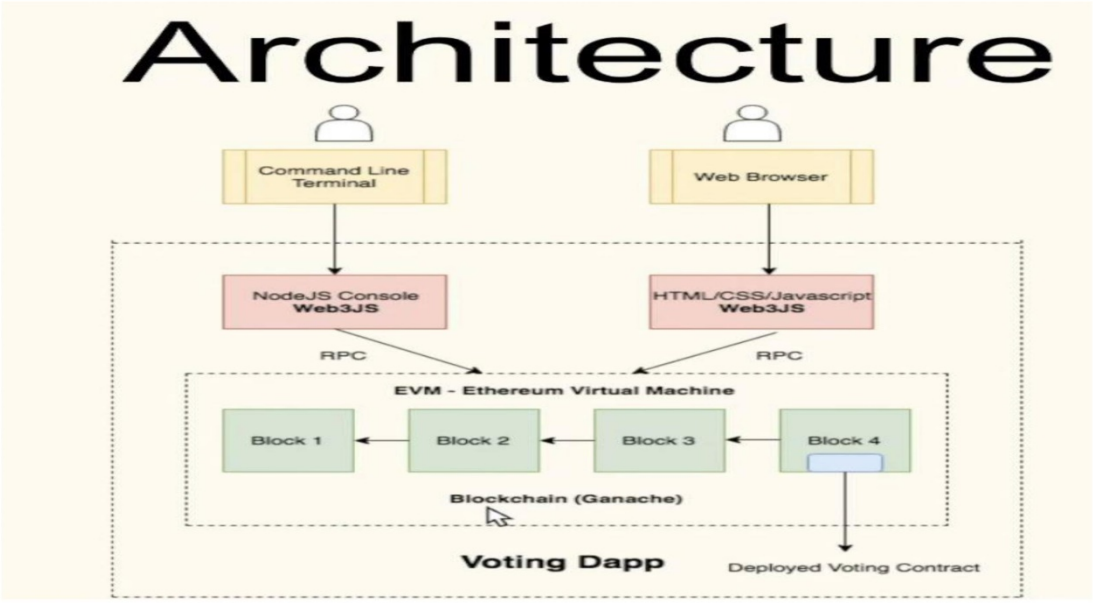
Basics of Solidity and Decentralized app

- 1. Learn to write Ethereum contract using Solidity programming language
- 2. Compile and deploy your contract to the blockchain
- 3. Interact with it through nodejs console and webpage

Project details



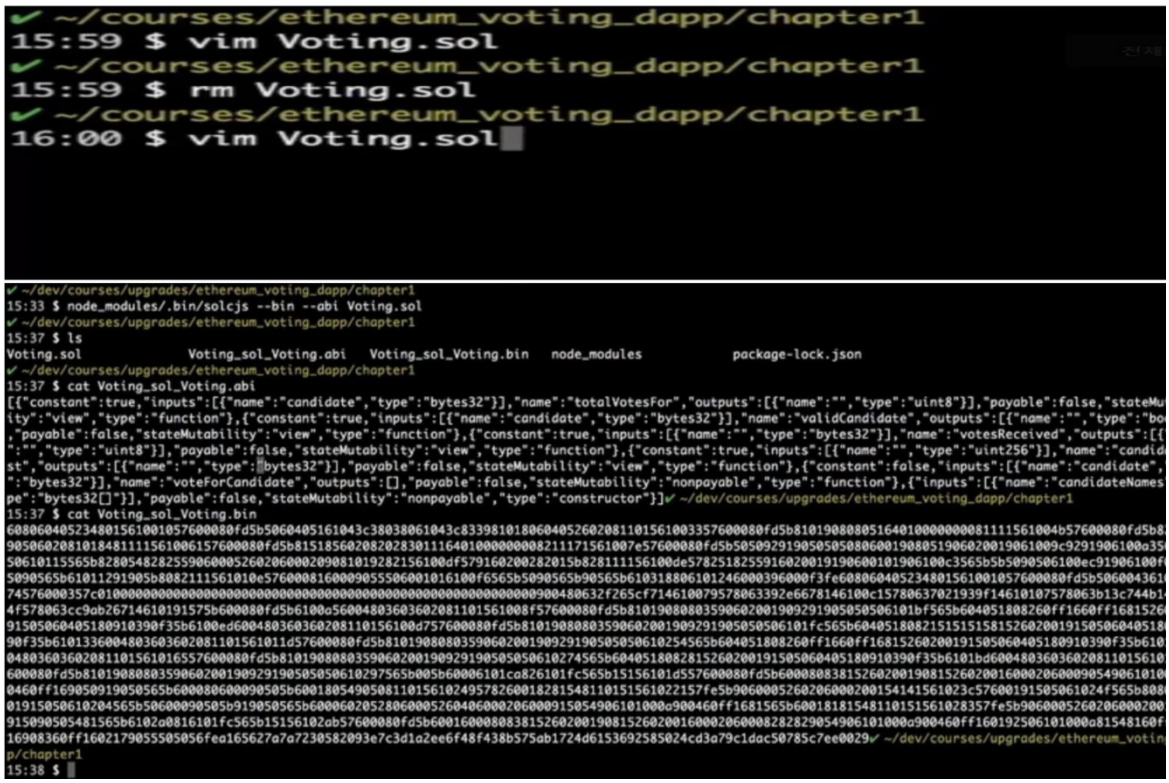
High level architecture



Learn to implement smart contract in Solidity

```
pragma solidity >=0.4.0 <0.6.0;
// This line says the code will compile with version greater than 0.4 and less than 0.6

contract Voting {
  // constructor to initialize candidates
  // vote for candidates
  // get count of votes for each candidates

  bytes32[] public candidateList;
  mapping (bytes32 => uint8) public votesReceived;

  constructor(bytes32[] memory candidateNames) public {
    // solidity requires that any
    candidateList = candidateNames;
  }

  function voteForCandidate(bytes32 candidate) public {
    require(validCandidate(candidate));
    votesReceived[candidate] += 1;
  }

  function totalVotesFor(bytes32 candidate) view public returns(uint8) {
    require(validCandidate(candidate));
    return votesReceived[candidate];
  }

  function validCandidate(bytes32 candidate) view public returns (bool) {
    for(uint i=0; i < candidateList.length; i++) {
      if (candidateList[i] == candidate) {
        return true;
      }
    }
    return false;
  }

}
```

Compile the smart contract



Deploy the smart contract to blockchain

```
Execute this in your node console:
> bytecode = fs.readFileSync('./Voting_sol_Voting.bin').toString()
> abi = JSON.parse(fs.readFileSync('./Voting_sol_Voting.abi').toString())
> Web3 = require('web3')
> web3 = new Web3("http://localhost:8545")
> deployedContract = new web3.eth.Contract(abi)
> web3.eth.getAccounts(console.log) <- Should output 10 accounts
> listOfCandidates = ['Rama', 'Nick', 'Jose']
> deployedContract.deploy({
data: bytecode,
arguments: [listOfCandidates.map(name => web3.utils.asciiToHex(name))]
}).send({
from: 'ENTER YOUR ACCOUNT ADDRESS',
gas: 1500000,
gasPrice: web3.utils.toWei('0.00003', 'ether')
}).then((newContractInstance) => {
deployedContract.options.address = newContractInstance.options.address
console.log(newContractInstance.options.address) // instance with the new contract address
});
```

Interact with solidity contract in nodejs console

```
In your node console:
> deployedContract.methods

> deployedContract.methods.totalVotesFor(web3.utils.asciiToHex('Rama')).call(console.log)

> deployedContract.methods.voteForCandidate(web3.utils.asciiToHex('Rama')).send({from: 'YOUR ACCOUNT ADDRESS'
```

Interact with solidity contract in the web browser

File: index.html

```
<!DOCTYPE html>
<html>
<head>
 <title>Hello World DApp</title>
 <link href='https://fonts.googleapis.com/css?family=Open Sans:400,700' rel='stylesheet' type='text/css
 <link href='https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css' rel='stylesheet' ty
</head>
<body class="container">
 <h1>A Simple Hello World Voting Application</h1>
 <div class="table-responsive">
  <table class="table table-bordered">
   <thead>
    <tr>
     <th>Candidate</th>
     <th>Votes</th>
    </tr>
   </thead>
   <tbody>
    <tr>
     <td>Rama</td>
     <td id="candidate-1"></td>
    </tr>
    <tr>
     <td>Nick</td>
     <td id="candidate-2"></td>
    </tr>
    <tr>
     <td>Jose</td>
     <td id="candidate-3"></td>
    </tr>
   </tbody>
  </table>
 </div>
 <input type="text" id="candidate" />
 <a href="#" onclick="voteForCandidate()" class="btn btn-primary">Vote</a>
</body>
```

File: index.js

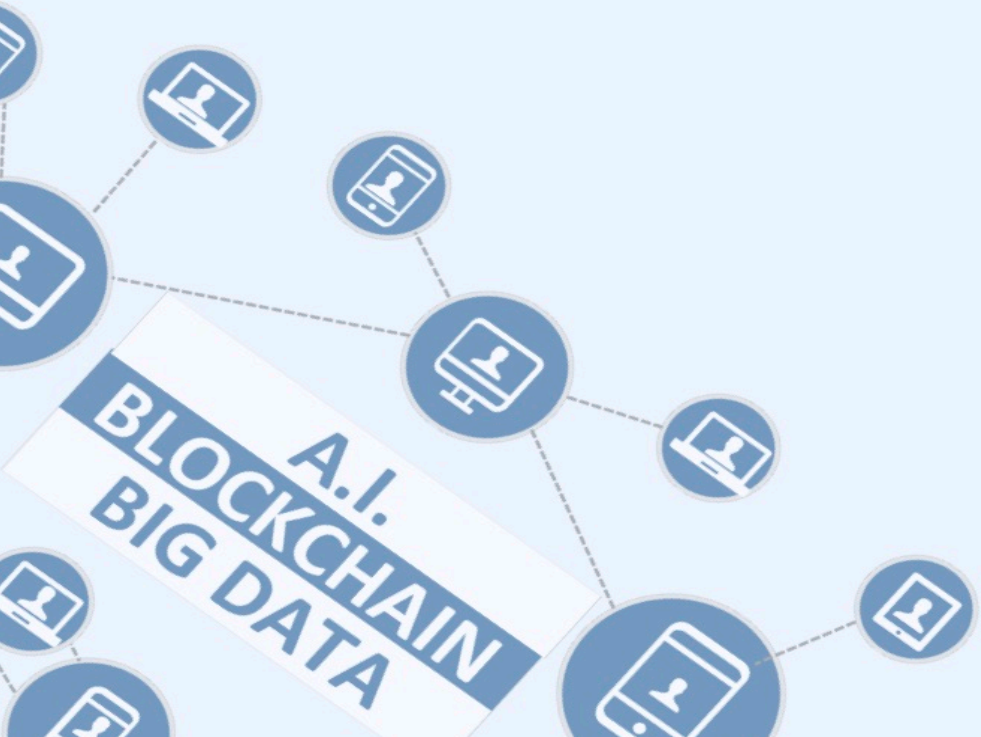
```
web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8545"))
var account;
web3.eth.getAccounts().then((f) => {
 account = f[0];
})

abi = JSON.parse('[{"constant":true,"inputs":[{"name":"candidate","type":"bytes32"}],"name":"totalVotes

contract = new web3.eth.Contract(abi);
contract.options.address = "0x71789831d83d4C8325b324eA9B5fFB27525480b5";
// update this contract address with your contract address

candidates = {"Rama": "candidate-1", "Nick": "candidate-2", "Jose": "candidate-3"}

function voteForCandidate(candidate) {
 candidateName = $("#candidate").val();
 console.log(candidateName);

 contract.methods.voteForCandidate(web3.utils.asciiToHex(candidateName)).send({from: account}).then((f
  let div_id = candidates[candidateName];
  contract.methods.totalVotesFor(web3.utils.asciiToHex(candidateName)).call().then((f) => {
   $("#" + div_id).html(f);
  })
 })
}

$(document).ready(function() {
 candidateNames = Object.keys(candidates);

 for(var i=0; i<candidateNames.length; i++) {
 let name = candidateNames[i];
```

6강

Ethereum Yellow Paper & Plasma MVP

정 순 형 대표

(주식회사 온더)



강의 동영상 URL

1 부: https://youtu.be/wcdaa5bIxbg

2 부: https://youtu.be/UcUAq--_2pE

3 부: https://youtu.be/q8xruxMo6F0

Understanding Ethereum Yellow Paper

(BYZANTIUM REVISION dbc2f9b)

kevin.j@onther.io
정순형

2019. 4. 11. at GIST

Onther Inc.

1. Introduction
    1. Driving Factors
    2. Previous Work
2. The Blockchain Paradigm
    1. Value
    2. Which History?
3. Conventions
4. Blocks, State and Transactions
    1. World State
    2. The Transaction
    3. The Block
        1. Transaction Receipt
        2. Holistic Validity
        3. Serialisation
        4. Block Header Validity

Onther Inc.

Onther Inc.

1.Introduction

1.1 Driving Factors

Onther Inc.

- The blockchain paradigm ; A Transactional singleton machine
- Ultimate Goal of Ethereum: Building Trustless State Transition System
  - facilitate transactions between consenting individuals who would otherwise have no means to trust one another
  - Incorruptability
  - Transparancy

1.2 Previous Work

Onther Inc.

- Dwork와 Naor [1992]
  - Proof of Work
  - They use this mechanism not for currency system, but for span deterrence mechanism
- Back [2002]: produces similar system
- Vish-numurthy[2003]
  - token was used to keep peer-to-peer file trading in check
  - Peer to Peer file Sharing
- Nakamoto[2008]
  - proof-of-work-secured value token
  - “Bitcoin” becomes first widely adopted global decentralised transaction ledger
- Other projects built on “Bitcoin” mechanisms
  - alt-coins: alteration of bitcoin protocols
  - Litecoin, Primecoin by Sprankel [2013])
  - Namecoin by Aron [2012] : Decentralized Name Registration Protocol
  - Mastercoin[2013] : built on Bitcoin
  - Ripple[2014] : “federated” system in sacrifice of decentralization
  - Szabo [1997] and Miller [1997] : Smart Contract concept but not implementation

Onther Inc.

2. The Blockchain Paradigm

Greek Letter

Α α	alpha, άλφα
Β β	beta, βήτα
Γ γ	gamma, γάμμα
Δ δ	delta, δέλτα
Ε ε	epsilon, έψιλον
Ζ ζ	zeta, ζήτα
Η η	eta, ήτα
Θ θ	theta, θήτα
Ι ι	iota, ιώτα
Κ κ	kappa, κάππα
Λ λ	la(m)bda λά(μ)βδα[note 3]
Μ μ	mu, μυ
Ν ν	nu, νυ
Ξ ξ	xi, ξι
Ο ο	omicron, όμικρον
Π π	pi, πι
Ρ ρ	rho, ρώ
Σ σ/ς, C c[note 4]	sigma, σίγμα
Τ τ	tau, ταυ
Υ υ	upsilon, ύψιλον
Φ φ	phi, φι
Χ χ	chi, χι
Ψ ψ	psi, ψι
Ω ω	omega, ωμέγα

Onther Inc.

7

- Ethereum
  - transaction-based state machine
  - from genesis to final state by incrementally execute transactions
  - state : account balances, reputations, trust arrangements, data

Onther Inc.

(1) $\boldsymbol{\sigma}_{t+1} \equiv \Upsilon(\boldsymbol{\sigma}_t, T)$ (2) $\boldsymbol{\sigma}_{t+1} \equiv \Pi(\boldsymbol{\sigma}_t, B)$

(3) $B \equiv (..., (T_0, T_1, ...))$ (4) $\Pi(\boldsymbol{\sigma}, B) \equiv \Omega(B, \Upsilon(\Upsilon(\boldsymbol{\sigma}, T_0), T_1)...)$

- (1) Next State = state transition function(current State, Transaction), Υ State Transition Function
- proof-of-work
  (2) Π Block level state-transition function
  (3) B Block : list of transactions, chained together using a cryptographic hash as a means of reference
  (4) Ω block-finalisation state transition function(reward function)

8

2.1 Value : incentivize computation

Onther Inc.

- Ethereum has an intrisic currency, Ether, known also as ETH
- smallest subdenomination of Ether is **Wei**
  - 1Ether = 10^{18} Wei
  - present work, balance, payment is **Wei**

Multiplier	Name
10^0	Wei
10^{12}	Szabo
10^{15}	Finney
10^{18}	Ether

9

2.2 Which History?

Onther Inc.

- If the system is decentralised, all parties have an opportunity to create a new block on some older pre-existing block
- resultant structure is necessarily a tree of blocks
- If there is ever a disagreement between nodes as to which root-to-leaf path down the block tree is the `best' blockchain, then a fork occurs.
  - multiple states of the system may coexist
  - simplified version of the GHOST protocol (kinds of PoW algorithms)

10

Onther Inc.

3. Conventions

Conventions(1/3)

Onther Inc.

- top-level state values : bold lowercase Greek letters
- μ: machine-state
- σ: world-state
- function: upper-case Greek letter ex) Υ Ethereum state transition function
- C: general cost function ex) C_{SSTORE} is SSTORE operation cost function
- KEC : Keccak-256 hash function
- KEC512 : Keccak 512 hash function
- Tuples: upper-case letter ex) T : Ethereum transaction
  - subscript is used to denote its type
  - ex) T_n: nonce of transaction

Conventions(2/3)

Onther Inc.

- Scalars and fixed-size byte sequences: normal lower-case letter
  - ex) n : transaction nonce
  - ex) δ (delta) : the number of items required on the stack for a given operation
- Arbitrary-length sequences are typically denoted as a bold lower-case letter
  - 예) **o** : sequence given as the output data of a message call
- important values: uppercase letter
- $\mathbb{N}$ scalars are non-negative integers
- $\mathbb{B}$: set of all byte-sequences (Appendix B에 정의됨)
- if series of sequence is limited,
  - $\mathbb{B}_{32}$: byte sequences of length 32
- $\mathbb{N}_{256}$: all non-negative integers smaller than 2^{256}
- [ ] index into and reference individual components or subsequences of sequences
  - 예) μ_s [0] : first item on the machine's stack
- Subsequences
  - 예) μ_m[0..31] : first 32 items of the machine's memory

13

Conventions(3/3)

Onther Inc.

- global state σ : a sequence of accounts and tuples
- square bracket: to reference an individual account
- modification
  - un-modfied `input' value : $\square$
  - modfied and utilisable value: $\square'$
  - intermediate values: $\square^*$, $\square^{**}$

(5) Last item in the given sequence

$$\ell(\mathbf{x}) \equiv \mathbf{x}[\|\mathbf{x}\| - 1]$$

14

Onther Inc.

4. Blocks, State and Transactions

15

4.1 World State(1/4)

Onther Inc.

- State : Mapping between Address and Account State σ
  - **Address** : 160-bit identiers (ex : 0xE05268C92117CBA26852A387F4657E9578304059)
  - Account State(encoded with RLP)
    - **Nonce**
      - number of transactions senf from this address
      - number of contract creation by this account
      - account of a in state of σ : $\sigma[a]_n$
    - **Balance** : scalar value equal to the number of Wei owned by this address : $\sigma[a]_b$
    - **Storage Root** : 256-bit hash of the root node of a Merkle Patricia tree that encodes the **storage contents(state variables)**
      - $\sigma[a]_s$
      - Related References
    - **Code Hash**
      - The hash of the EVM code of this account
      - immutable(unlike any other fields)
      - $\sigma[a]_c$,If code is b then, KEC(b) = $\sigma[a]_c$

16

4.1 World State(2/4)

Onther Inc.

$$(6) \qquad \mathtt{TRIE}\left(L_I^*(\boldsymbol{\sigma}[a]_s)\right) \equiv \boldsymbol{\sigma}[a]_s$$

** L_I^* **collapse function** for the set of key/value pairs in the trie

→ 스토리지 루트가 트라이 구조를 가짐

$$(7) \qquad L_I\left((k, v)\right) \equiv \left(\mathtt{KEC}(k), \mathtt{RLP}(v)\right)$$

where:

$$(8) \qquad k \in \mathbb{B}_{32} \quad \wedge \quad v \in \mathbb{N}$$

17

4.1 World State(3/4)

Onther Inc.

If account has no code hash, then this external account or non-contract account

$$\boldsymbol{\sigma}[a]_c = \mathtt{KEC}(())$$

world state collapse function => L_S

$$(9) \qquad L_S(\boldsymbol{\sigma}) \equiv \{p(a) : \boldsymbol{\sigma}[a] \neq \varnothing\}$$

where

$$(10) \quad p(a) \equiv \left(\mathtt{KEC}(a), \mathtt{RLP}\left((\boldsymbol{\sigma}[a]_n, \boldsymbol{\sigma}[a]_b, \boldsymbol{\sigma}[a]_s, \boldsymbol{\sigma}[a]_c)\right)\right)$$

validity function : trie function to provide a short identity (hash) of the world state

$$(11) \qquad \forall a : \boldsymbol{\sigma}[a] = \varnothing \ \vee \ (a \in \mathbb{B}_{20} \ \wedge \ v(\boldsymbol{\sigma}[a]))$$

where v is the account validity function:

$$(12) \qquad v(x) \equiv x_n \in \mathbb{P}_{256} \wedge x_b \in \mathbb{P}_{256} \wedge x_s \in \mathbb{B}_{32} \wedge x_c \in \mathbb{B}_{32}$$

18

4.1 World State(4/4)

Onther Inc.

Empty Account : when it has no code, zero nonce and zero balance

$$(13) \quad \text{EMPTY}(\sigma, a) \equiv \sigma[a]_{\text{c}} = \text{KEC}(()) \wedge \sigma[a]_{\text{n}} = 0 \wedge \sigma[a]_{\text{b}} = 0$$

DEAD Account : when its account state is non-existent or empty

$$(14) \quad \text{DEAD}(\sigma, a) \equiv \sigma[a] = \varnothing \vee \text{EMPTY}(\sigma, a)$$

What is DEAD but not EMPTY? → precompile contract

19

4.2 The Transaction(1/3)

Onther Inc.

- A single cryptographically-signed instruction

a. message call

- mainly, state manipulation

b. contract creation

- new accounts with associated code

20

4.3 The Transaction(2/3)

Onther Inc.

- Common transaction fields
  a. **nonce**: A scalar value equal to the number of transactions sent by the sender
  b. **gasPrice**: A scalar value equal to the number of Wei to be paid per unit of gas for all computation costs incurred as a result of the execution of this transaction
  c. **gasLimit**: A scalar value equal to the maximum amount of gas that should be used in executing this transaction, up-front cost
  d. **to**: The 160-bit address of the message call's recipient, or None(for contract creation)
  e. **value**: A scalar value equal to the number of Wei to be transferred to the message call's recipient or endowment(for contract creation)
  f. **v, r, s** : Values corresponding to the signature of the transaction and used to determine the sender of the transaction
  g. **init** (for contract creation): EVM-code
     - An unlimited size byte array specifying the EVM-code for the account initialisation procedure
     - EtherScan
  h. **data**(for message call): An unlimited size byte array specifying the input data of the message call

21

4.3 The Transaction(3/3)

Onther Inc.

Contract Creation vs Message Call

$$(15) \quad L_T(T) \equiv \begin{cases} (T_n, T_p, T_g, T_t, T_v, T_i, T_w, T_r, T_s) & \text{if } T_t = \varnothing \\ (T_n, T_p, T_g, T_t, T_v, T_d, T_w, T_r, T_s) & \text{otherwise} \end{cases}$$

Specs

$$(16) \quad \begin{array}{lllllll} T_n \in \mathbb{N}_{256} & \wedge & T_v \in \mathbb{N}_{256} & \wedge & T_p \in \mathbb{N}_{256} & \wedge \\ T_g \in \mathbb{N}_{256} & \wedge & T_w \in \mathbb{N}_5 & \wedge & T_r \in \mathbb{N}_{256} & \wedge \\ T_s \in \mathbb{N}_{256} & \wedge & T_d \in \mathbb{B} & \wedge & T_i \in \mathbb{B} & \end{array}$$

where

$$(17) \quad \mathbb{N}_n = \{P : P \in \mathbb{N} \wedge P < 2^n\}$$

22

4.4 The Block(1/6) $B \equiv (B_H, B_\mathbf{T}, B_\mathbf{U})$

- Block := (**Block header, Transactions, Ommer Block Headers**)

1. **parentHash(H_p)** : The Keccak 256-bit hash of the parent block's header
2. **ommersHash(H_o)** : The Keccak 256-bit hash of the ommers list portion of this block
3. **beneficiary(H_c)** : The 160-bit address to which all fees collected from the successful mining of this block be transferred
4. **stateRoot(H_r)** : The Keccak 256-bit hash of the root node of the state trie
5. **transactionRoot(H_t)** : The Keccak 256-bit hash of the root node of the trie structure populated with each transaction
6. **receiptsRoot(H_e)** : The Keccak 256-bit hash of the root node of the trie structure populated with the receipts of each transaction
7. **logsBloom(H_b)**: The Bloom lter composed from indexable information (logger address and log topics) contained in each log entry from the receipt of each transaction
8. **difficulty(H_d)**: A scalar value corresponding to the difficulty level of this block
9. **number(H_i)** : A scalar value equal to the number of ancestor blocks
10. **gasLimit(H_l)** : A scalar value equal to the current limit of gas expenditure per block
11. **gasUsed(H_g)** : A scalar value equal to the total gas used in transactions in this block
12. **timestamp(H_s)** : unix time
13. **extraData(H_x)** : An arbitrary byte array containing data relevant to this block
14. **mixHash(H_m)** : A 256-bit hash which, combined with the nonce, proves that a sucient amount of computation has been carried out on this block
15. **nonce(H_n)** : A 64-bit value which, combined with the mixhash, proves that a sucient amount of computation has been carried out on this block

Onther Inc.

23

4.4 The Block(2/6)

Onther Inc.

- Transaction Receipt : four items $R \equiv (R_\mathbf{u}, R_\mathbf{b}, R_\mathbf{l}, R_\mathbf{z})$

a. culmulative gas used after transaction : R_u

b. set of logs : R_l

c. bloom filter of those logs : R_b

d. status code : R_z

$$R_\mathbf{u} \in \mathbb{N} \quad \wedge \quad R_\mathbf{b} \in \mathbb{B}_{256}$$

$$O \equiv (O_\mathbf{a}, (O_{\mathbf{t}0}, O_{\mathbf{t}1}, ...), O_\mathbf{d}) \tag{24}$$

$$O_\mathbf{a} \in \mathbb{B}_{20} \quad \wedge \quad \forall_{x \in O_\mathbf{t}} : x \in \mathbb{B}_{32} \quad \wedge \quad O_\mathbf{d} \in \mathbb{B} \tag{25}$$

$$R_\mathbf{z} \in \mathbb{N}$$

24

4.4 The Block(3/6)

Onther Inc.

Goal of Light Client
- I want to know data but private

https://github.com/ethereum/wiki/wiki/Light-client-protocol

4.4 The Block(4/6)

Onther Inc.

Block's Validity

1. stateRoot
2. ommersHash
3. transactionsRoot
4. receiptsRoot
5. logsBloom

함수 정의는 다음 페이지 참조

$$
\begin{aligned}
H_r &\equiv \texttt{TRIE}(L_S(\Pi(\boldsymbol{\sigma}, B))) &\wedge\\
H_o &\equiv \texttt{KEC}(\texttt{RLP}(L^*_H(B_{\mathbf{U}}))) &\wedge\\
H_t &\equiv \texttt{TRIE}(\{\forall i < \|B_{\mathbf{T}}\|, i \in \mathbb{P} : p(i, L_T(B_{\mathbf{T}}[i]))\}) &\wedge\\
H_e &\equiv \texttt{TRIE}(\{\forall i < \|B_{\mathbf{R}}\|, i \in \mathbb{P} : p(i, L_R(B_{\mathbf{R}}[i]))\}) &\wedge\\
H_b &\equiv \bigvee_{\mathbf{r} \in B_{\mathbf{R}}} (\mathbf{r}_b)
\end{aligned}
$$

stateRoot : state trie's root node of KEC hash
ommersHash : ommer block's RLP-encoded KEC hash
transactionsRoot : Transactions Trie's root node of KEC hash
receiptsRoot : Receipts Trie's root node of KEC hash
logsBloom :Transaction Receipts of log entries' Bloom Filters

4.4 The Block(5/6)

Onther Inc.

$$(34)\quad L_H(H) \equiv (\ H_\mathrm{p}, H_\mathrm{o}, H_\mathrm{c}, H_\mathrm{r}, H_\mathrm{t}, H_\mathrm{e}, H_\mathrm{b}, H_\mathrm{d}, H_\mathrm{i}, H_\mathrm{l}, H_\mathrm{g}, H_\mathrm{s}, H_\mathrm{x}, H_\mathrm{m}, H_\mathrm{n}\ )$$

$$(35)\quad L_B(B) \equiv (L_H(B_H), L_T^*(B_\mathbf{T}), L_H^*(B_\mathbf{U}))$$

With L_T^* and L_H^* being element-wise sequence transformations, thus:

$$(36)\quad f^*((x_0, x_1, ...)) \equiv (f(x_0), f(x_1), ...) \quad \text{for any function } f$$

The component types are defined thus:

$$(37)\quad \begin{array}{lllllll} H_\mathrm{p} \in \mathbb{B}_{32} & \wedge & H_\mathrm{o} \in \mathbb{B}_{32} & \wedge & H_\mathrm{c} \in \mathbb{B}_{20} & \wedge \\ H_\mathrm{r} \in \mathbb{B}_{32} & \wedge & H_\mathrm{t} \in \mathbb{B}_{32} & \wedge & H_\mathrm{e} \in \mathbb{B}_{32} & \wedge \\ H_\mathrm{b} \in \mathbb{B}_{256} & \wedge & H_\mathrm{d} \in \mathbb{N} & \wedge & H_\mathrm{i} \in \mathbb{N} & \wedge \\ H_\mathrm{l} \in \mathbb{N} & \wedge & H_\mathrm{g} \in \mathbb{N} & \wedge & H_\mathrm{s} \in \mathbb{N}_{256} & \wedge \\ H_\mathrm{x} \in \mathbb{B} & \wedge & H_\mathrm{m} \in \mathbb{B}_{32} & \wedge & H_\mathrm{n} \in \mathbb{B}_8 & \end{array}$$

27

$R \equiv (R_\sigma, R_u, R_p, R_t)$

4.4 The Block(6/6)

Onther Inc.

- Block Header Validity
  a. pow
  b. difficulty
  c. gas used
  d. gas limit
  e. time stamp
  f. block number
  g. extraData size

$$(50)\quad V(H) \equiv n \leqslant \frac{2^{256}}{H_d} \wedge m = H_m \quad \wedge$$
$$(51)\quad H_d = D(H) \quad \wedge$$
$$(52)\quad H_g \leq H_l \quad \wedge$$
$$(53)\quad H_l < P(H)_{H_l} + \left\lfloor \frac{P(H)_{H_l}}{1024} \right\rfloor \quad \wedge$$
$$(54)\quad H_l > P(H)_{H_l} - \left\lfloor \frac{P(H)_{H_l}}{1024} \right\rfloor \quad \wedge$$
$$(55)\quad H_l \geqslant 125000 \quad \wedge$$
$$(56)\quad H_s > P(H)_{H_s} \quad \wedge$$
$$(57)\quad H_i = P(H)_{H_i} + 1 \quad \wedge$$
$$(58)\quad \|H_x\| \leq 32$$

$$(39)\quad D(H) \equiv \begin{cases} D_0 & \text{if } H_i = 0 \\ \max(D_0, P(H)_{H_d} + x \times \varsigma_1 + \epsilon) & \text{if } H_i < N_H \\ \max(D_0, P(H)_{H_d} + x \times \varsigma_2 + \epsilon) & \text{otherwise} \end{cases}$$

28

Onther Inc.

5. Gas and Payment

5. Gas and Payment

Onther Inc.

- Network abuse / Turing Completeness
  - In order to avoid issues of network abuse and to sidestep the inevitable questions stemming from Turing completeness, all programmable computation in Ethereum is subject to fees

- Fee Schedule
  - **fee schedule** is specied in units of gas (Appendix G, fee schedule)
  - **gasLimit**: transaction has a specic amount of gas associated with it
  - **gasPrice**: willingness to paying price per gas
    - TX fee (= gasLimit * gasPrice)
  - miners choose to which transaction is included first → data censorship
  - trade-off to make between lowering the gas price and maximising the chance that their transaction will be mined in a timely manner

Onther Inc.

6. Transaction Execution

6. Transaction Execution

Onther Inc.

1. Υ : state transition function $\sigma' = \Upsilon(\sigma, T)$

2. initial tests of intrinsic validity

   a. The transaction is well-formed **RLP**, with no additional trailing bytes
   b. the transaction **signature** is valid
   c. the transaction **nonce** is valid (equivalent to the sender account's current nonce
   d. the **gas limit** is no smaller than the intrinsic gas, g0, used by the transaction
   e. the sender account **balance** contains at least the cost, v0, required in up-front payment.

6.1 Substate

Onther Inc.

1. Transaction Substate
   a. accrue certain information that is acted upon immediately
   b. following the transaction

$$A \equiv (A_{\mathbf{s}}, A_{\mathbf{l}}, A_{\mathbf{t}}, A_{\mathbf{r}})$$

$A_{\mathbf{s}}$, the self-destruct set
$A_{\mathbf{l}}$ is the log series
$A_{\mathbf{t}}$ is the set of touched accounts.
$A_{\mathbf{r}}$, the refund balance.

   c. $A^0 \equiv (\varnothing, (), \varnothing, 0)$: no self-destructs, no logs, no touched and a zero refund balance

   d. negative gas
   opcode list

33

6.2 Execution(1/3)

Onther Inc.

- intrinsic gas g_0
  - the amount of gas this transaction requires to be paid prior to execution

$$g_0 \equiv \sum_{i \in T_{\mathbf{i}}, T_{\mathbf{d}}} \begin{cases} G_{\text{txdatazero}} & \text{if} \quad i = 0 \\ G_{\text{txdatanonzero}} & \text{otherwise} \end{cases} + \begin{cases} G_{\text{txcreate}} & \text{if} \quad T_{\mathbf{t}} = \varnothing \\ 0 & \text{otherwise} \end{cases} + G_{\text{transaction}}$$

G_{txcreate}	32000	Paid by all contract-creating transactions after the *Homestead transition*.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.

34

6.2 Execution(2/3)

Onther Inc.

- up-front cost v_0

$$v_0 \equiv T_g T_p + T_v$$

- validity
  - sender address exists
  - sender's account state exists
  - TX nonce and sender's nonce are equal
  - intrinsic gas is less then TX's gas limit
  - sender can pay up-front cost
  - TX's gas limit is less than gas limit - cumulative gas used

$$\begin{aligned} S(T) &\neq \varnothing \quad \wedge \\ \boldsymbol{\sigma}[S(T)] &\neq \varnothing \quad \wedge \\ T_n &= \boldsymbol{\sigma}[S(T)]_n \quad \wedge \\ g_0 &\leqslant T_g \quad \wedge \\ v_0 &\leqslant \boldsymbol{\sigma}[S(T)]_b \quad \wedge \\ T_g &\leqslant B_{Hl} - \ell(B_{\mathbf{R}})_u \end{aligned}$$

35

6.2 Execution(3/3)

Onther Inc.

- state transition at the beggining of transaction
  - Check point state $\boldsymbol{\sigma}_0$
  - $$\begin{aligned} (65) \quad \boldsymbol{\sigma}_0 &\equiv \boldsymbol{\sigma} \quad \text{except:} \\ (66) \quad \boldsymbol{\sigma}_0[S(T)]_b &\equiv \boldsymbol{\sigma}[S(T)]_b - T_g T_p \\ (67) \quad \boldsymbol{\sigma}_0[S(T)]_n &\equiv \boldsymbol{\sigma}[S(T)]_n + 1 \end{aligned}$$
  - gasLimit * gasPrice is substracted from balance
  - sender's nonce increases by 1

36

Onther Inc.

7. Contract Creation

7 Contract Creation(1/5)

Onther Inc.

- Λ를 Contract Creation Function 이라고 할때

$$(\sigma', g', A) \equiv \Lambda(\sigma, s, o, g, p, v, \mathbf{i}, e)$$

- **σ**′ : new state
- g' : remaining gas
- *A* : substate

- **σ** : state
- s : sender
- o : original transactor
- g : available gas
- p : gas price
- v : endowment(ehter)
- i : bytecode array initialisation EVM code
- e : the present depth of the message call / contract creation stack

7 Contract Creation(2/5) + Constantinople(19/2/22)

Onther Inc.

- Contract Address

(80) $a \equiv \mathcal{B}_{96..255}\Big(\mathtt{KEC}\Big(\mathtt{RLP}\big(\ (s, \boldsymbol{\sigma}[s]_n - 1)\ \big)\Big)\Big)$

- Contract Creation

(81) $\boldsymbol{\sigma}^* \equiv \boldsymbol{\sigma}$ except:

(82) $\boldsymbol{\sigma}^*[a] \equiv (0, v + v', \mathtt{TRIE}(\varnothing), \mathtt{KEC}(()))$

(83) $\boldsymbol{\sigma}^*[s]_b \equiv \boldsymbol{\sigma}[s]_b - v$

(84) $v' \equiv \begin{cases} 0 & \text{if } \boldsymbol{\sigma}[a] = \varnothing \\ \boldsymbol{\sigma}[a]_b & \text{otherwise} \end{cases}$

- mutated state
- (82) mutate state(contract address) = (contract account state(nonce, balance, storage, codehash))
- v' : pre-existing value
- (83) substracted from sender's balance by value (sendTransaction)

39

7 Contract Creation(3/5)

Onther Inc.

- Contract Creation Execution

(85) $(\boldsymbol{\sigma}^{**}, g^{**}, A, \mathbf{o}) \equiv \Xi(\boldsymbol{\sigma}^*, g, I)$

- the code execution function Ξ

(86) $I_a \equiv a$

(87) $I_o \equiv o$

(88) $I_p \equiv p$

(89) $I_{\mathbf{d}} \equiv ()$

(90) $I_s \equiv s$

(91) $I_v \equiv v$

(92) $I_{\mathbf{b}} \equiv \mathbf{i}$

(93) $I_e \equiv e$

(94) $c \equiv G_{codedeposit} \times |\mathbf{o}|$

I is parameters

40

7 Contract Creation(4/5)

Onther Inc.

- Contract Creation Execution

$$c \equiv G_{codedeposit} \times |\mathbf{o}|$$

- if initialisation is success then,
- (94) c : code deposit cost calculate
- |o| : body code

$$(95) \qquad g' \equiv \begin{cases} 0 & \text{if } F \\ g^{**} - c & \text{otherwise} \end{cases}$$

$$(96) \qquad \sigma' \equiv \begin{cases} \sigma & \text{if } F \\ \sigma^{**} \quad \text{except:} & \\ \quad \sigma'[a]_c = \text{KEC}(\mathbf{o}) & \text{otherwise} \end{cases}$$

where

$$(97) \qquad F \equiv \left(\sigma^{**} = \varnothing \ \vee \ g^{**} < c \ \vee \ |\mathbf{o}| > 24576\right)$$

41

7 Contract Creation(5/5)

Onther Inc.

- 7.1 Subtleties

- Note that while the initialisation code is executing, the newly created address exists but with no intrinsic body code.
- Thus any message call received by it during this time causes no code to be executed. If the initialisation execution ends with a SELFDESTRUCT instruction, the matter is moot since the account will be deleted before the transaction is completed.
- For a normal STOP code, or if the code returned is otherwise empty, then the state is left with a zombie account, and any remaining balance will be locked into the account forever.

42

Onther Inc.

8. Message Call

8 Message Call(1/3)

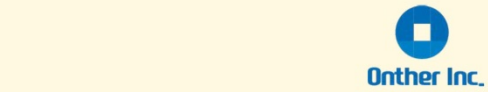
Onther Inc.

- $$(98) \quad (\boldsymbol{\sigma}', g', A, \mathbf{o}) \equiv \Theta(\boldsymbol{\sigma}, s, o, r, c, g, p, v, \tilde{v}, \mathbf{d}, e)$$

  $$(99) \quad \boldsymbol{\sigma}_1[r]_b \equiv \boldsymbol{\sigma}[r]_b + v \quad \wedge \quad \boldsymbol{\sigma}_1[s]_b \equiv \boldsymbol{\sigma}[s]_b - v$$

- **σ**′ : new state
- g' : remaining gas
- A : substate
- **σ** : state
- s : sender
- o : original transactor
- g : available gas
- p : gas price
- v : value (ether)
- v : delegate call instruction value
- e : the present depth of the message call / contract creation stack
- d : arbitrary length byte array

8 Message Call(2/3)



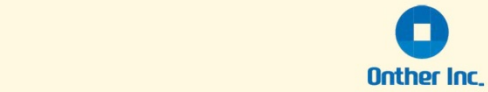
- (100) $\boldsymbol{\sigma}_1 \equiv \boldsymbol{\sigma}'_1 \quad \text{except:}$

  (101) $\boldsymbol{\sigma}_1[s]_b \equiv \boldsymbol{\sigma}'_1[s]_b - v$

  (102) $\text{and} \quad \boldsymbol{\sigma}'_1 \equiv \boldsymbol{\sigma} \quad \text{except:}$

  (103) $$\begin{cases} \boldsymbol{\sigma}'_1[r] \equiv (v, 0, \texttt{KEC}(()), \texttt{TRIE}(\varnothing)) & \text{if} \quad \boldsymbol{\sigma}[r] = \varnothing \\ \boldsymbol{\sigma}'_1[r]_b \equiv \boldsymbol{\sigma}[r]_b + v & \text{otherwise} \end{cases}$$

8 Message Call(3/3)



- (104) $$\boldsymbol{\sigma}' \equiv \begin{cases} \boldsymbol{\sigma} & \text{if} \quad \boldsymbol{\sigma}^{**} = \varnothing \\ \boldsymbol{\sigma}^{**} & \text{otherwise} \end{cases}$$

  (105) $$g' \equiv \begin{cases} 0 & \text{if} \quad \boldsymbol{\sigma}^{**} = \varnothing \\ g^{**} & \text{otherwise} \end{cases}$$

  (106) $$(\boldsymbol{\sigma}^{**}, g^{**}, A, \mathbf{o}) \equiv \begin{cases} \Xi_{\texttt{ECREC}}(\boldsymbol{\sigma}_1, g, I) & \text{if} \quad r = 1 \\ \Xi_{\texttt{SHA256}}(\boldsymbol{\sigma}_1, g, I) & \text{if} \quad r = 2 \\ \Xi_{\texttt{RIP160}}(\boldsymbol{\sigma}_1, g, I) & \text{if} \quad r = 3 \\ \Xi_{\texttt{ID}}(\boldsymbol{\sigma}_1, g, I) & \text{if} \quad r = 4 \\ \Xi(\boldsymbol{\sigma}_1, g, I) & \text{otherwise} \end{cases}$$

  (107) $I_a \equiv r$

  (108) $I_o \equiv o$

  (109) $I_p \equiv p$

  (110) $I_{\mathbf{d}} \equiv \mathbf{d}$

  (111) $I_s \equiv s$

  (112) $I_v \equiv \tilde{v}$

  (113) $I_e \equiv e$

  (114) $\text{Let } \texttt{KEC}(I_{\mathbf{b}}) = \boldsymbol{\sigma}[c]_c$

Onther Inc.

9. Execution Model

47

9.1 Basies

Onther Inc.

1. Execution model
   a. The execution model species how the system state is altered given a series of bytecode instructions and a small tuple of environmental data
2. EVM(Ethereum Virtual Machine)
   a. simple stack-based architecture
   b. The word size of the machine (and thus size of stack items) is 256-bit
      i. to facilitate the Keccak-256 hash scheme and elliptic-curve computations
3. Memory model
   a. word-addressed **byte array**
   b. stack has a maximum size of 1024
   c. volatile
4. Storage model
   a. word-addressable **word array**
   b. non-volatile

48

9.2 Fees Overview

- Fees are charged under three distinct circumstances
  - fee intrinsic to the computation of the operation
  - gas may be deducted in order to form the payment for a subordinate message call or contract creation(CREATE, CALL and CALLCODE)
  - increase in the usage of the memory
- Memory usage
  - memory usage payable is proportional to smallest multiple of 32 bytes that are required such that all memory indices (whether for read or write) are included in the range
  - referencing an area of memory at least 32 bytes greater than any previously indexed memory will certainly result in an additional memory usage fee
- Storage fee
  - the execution fee for an operation that clears an entry in the storage is not only waived, a qualied refund is given
  - storage location costs substantially more than normal usage

49

9.3 Execution Environment(1/2)

- I_a, the address of the account which owns the code that is executing.
- I_o, the sender address of the transaction that originated this execution.
- I_p, the price of gas in the transaction that originated this execution.
- I_d, the byte array that is the input data to this execution; if the execution agent is a transaction, this would be the transaction data.
- I_s, the address of the account which caused the code to be executing; if the execution agent is a transaction, this would be the transaction sender.

50

9.3 Execution Environment(1/2)

- I_{v}, the value, in Wei, passed to this account as part of the same procedure as execution; if the execution agent is a transaction, this would be the transaction value.
- I_{b}, the byte array that is the machine code to be executed.
- I_{H}, the block header of the present block.
- I_{e}, the depth of the present message-call or contract-creation (i.e. the number of CALLs or CREATEs being executed at present).
- I_{w}, the permission to make modifications to the state.

51

9.3 Execution Environment(2/2)

(115) $(\boldsymbol{\sigma}', g', A, \mathbf{o}) \equiv \Xi(\boldsymbol{\sigma}, g, I)$

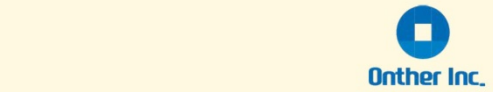
- Ξ : $\boldsymbol{\sigma}', g', A, \mathbf{o}$ exection function
- $\boldsymbol{\sigma}'$: the resultant state
- g' : the remaining gas
- $\mathbf{o}$: the resultant output
- A : transaction substate

(116) $A \equiv (\mathbf{s}, \mathbf{l}, r)$

- A : the accrued substate
- $\mathbf{l}$: the log series
- $\mathbf{s}$: the suicides set
- r : the refunds

52

9.4 Execution Overview



X is thus cycled (recursively here, but implementations are generally expected to use a simple iterative loop) until either

Z becomes true indicating that the present state is exceptional and that the machine must be halted and any changes discarded or until

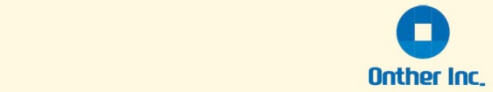
H becomes a series (rather than the empty set) indicating that the machine has reached a controlled halt.

(131)

$$X((\sigma, \mu, A, I)) \equiv \begin{cases} (\varnothing, \mu, A^0, I, \varnothing) & \text{if } Z(\sigma, \mu, I) \\ (\varnothing, \mu', A^0, I, \mathbf{o}) & \text{if } w = \text{REVERT} \\ O(\sigma, \mu, A, I) \cdot \mathbf{o} & \text{if } \mathbf{o} \neq \varnothing \\ X(O(\sigma, \mu, A, I)) & \text{otherwise} \end{cases}$$

53

9.4.1 Machine State



g: gas available

pc : program counter (pc $\in \mathbb{P}_{256}$) ,

m: memory contents (The memory contents μm are a series of zeroes of size 2^{256})

i : active number of words in memory (counting continuously from position 0)

s : stack contents

The machine state $\boldsymbol{\mu}$

$$(g, pc, \mathbf{m}, i, \mathbf{s})$$

54

9.4.2 Exceptional Halting

1. insufficient gas
1. if the instruction is invalid (and therefore its δ subscript is undefined)
1. if there are insufficient stack items
1. if a JUMP/JUMPI destination is invalid
1. new stack size would be larger than 1024

$$Z(\boldsymbol{\sigma}, \boldsymbol{\mu}, I) \equiv \begin{array}{l} \boldsymbol{\mu}_g < C(\boldsymbol{\sigma}, \boldsymbol{\mu}, I) \quad \vee \\ \delta_w = \varnothing \quad \vee \\ \|\boldsymbol{\mu}_{\mathbf{s}}\| < \delta_w \quad \vee \\ (w \in \{\text{JUMP}, \text{JUMPI}\} \quad \wedge \\ \quad \boldsymbol{\mu}_{\mathbf{s}}[0] \notin D(I_{\mathbf{b}})) \quad \vee \\ \|\boldsymbol{\mu}_{\mathbf{s}}\| - \delta_w + \alpha_w > 1024 \end{array}$$

$$w \equiv \begin{cases} I_{\mathbf{b}}[\boldsymbol{\mu}_{pc}] & \text{if} \quad \boldsymbol{\mu}_{pc} < \|I_{\mathbf{b}}\| \\ \text{STOP} & \text{otherwise} \end{cases}$$

55

9.4.3 Jump Destination Validity

All jump positions must be on valid instruction boundaries

rather than sitting in the data portion of PUSH operations
must appear within the explicitly defined portion of the code (rather than in the implicitly defined STOP operations that trail it)

(130)

$$D_J(\mathbf{c}, i) \equiv \begin{cases} \{\} & \text{if} \quad i \geqslant |\mathbf{c}| \\ \{i\} \cup D_J(\mathbf{c}, N(i, \mathbf{c}[i])) & \text{if} \quad \mathbf{c}[i] = \text{JUMPDEST} \\ D_J(\mathbf{c}, N(i, \mathbf{c}[i])) & \text{otherwise} \end{cases}$$

(131)

$$N(i, w) \equiv \begin{cases} i + w - \text{PUSH1} + 2 & \text{if} \quad w \in [\text{PUSH1}, \text{PUSH32}] \\ i + 1 & \text{otherwise} \end{cases}$$

56

9.4.3 Normal Halting

(132)

$$H(\mu, I) \equiv \begin{cases} H_{\text{RETURN}}(\mu) & \text{if} \quad w = \text{RETURN} \\ () & \text{if} \quad w \in \{\text{STOP}, \text{SELFDESTRUCT}\} \\ \varnothing & \text{otherwise} \end{cases}$$

0xf3 RETURN 2 0 Halt execution returning output data.
$H_{\text{RETURN}}(\mu) \equiv \mu_{\mathbf{m}}[\mu_{\mathbf{s}}[0] \dots (\mu_{\mathbf{s}}[0] + \mu_{\mathbf{s}}[1] - 1)]$
This has the effect of halting the execution at this point with output defined.
See section 9.
$\mu'_i \equiv M(\mu_i, \mu_{\mathbf{s}}[0], \mu_{\mathbf{s}}[1])$

$$M(s, f, l) \equiv \begin{cases} s & \text{if} \quad l = 0 \\ \max(s, \lceil (f + l) \div 32 \rceil) & \text{otherwise} \end{cases}$$

57

RLP

RLP(Recursive Length Prefix)

: to encode arbitrarily nested arrays of binary data

https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP

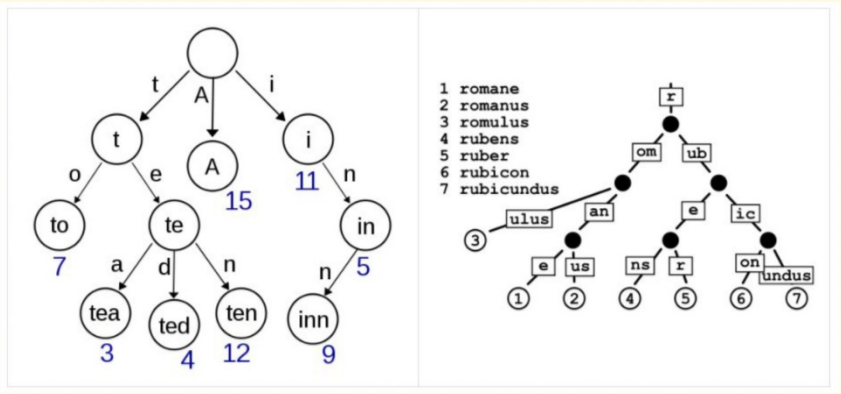
58

Radix Tree

Onther Inc.

Modified Merkle Patricia Tree(trie)

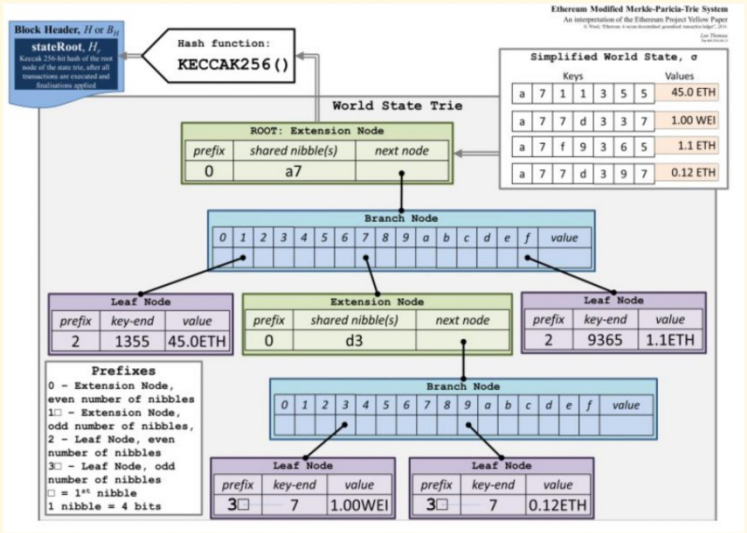
radix trie



Modified Merkle Patricia Tree

Onther Inc.

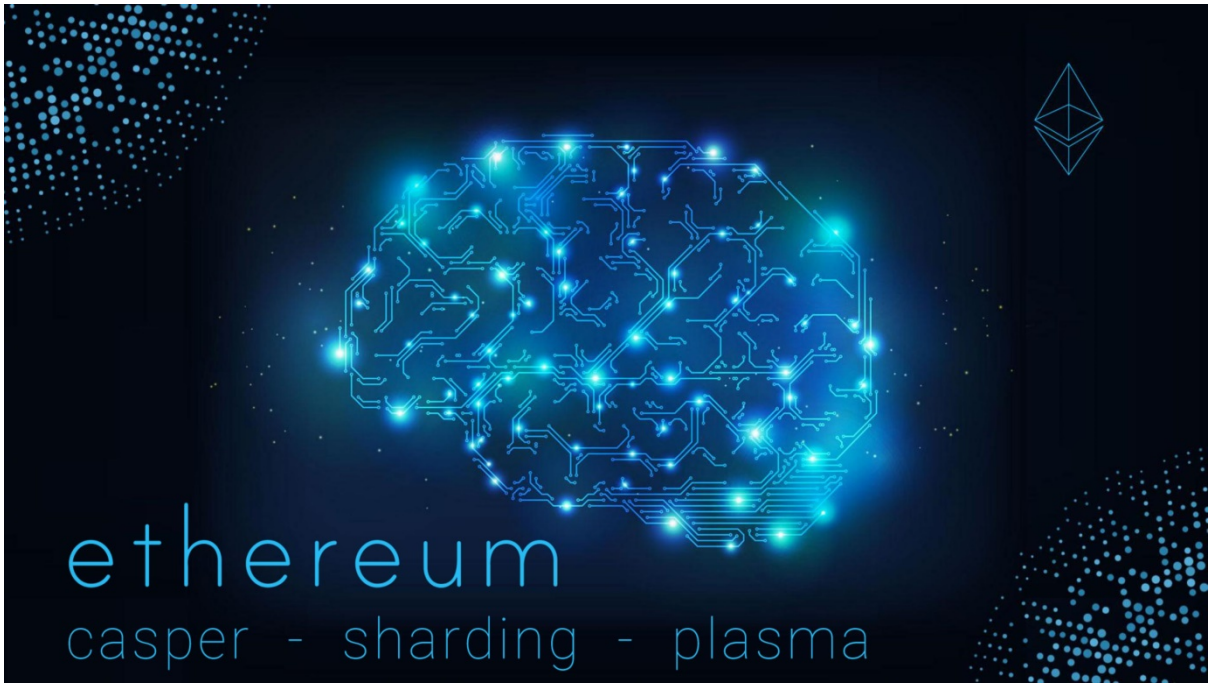
Modified Merkle Patricia Tree(trie) - Merkle Patricia Tree(trie)



Precompiled Contracts

- https://github.com/ethereum/pyethereum/blob/develop/ethereum/specials.py

61



2.

Minimal Viable Plasma

A Plasma chain for scalable payments

Plasma Provides: Massive Scaling

- Massively scalable
  - MVP can scale to more than 1,000 TPS
  - Later versions TPS in the millions

Plasma Provides: Asset Security

- Strong security guarantees
  - Tokens cannot be double spent
  - Tokens cannot be withheld
  - Tokens can always be redeemed on the root chain

Plasma Exits

- The key mechanism which secures Plasma chains
- Coded in a smart contract on the root chain (mainnet Ethereum)
- MVP is designed for token transfers
- Can be designed for ERC 721, general state transitions, etc
  - Check out the Plasma Implementers Call!

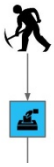
Plasma Implementers Call #3: ❤️ & Updates
3.9K views • 6 days ago

Plasma Implementers Call #2: Q&A
2.5K views • 2 weeks ago

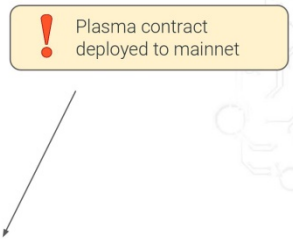
Plasma Implementers Call #1
9.1K views • 1 month ago

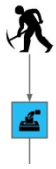
Minimal Viable Plasma

Plasma operator

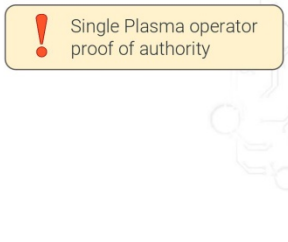


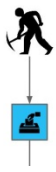
Minimal Viable Plasma





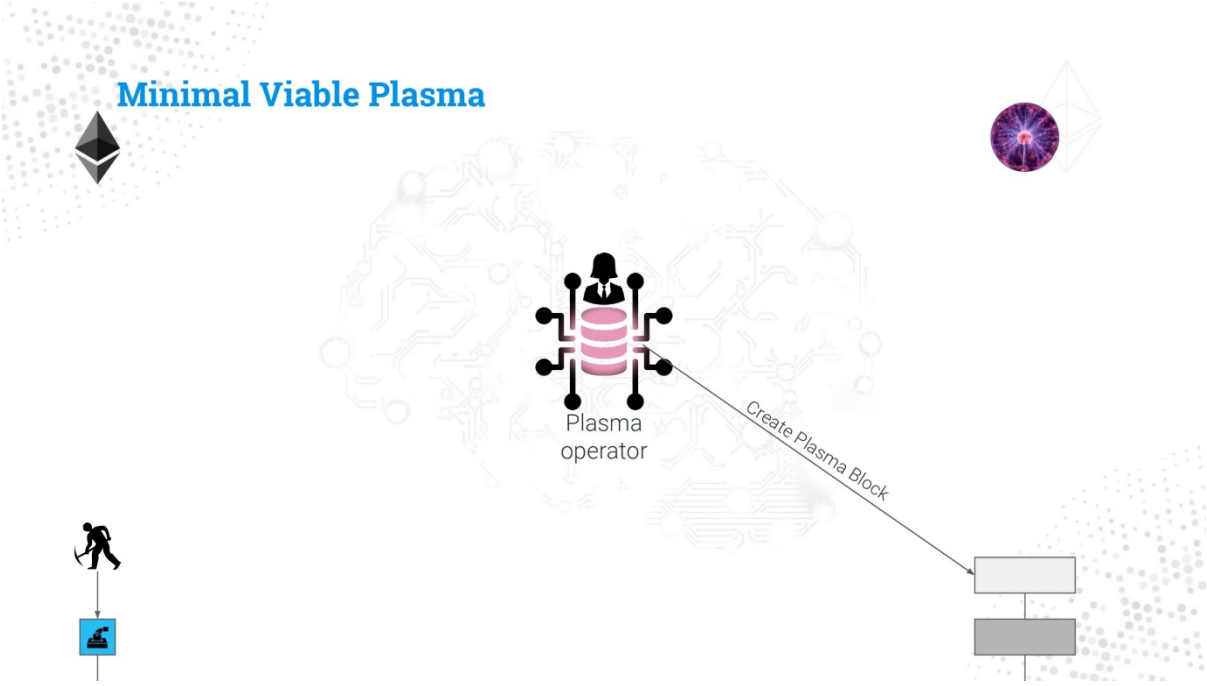
Minimal Viable Plasma

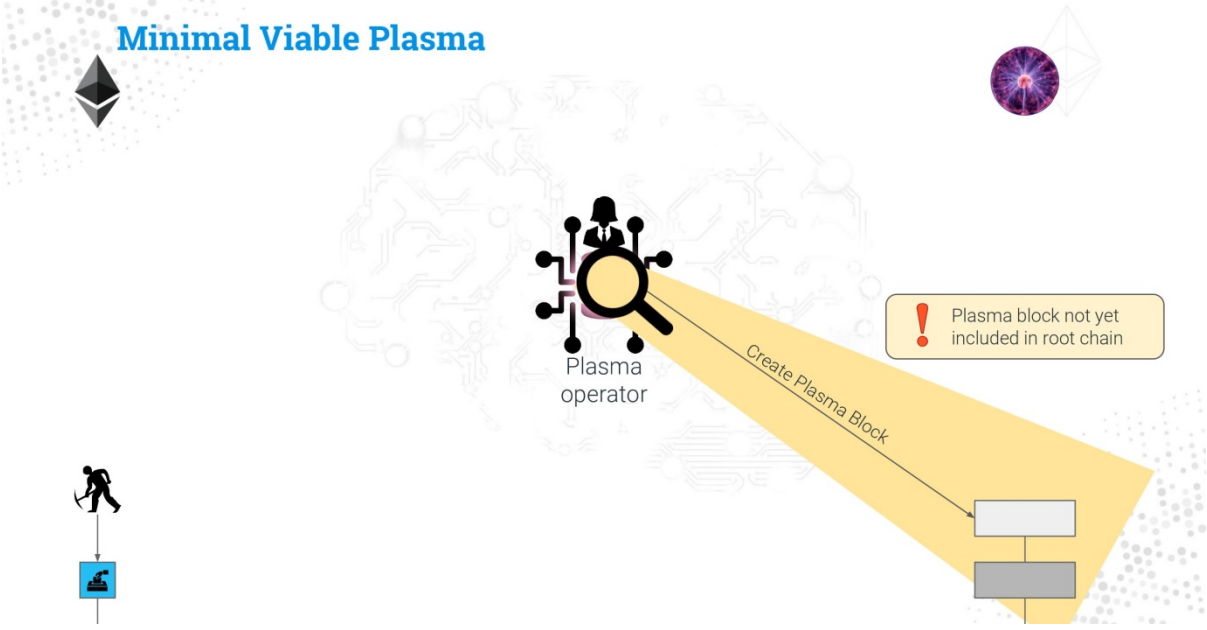




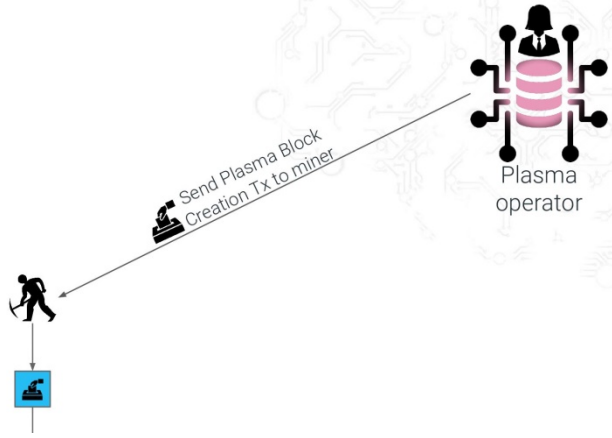
1. Operator creates a block
2. A new user, Sam, deposits ETH into the Plasma chain
3. Sam sends a bunch of transactions to Alice
4. Sam attempts to exit with all 5 PETH but fails
5. Operator creates an invalid block and all users exit

1. Operator creates a block
2. Sam deposits ETH into the Plasma chain
    a. New Plasma block is created
    b. Sam begins watching Plasma chain for misbehavior
3. Sam sends a bunch of transactions to Alice
    a. Sam confirms the transactions
4. Sam attempts to exit with all 5 PETH
    a. Alice stops the exit with challenge
5. Operator creates an invalid block
    a. Sam and Alice exit before operator steals their ETH

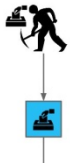

Minimal Viable Plasma
Plasma
operator
Create Plasma Block


Minimal Viable Plasma
Plasma
operator
Create Plasma Block
Plasma block not yet
included in root chain

Minimal Viable Plasma



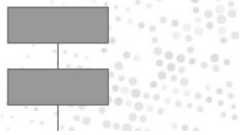
Minimal Viable Plasma



Minimal Viable Plasma

Plasma
operator

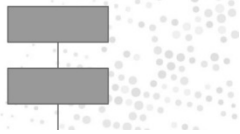
Plasma block
"confirmed"



Minimal Viable Plasma

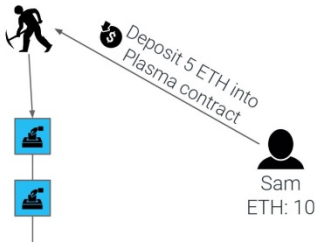
Plasma
operator

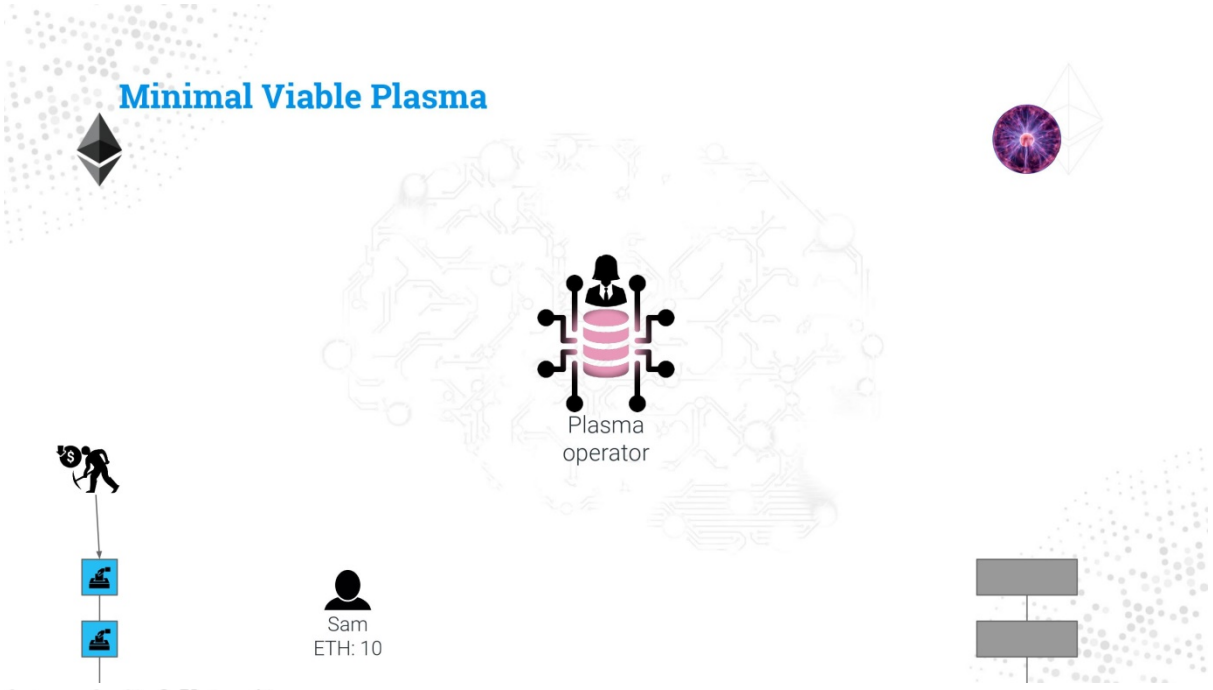
Sam
ETH: 10

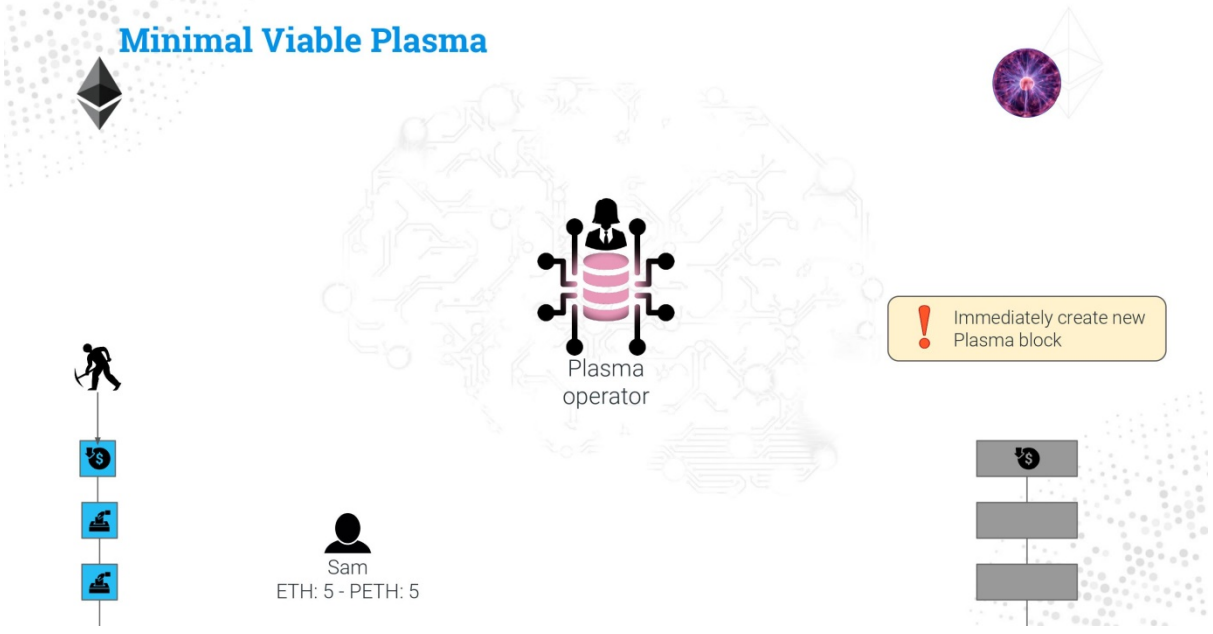


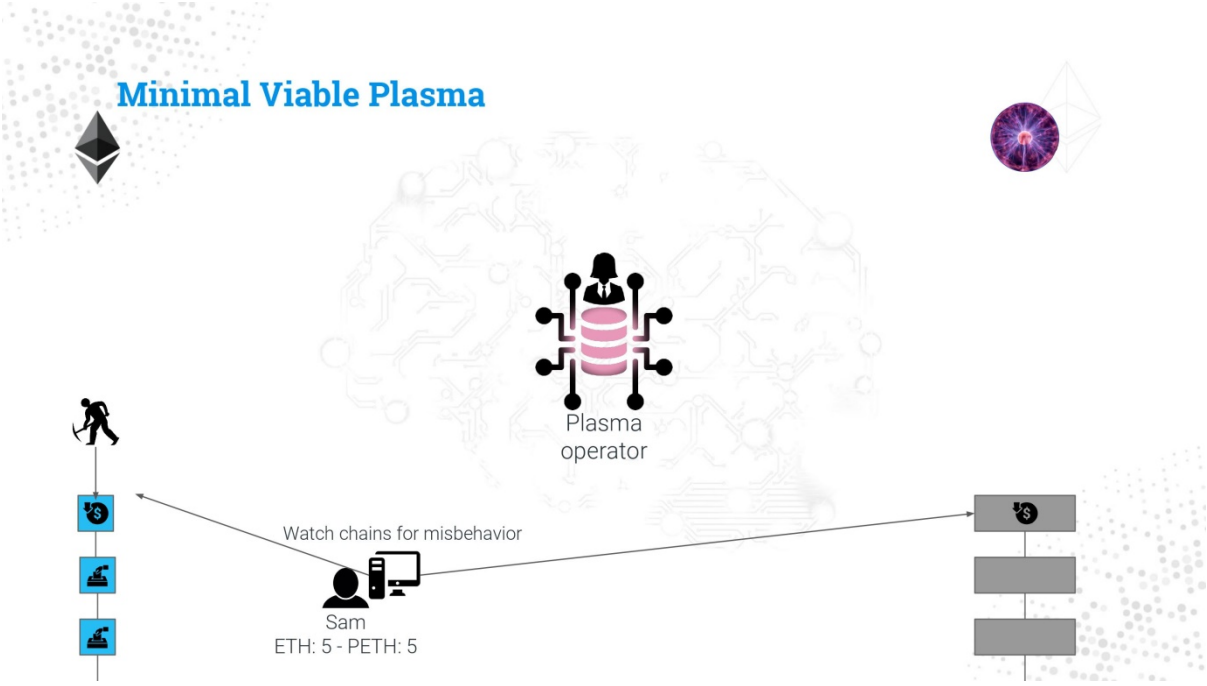
1. Operator creates a block
2. Sam deposits ETH into the Plasma chain
   a. New Plasma block is created
   b. Sam begins watching Plasma chain for misbehavior
3. Sam sends a bunch of transactions to Alice
   a. Sam confirms the transactions
4. Sam attempts to exit with all 5 PETH
   a. Alice stops the exit with challenge
5. Operator creates an invalid block
   a. Sam and Alice exit before operator steals their ETH

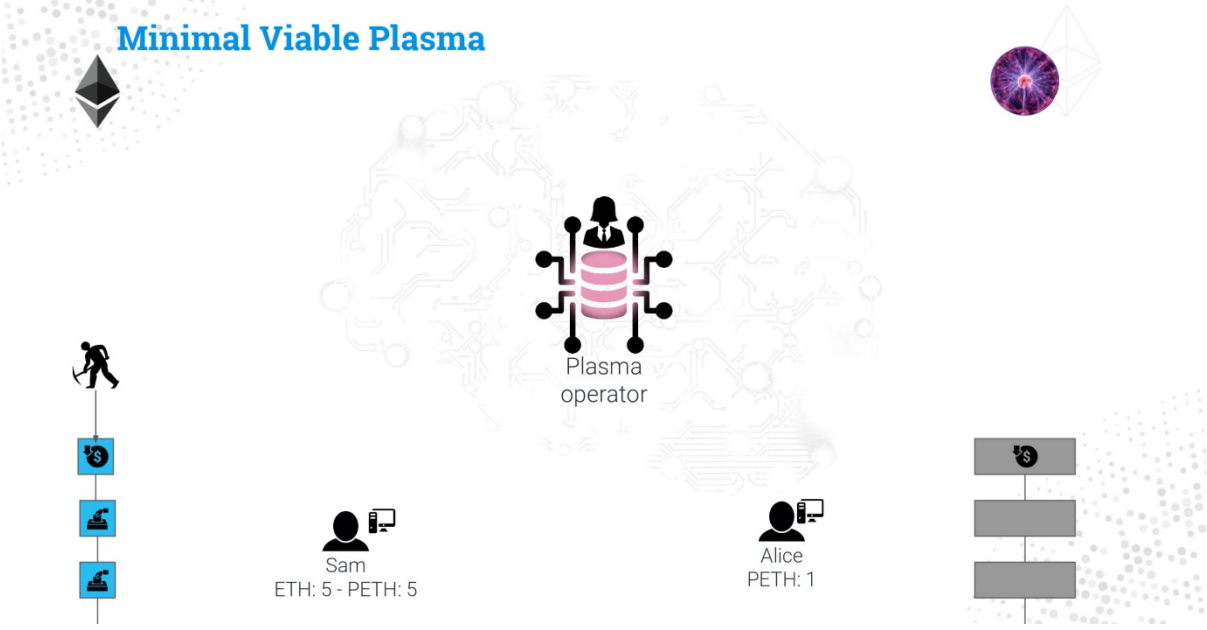
Minimal Viable Plasma



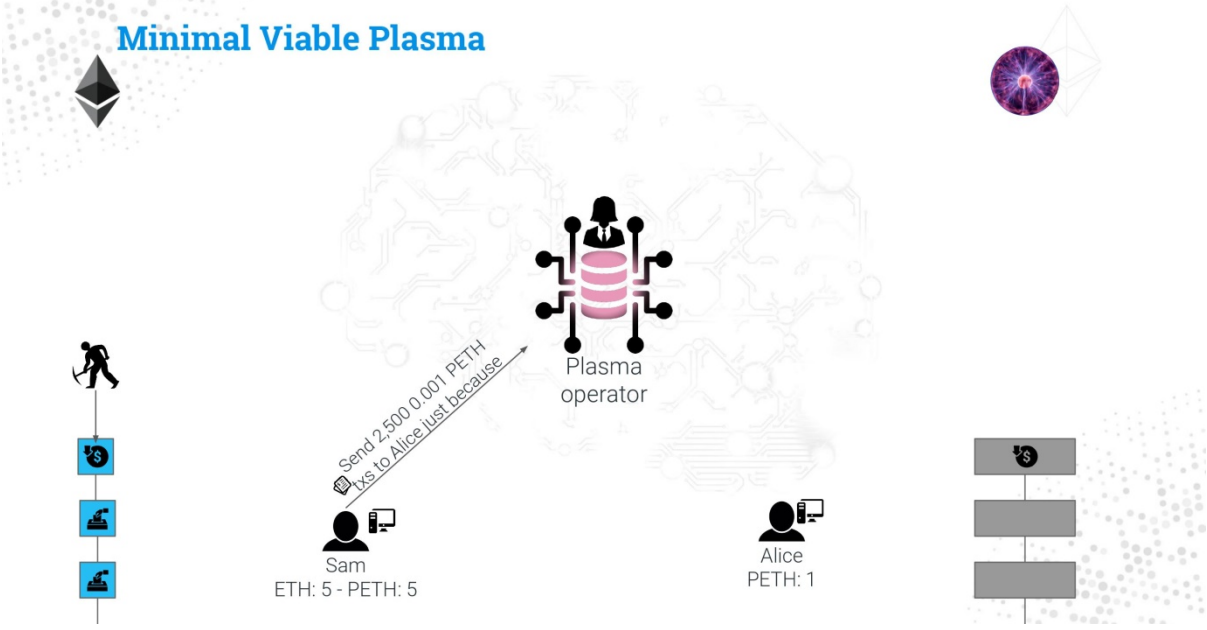

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 10

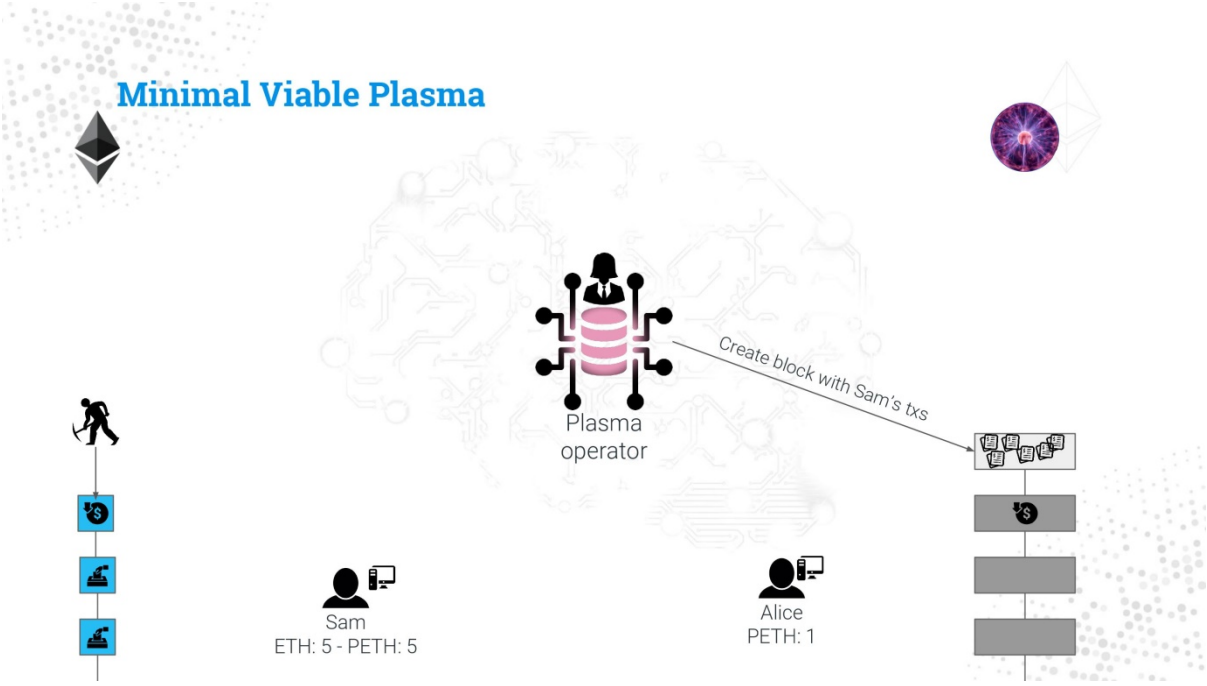

Minimal Viable Plasma
Plasma
operator
Immediately create new
Plasma block
Sam
ETH: 5 - PETH: 5

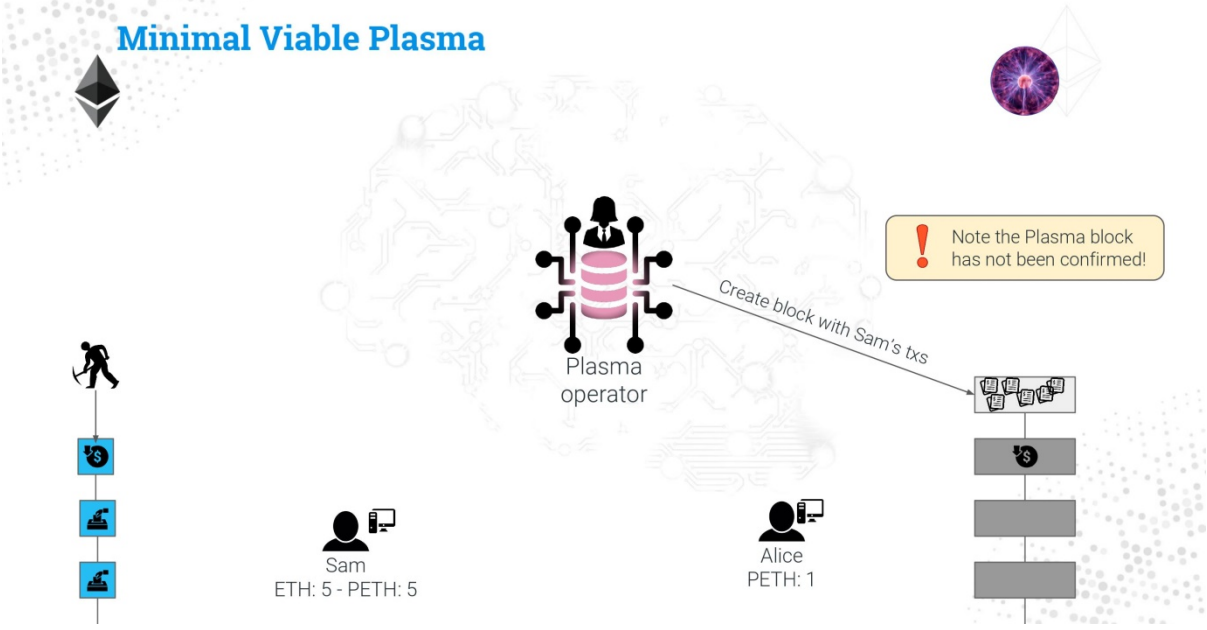

Minimal Viable Plasma
Plasma
operator
Watch chains for misbehavior
Sam
ETH: 5 - PETH: 5

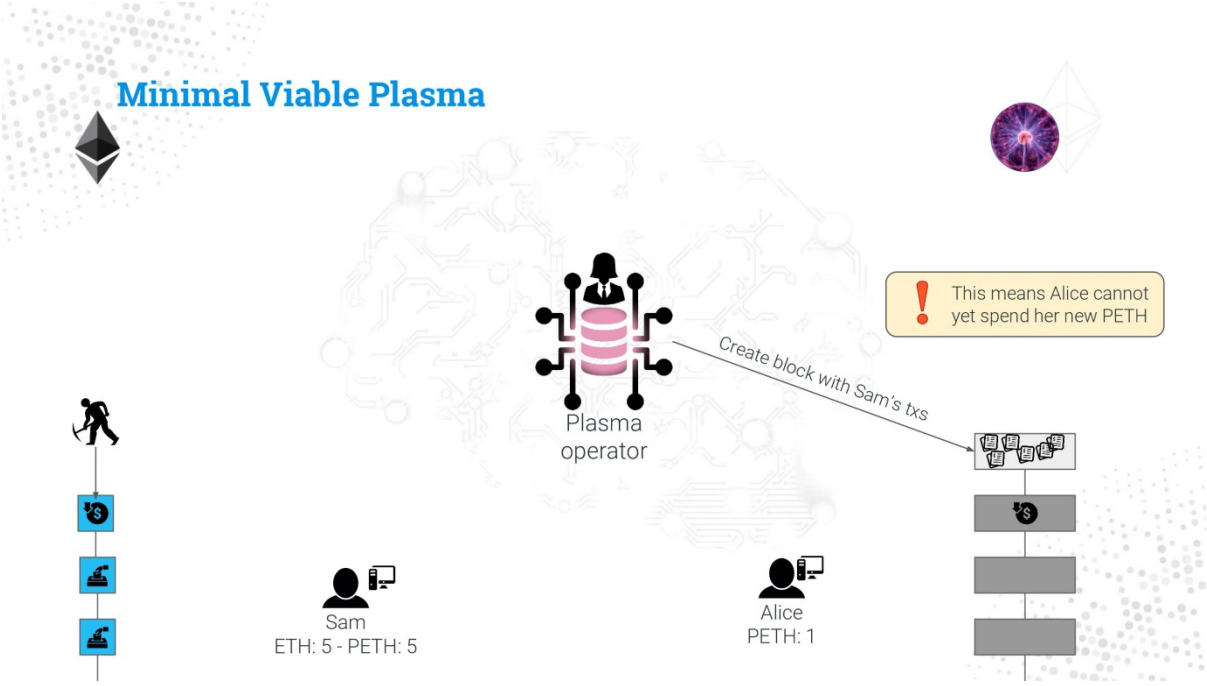

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1

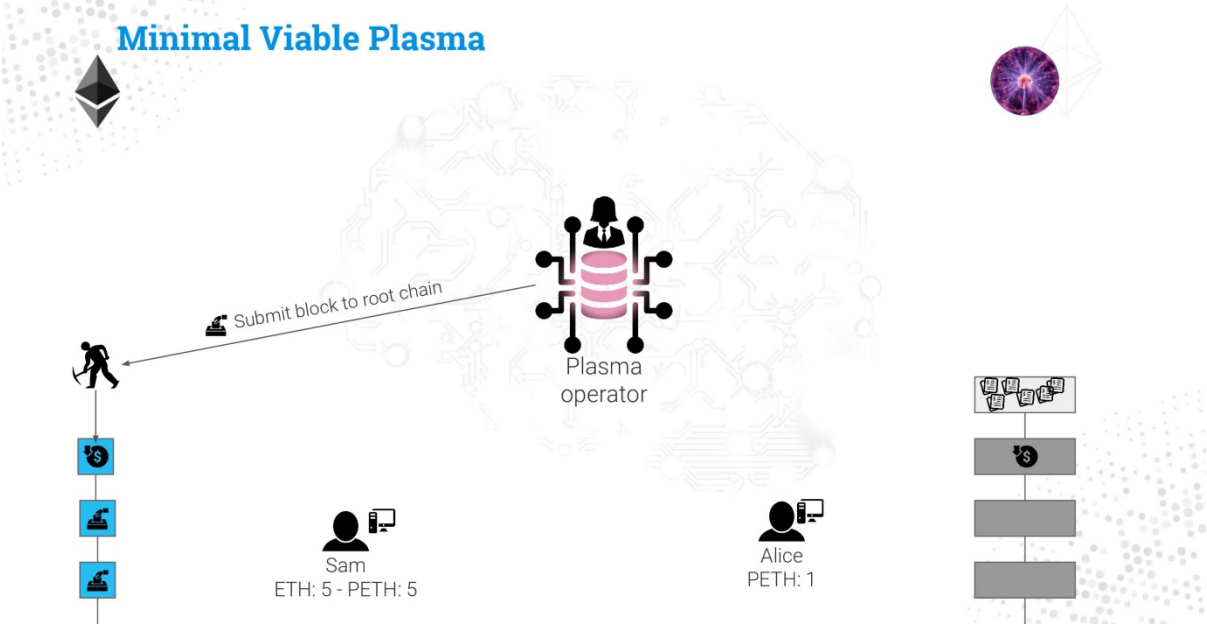
1. Operator creates a block
2. Sam deposits ETH into the Plasma chain
   a. New Plasma block is created
   b. Sam begins watching Plasma chain for misbehavior
3. Sam sends a bunch of transactions to Alice
   a. Sam confirms the transactions
4. Sam attempts to exit with all 5 PETH
   a. Alice stops the exit with challenge
5. Operator creates an invalid block
   a. Sam and Alice exit before operator steals their ETH

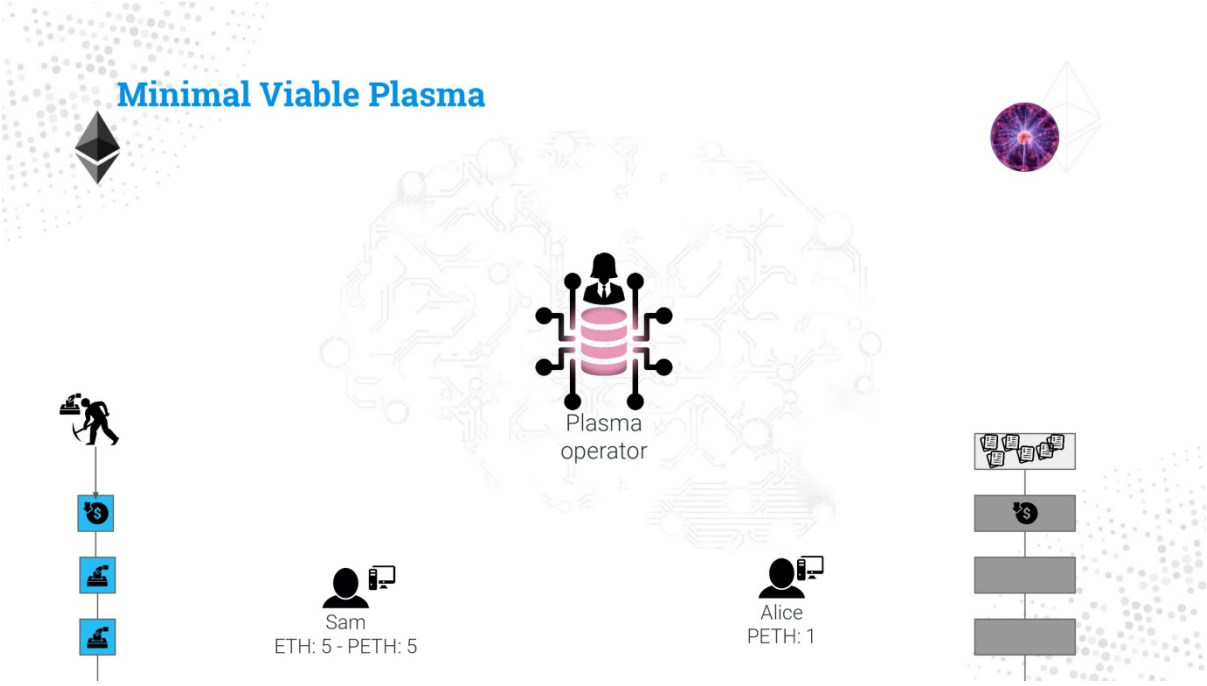


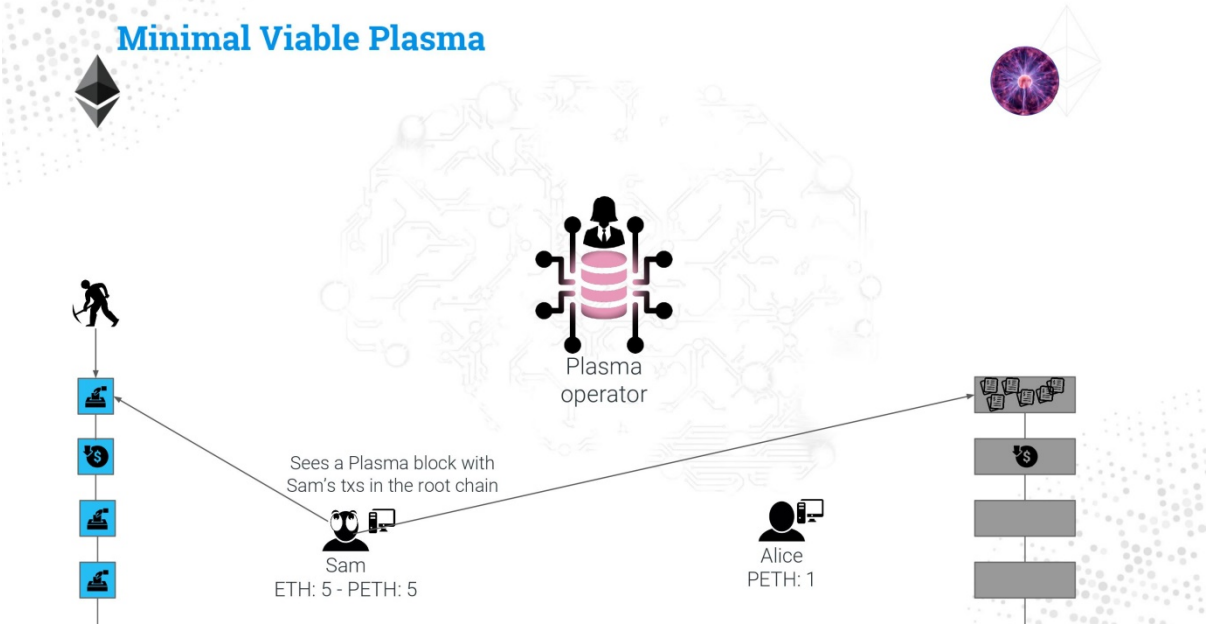

Minimal Viable Plasma
Plasma
operator
Create block with Sam's txs
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1


Minimal Viable Plasma
Note the Plasma block
has not been confirmed!
Plasma
operator
Create block with Sam's txs
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1

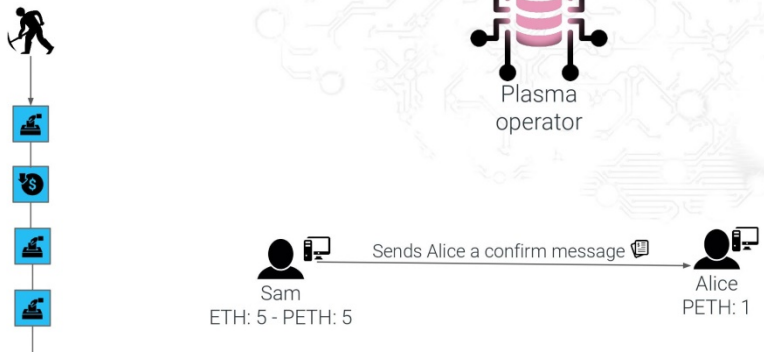

Minimal Viable Plasma
This means Alice cannot yet spend her new PETH
Create block with Sam's txs
Plasma operator
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1


Minimal Viable Plasma
Submit block to root chain
Plasma operator
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1

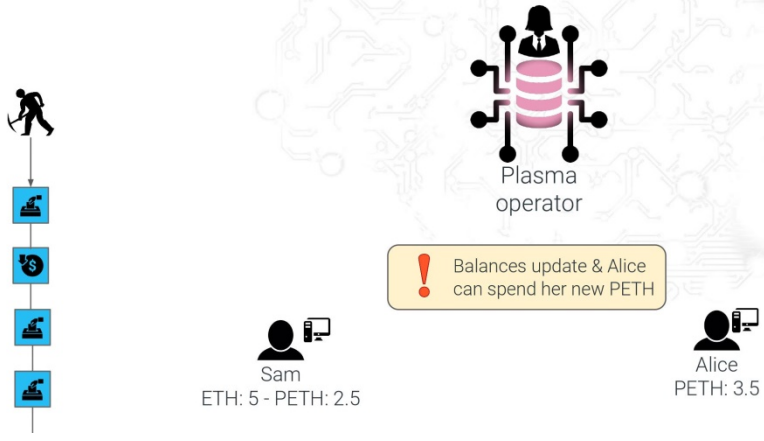

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1


Minimal Viable Plasma
Plasma
operator
Sees a Plasma block with
Sam's txs in the root chain
Sam
ETH: 5 - PETH: 5
Alice
PETH: 1

Minimal Viable Plasma

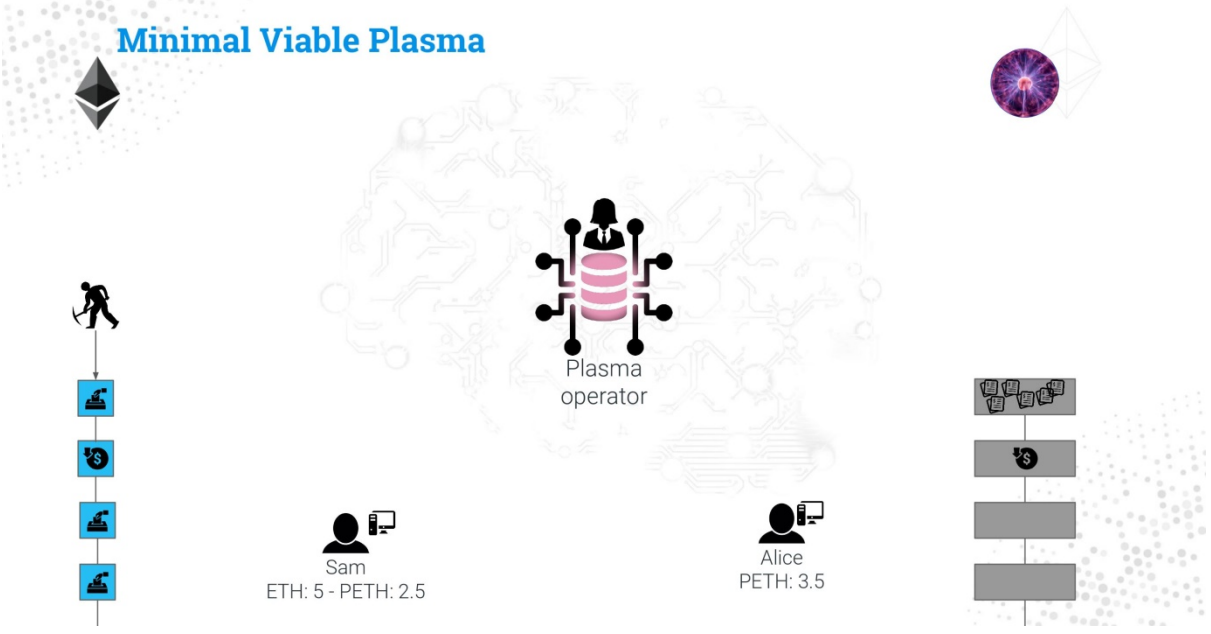


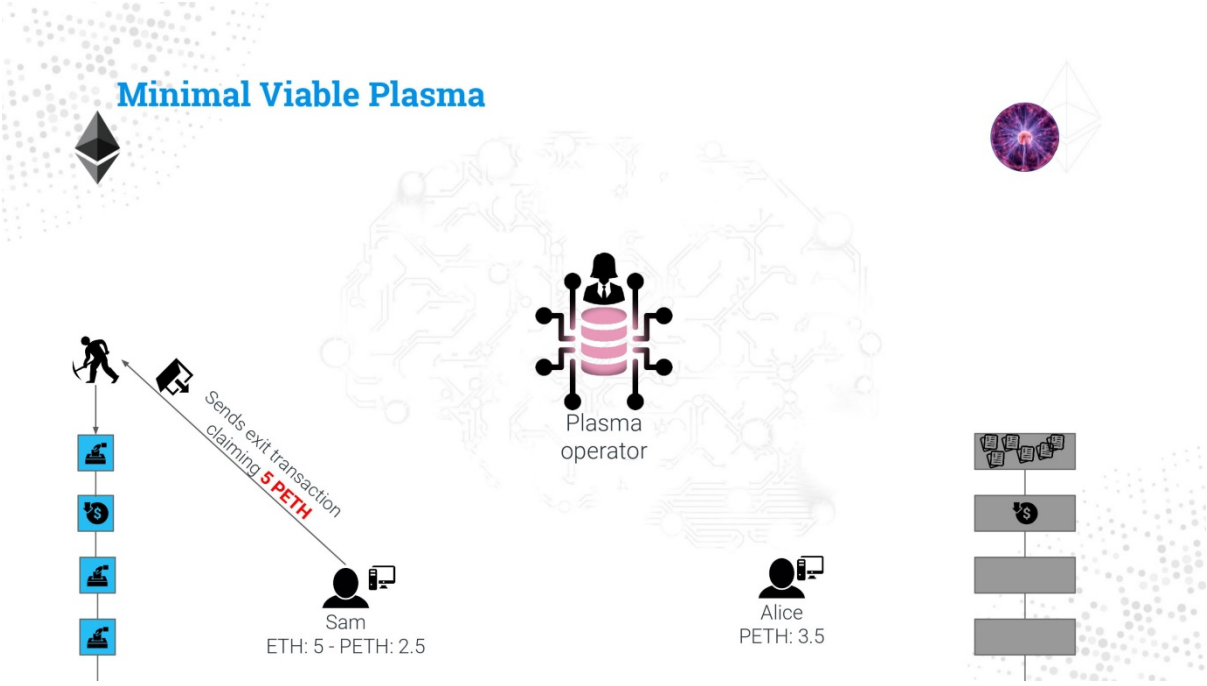
Minimal Viable Plasma

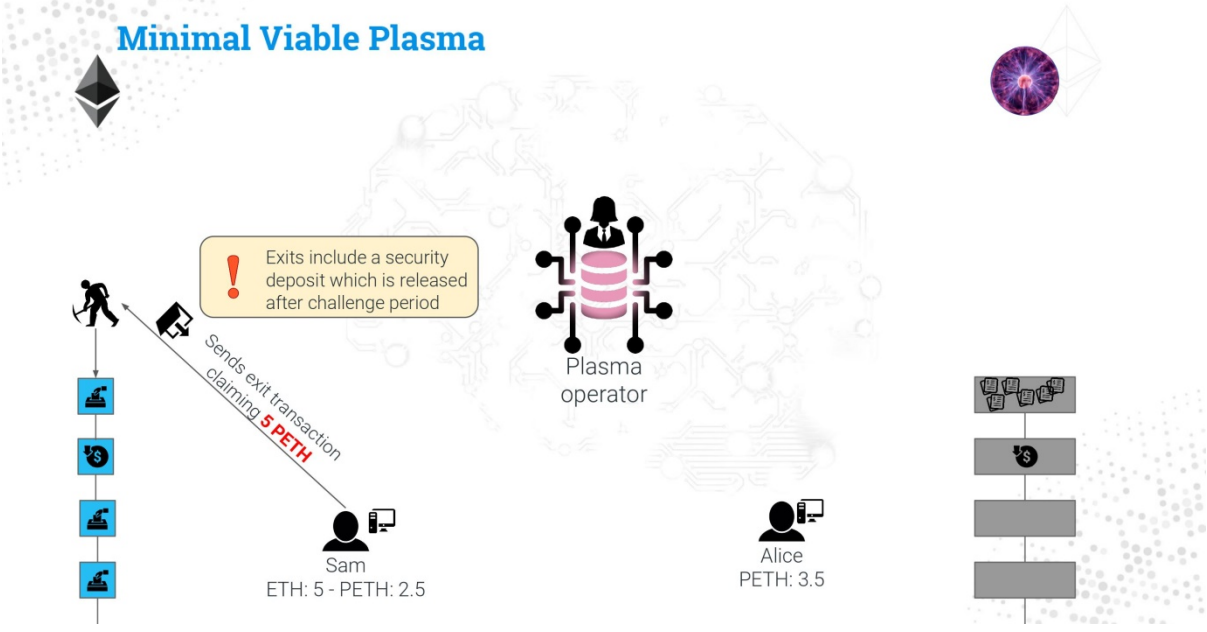


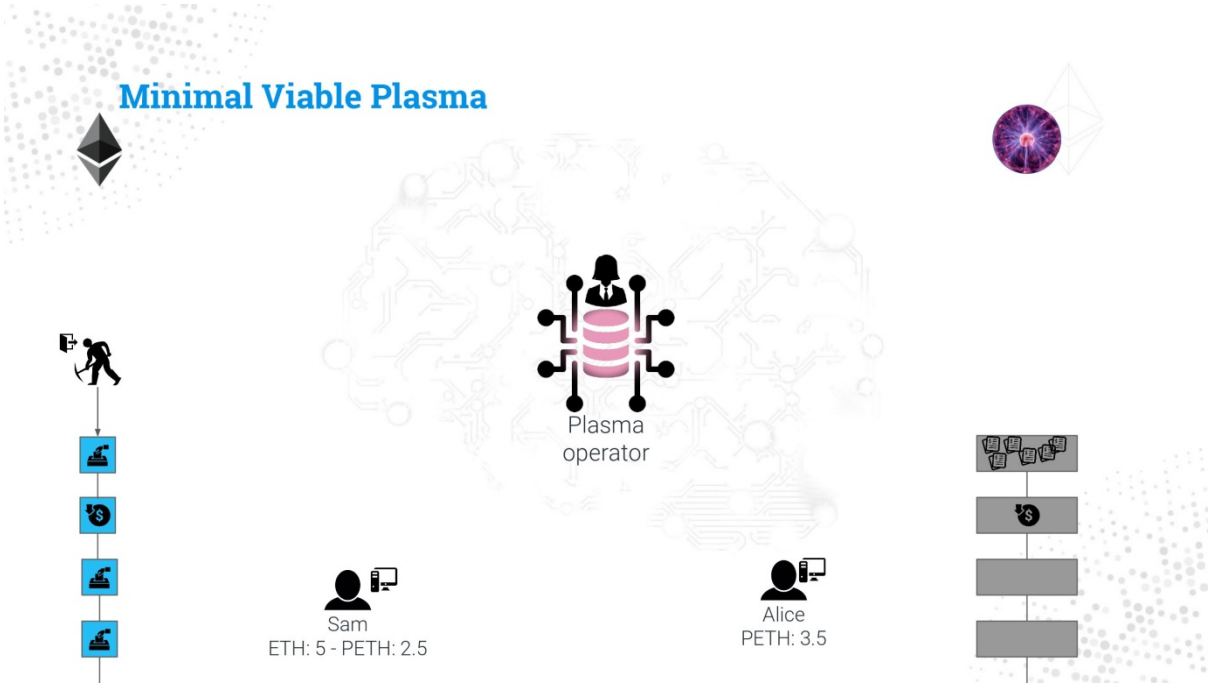
Minimal Viable Plasma

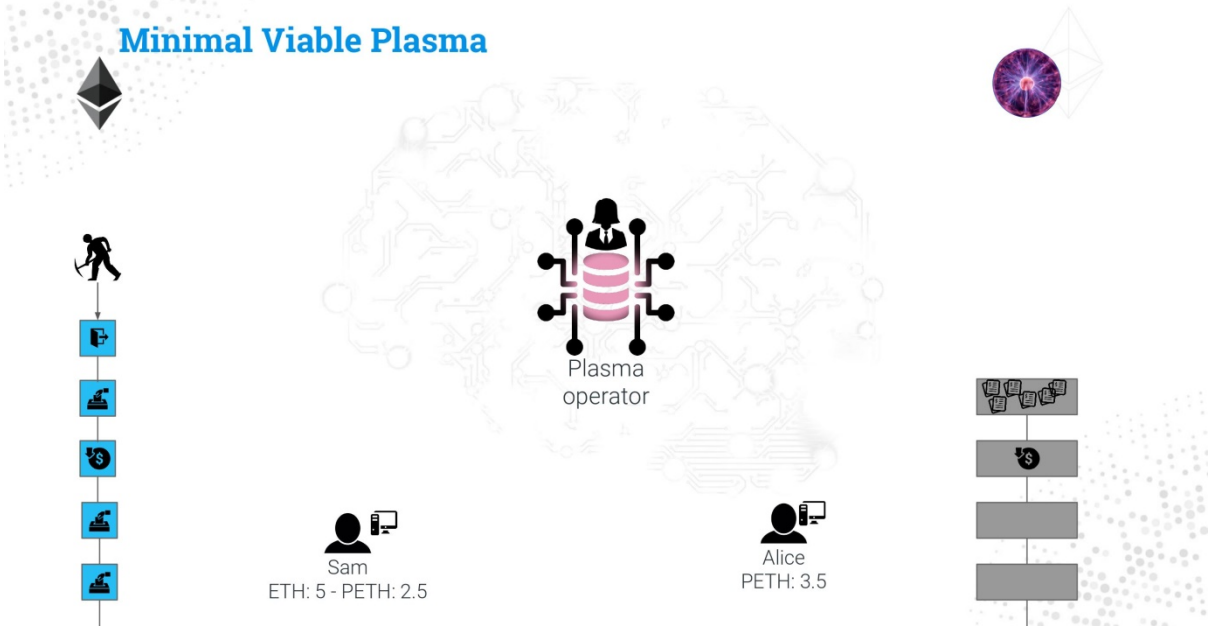
1. Operator creates a block
2. Sam deposits ETH into the Plasma chain
   a. New Plasma block is created
   b. Sam begins watching Plasma chain for misbehavior
3. Sam sends a bunch of transactions to Alice
   a. Sam confirms the transactions
4. Sam attempts to exit with all 5 PETH
   a. Alice stops the exit with challenge
5. Operator creates an invalid block
   a. Sam and Alice exit before operator steals their ETH

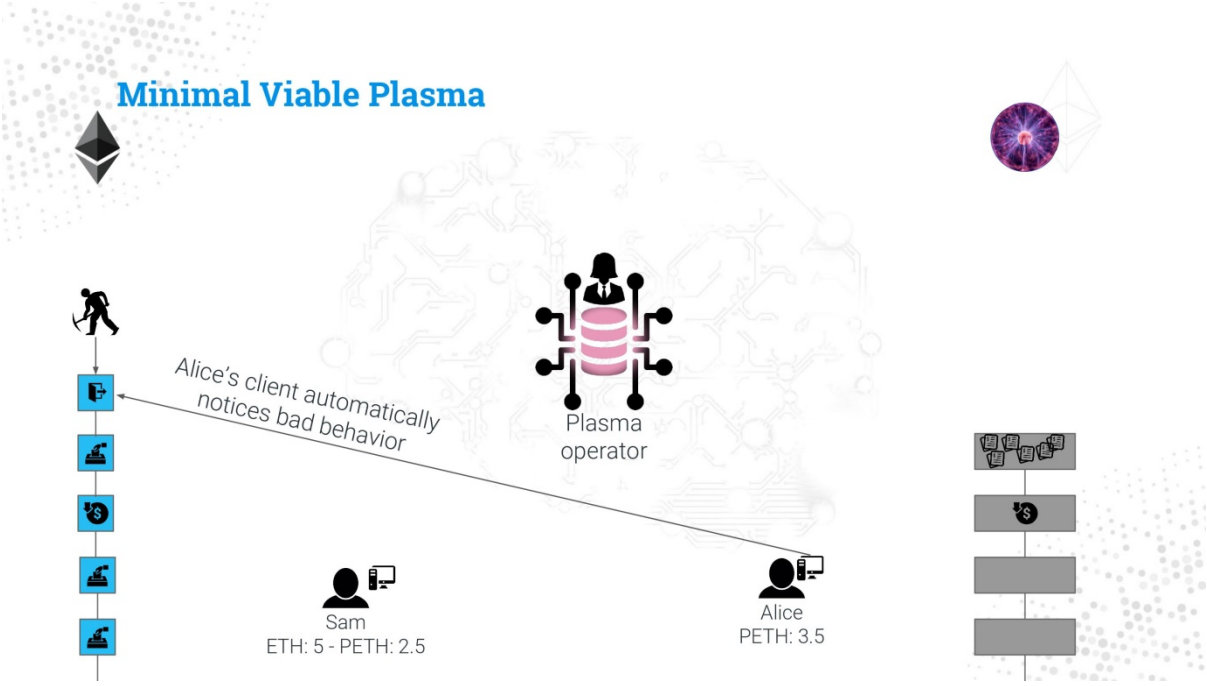


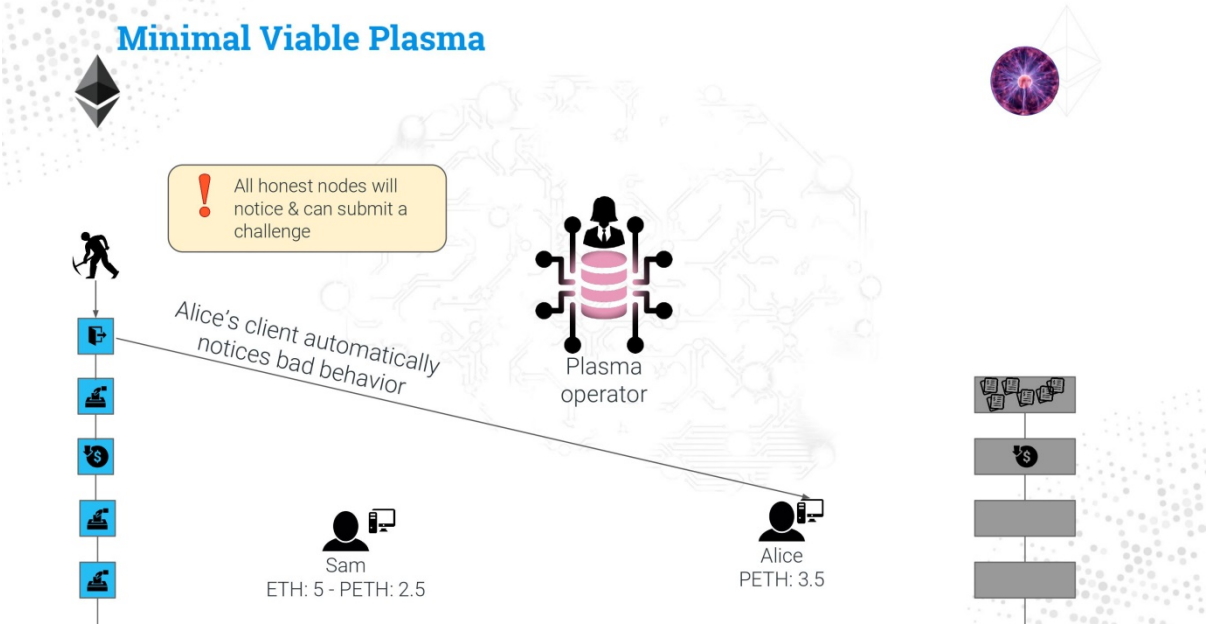

Minimal Viable Plasma
Plasma operator
Sends exit transaction claiming 5 PETH
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

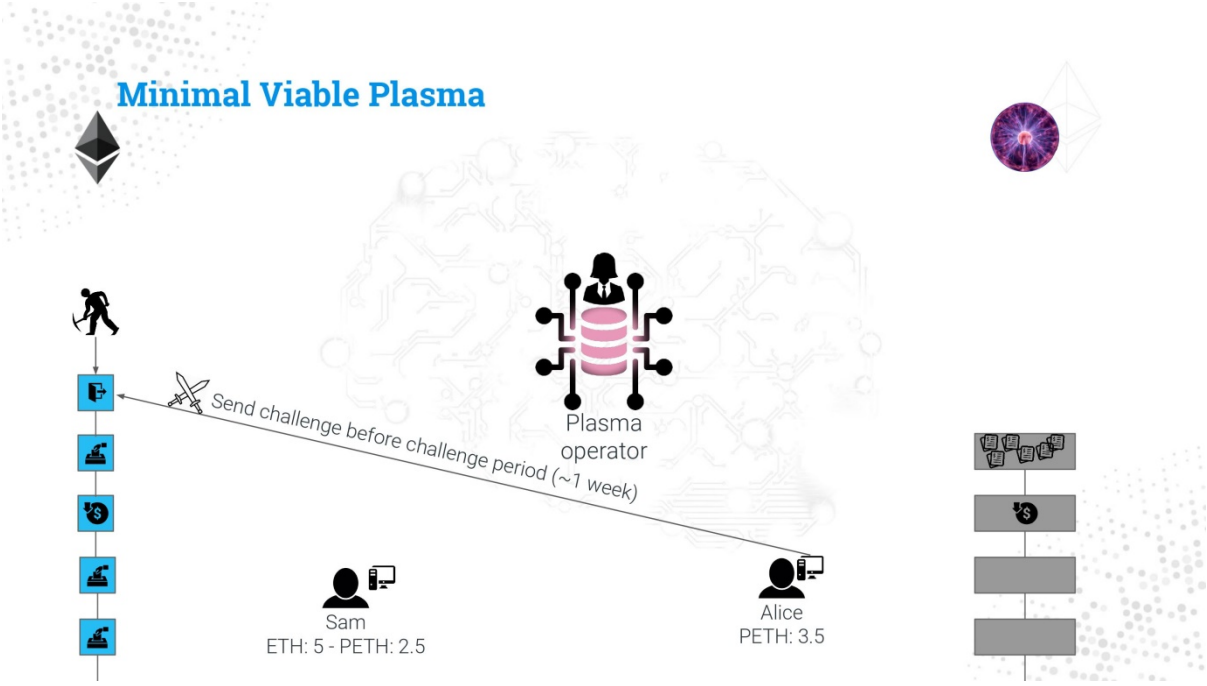

Minimal Viable Plasma
Exits include a security deposit which is released after challenge period
Plasma operator
Sends exit transaction claiming 5 PETH
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

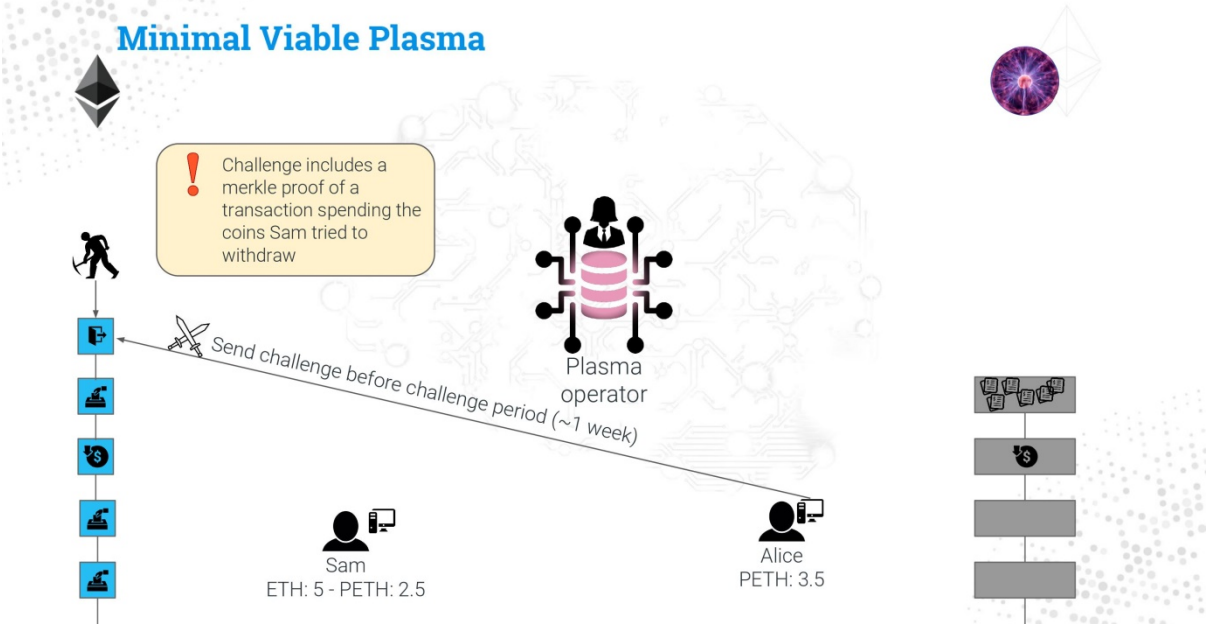

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

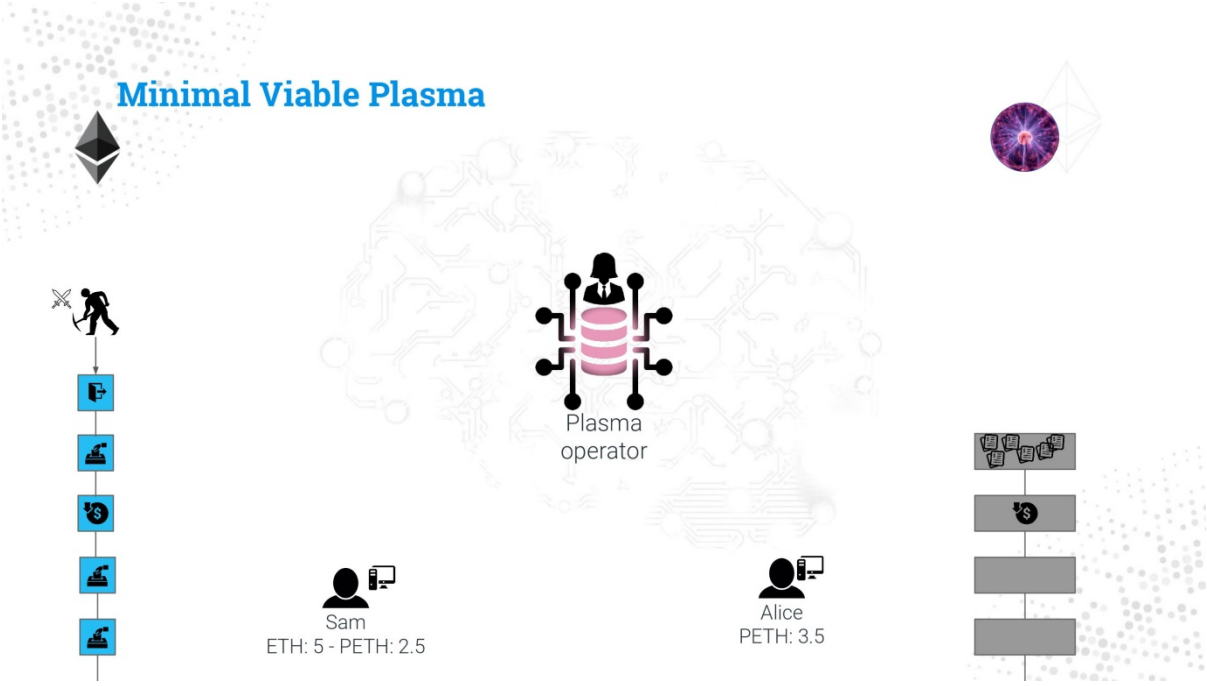

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

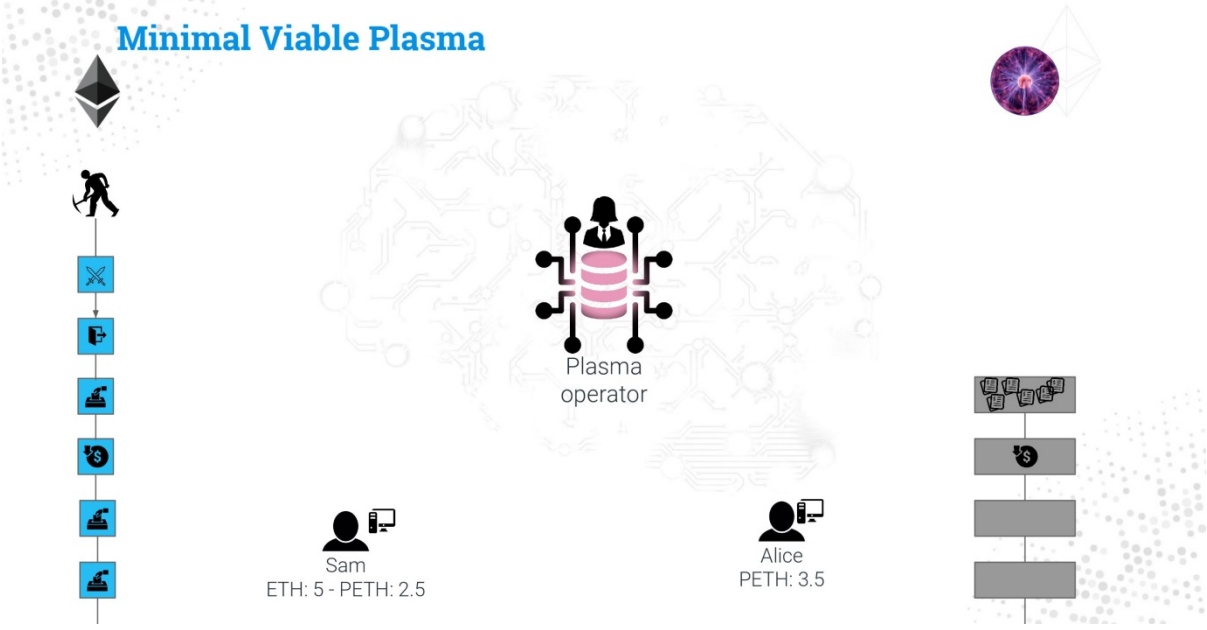

Minimal Viable Plasma
Alice's client automatically notices bad behavior
Plasma operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

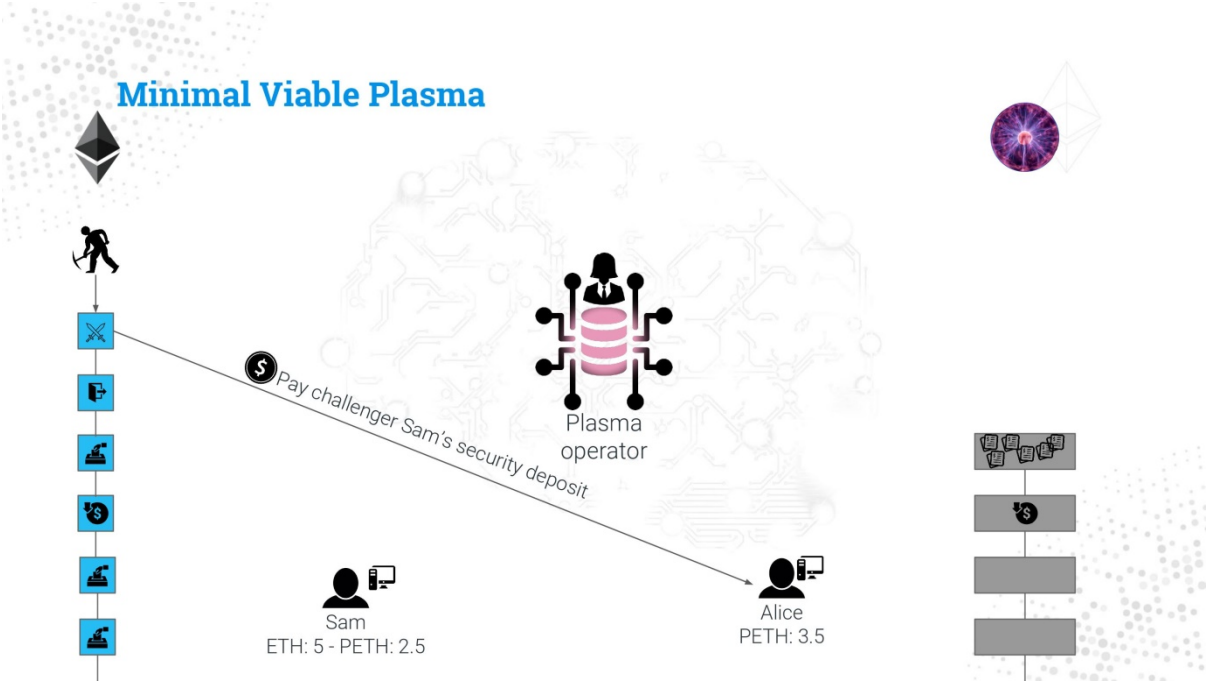

Minimal Viable Plasma
All honest nodes will notice & can submit a challenge
Alice's client automatically notices bad behavior
Plasma operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

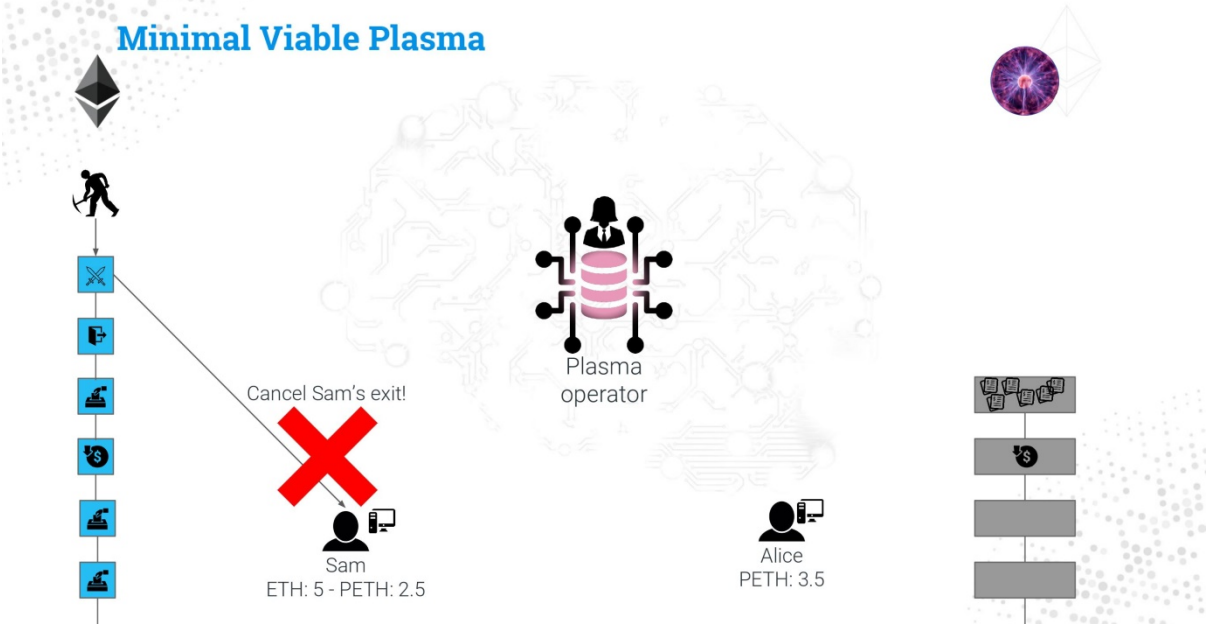

Minimal Viable Plasma
Send challenge before challenge period (~1 week)
Plasma operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

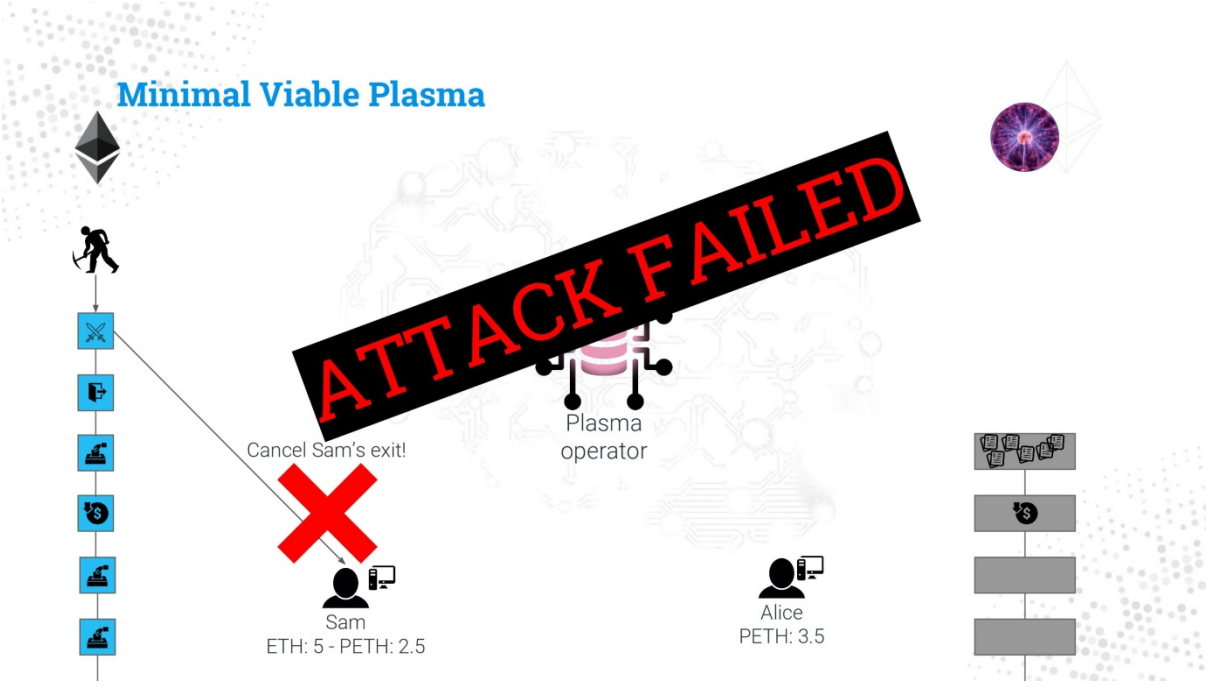

Minimal Viable Plasma
Challenge includes a merkle proof of a transaction spending the coins Sam tried to withdraw
Send challenge before challenge period (~1 week)
Plasma operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

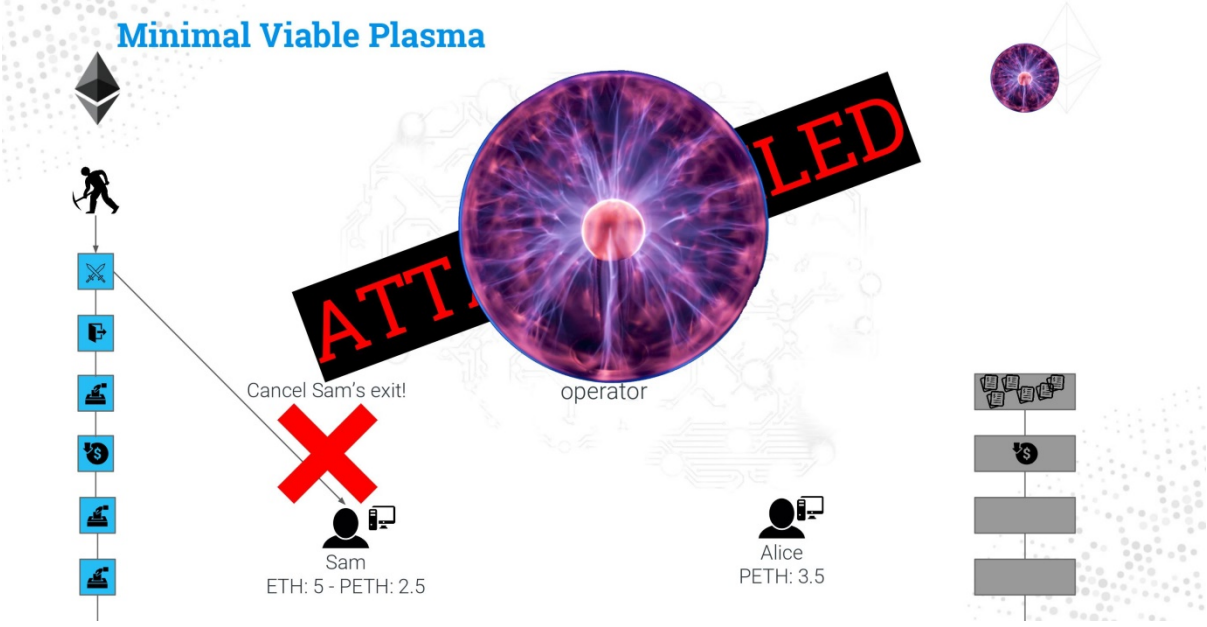

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5


Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

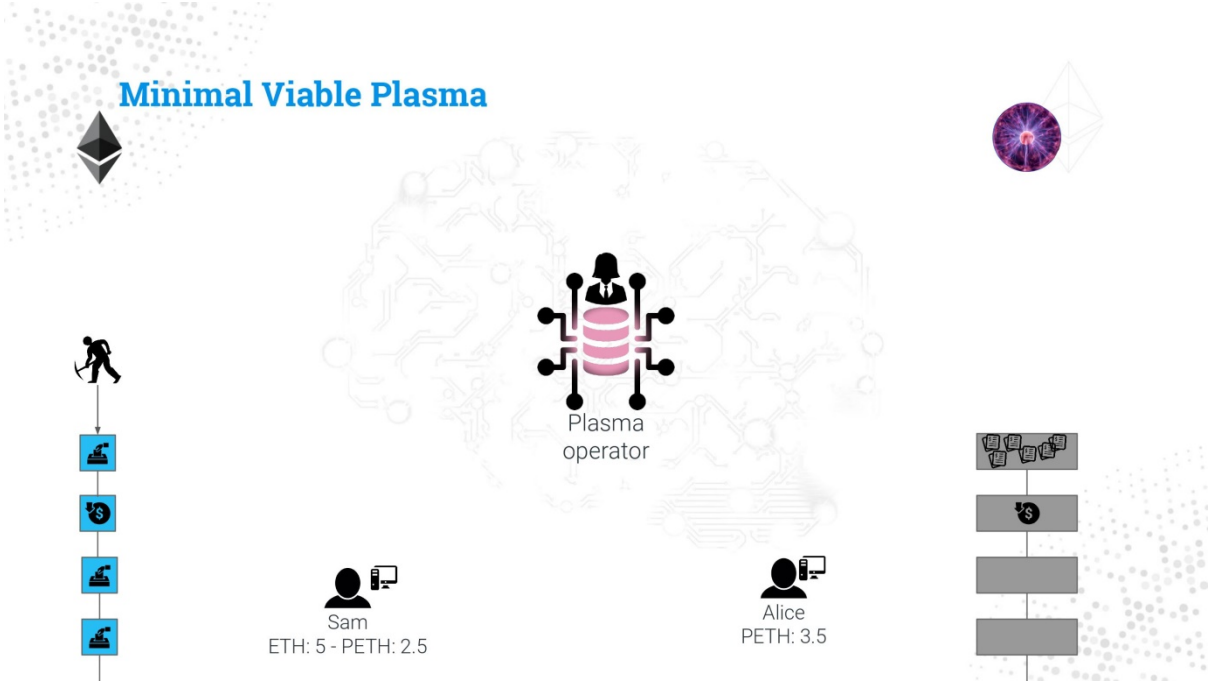

Minimal Viable Plasma
Pay challenger Sam's security deposit
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

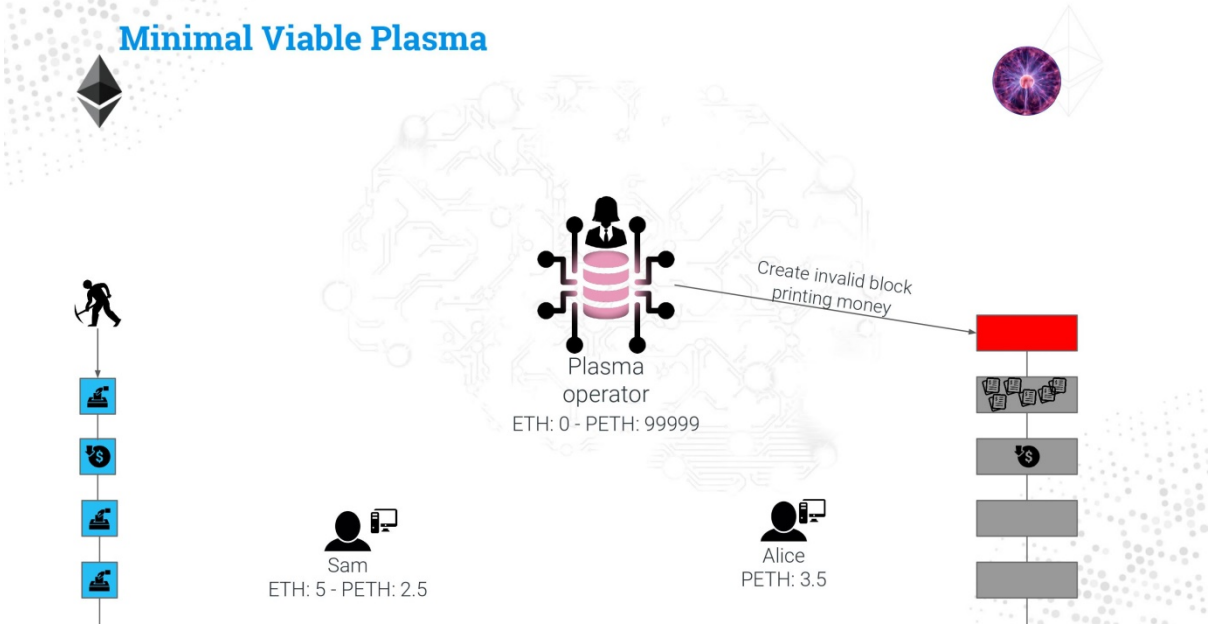

Minimal Viable Plasma
Cancel Sam's exit!
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

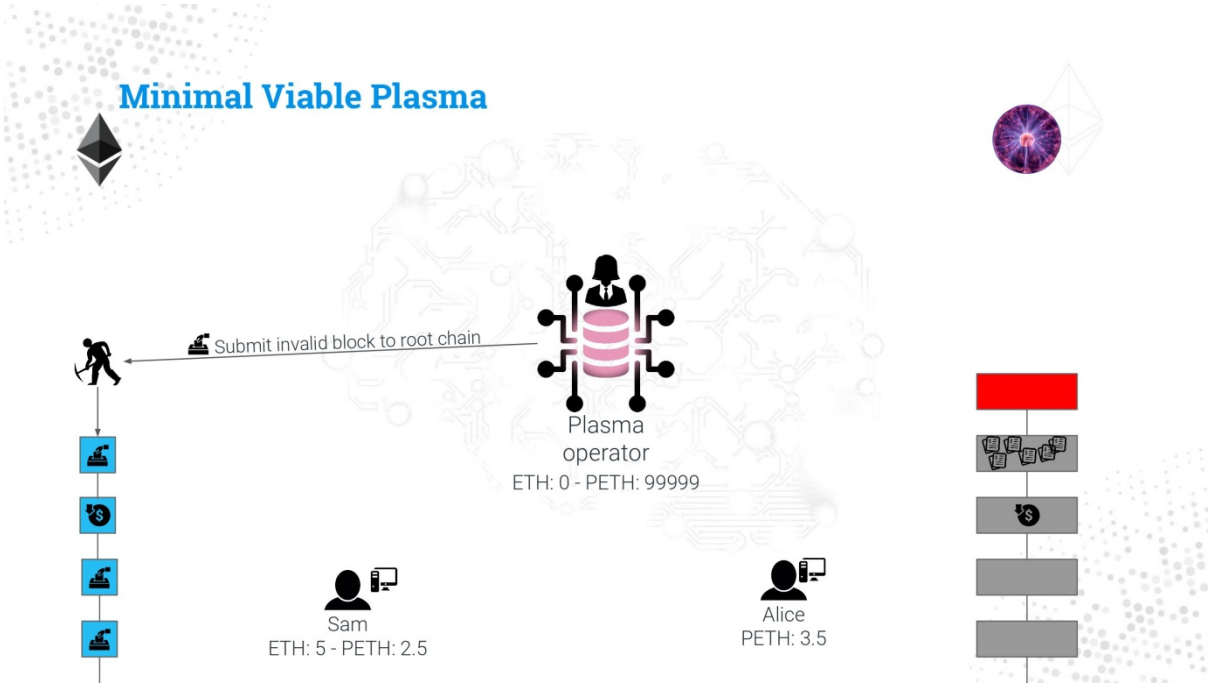

Minimal Viable Plasma
ATTACK FAILED
Plasma
operator
Cancel Sam's exit!
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

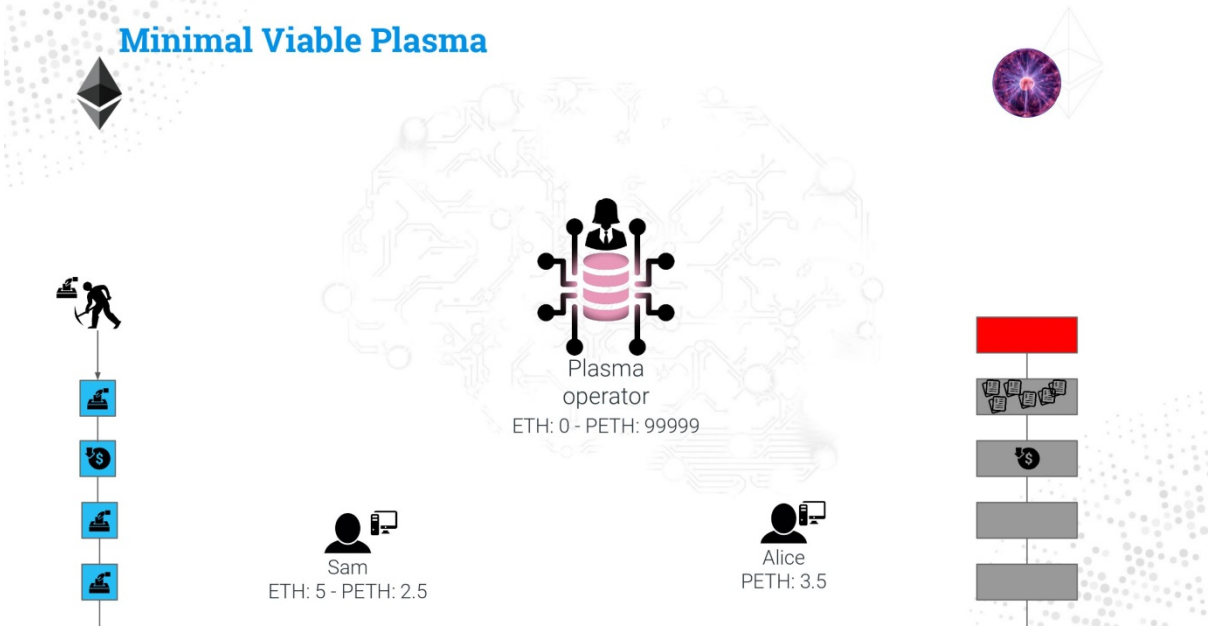

Minimal Viable Plasma
operator
Cancel Sam's exit!
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

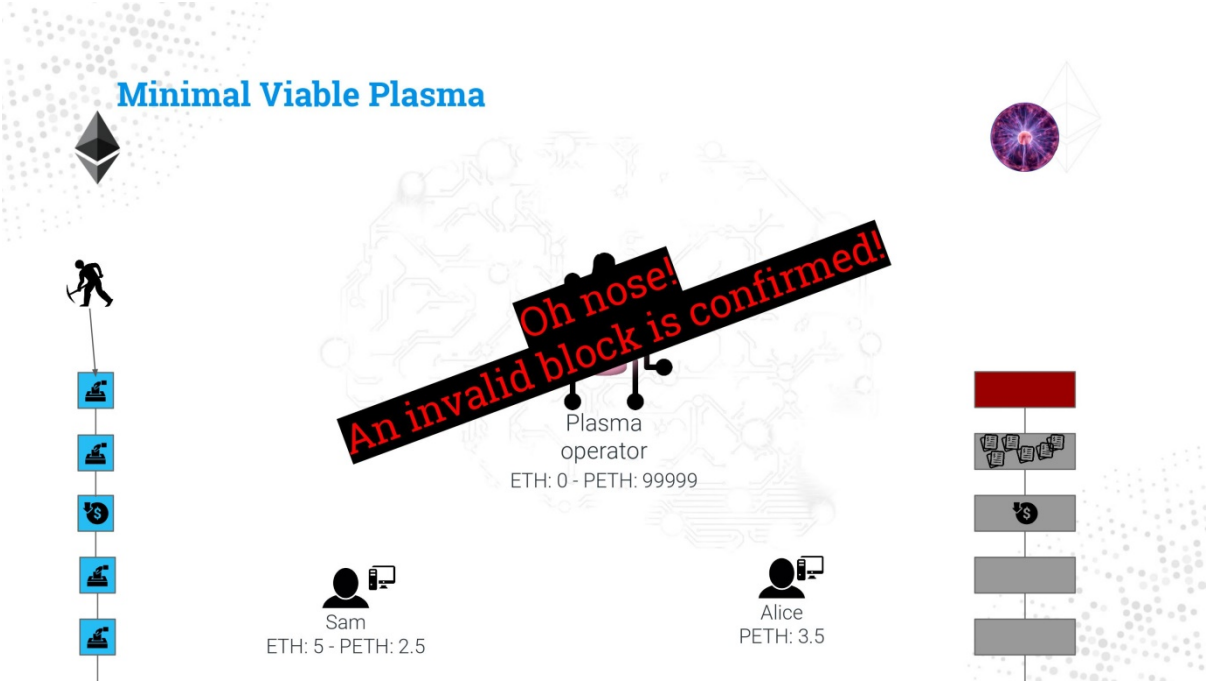
1. Operator creates a block
2. Sam deposits ETH into the Plasma chain
   a. New Plasma block is created
   b. Sam begins watching Plasma chain for misbehavior
3. Sam sends a bunch of transactions to Alice
   a. Sam confirms the transactions
4. Sam attempts to exit with all 5 PETH
   a. Alice stops the exit with challenge
5. Operator creates an invalid block
   a. Sam and Alice exit before operator steals their ETH

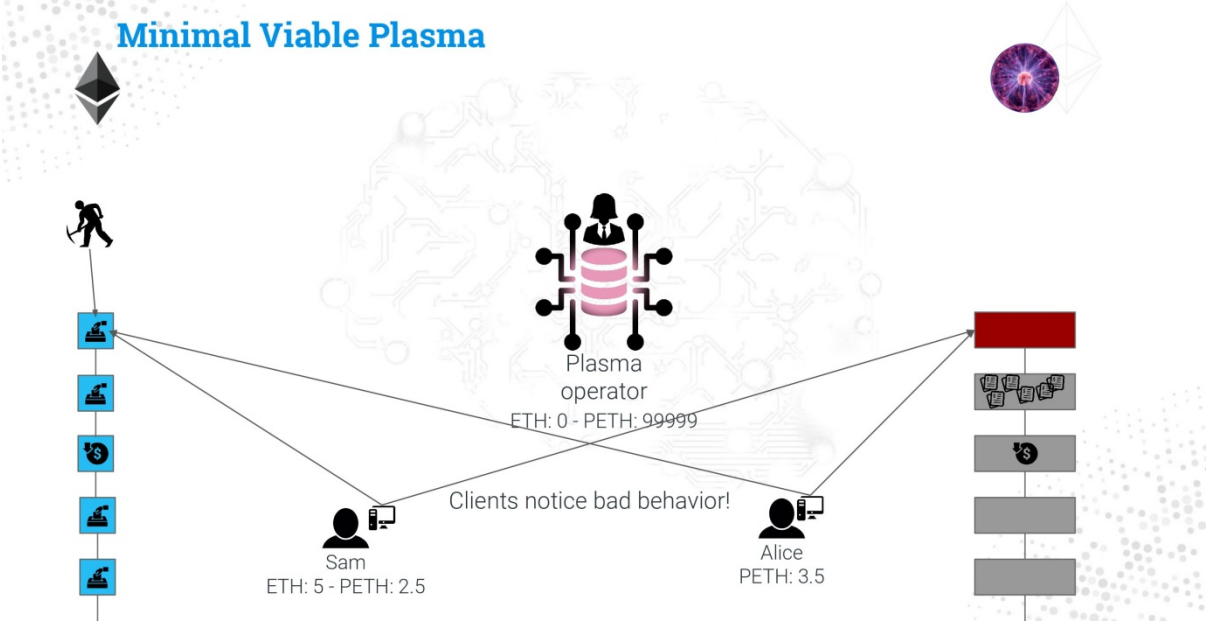

Minimal Viable Plasma
Plasma
operator
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

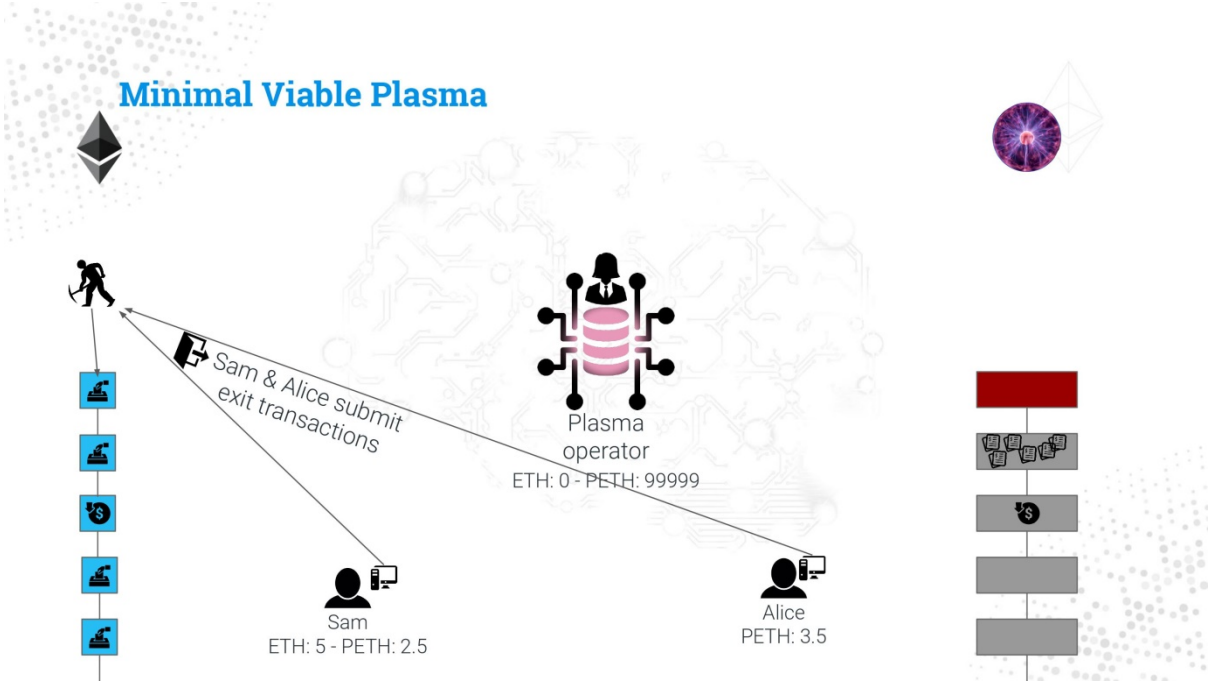

Minimal Viable Plasma
Create invalid block
printing money
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

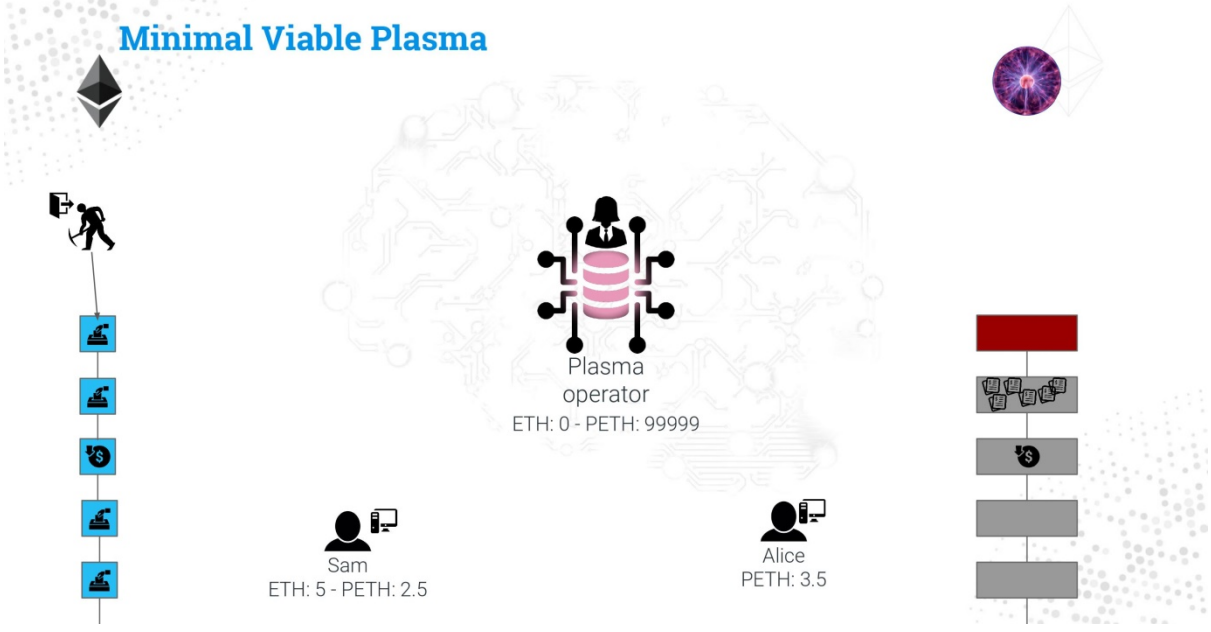

Minimal Viable Plasma
Submit invalid block to root chain
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

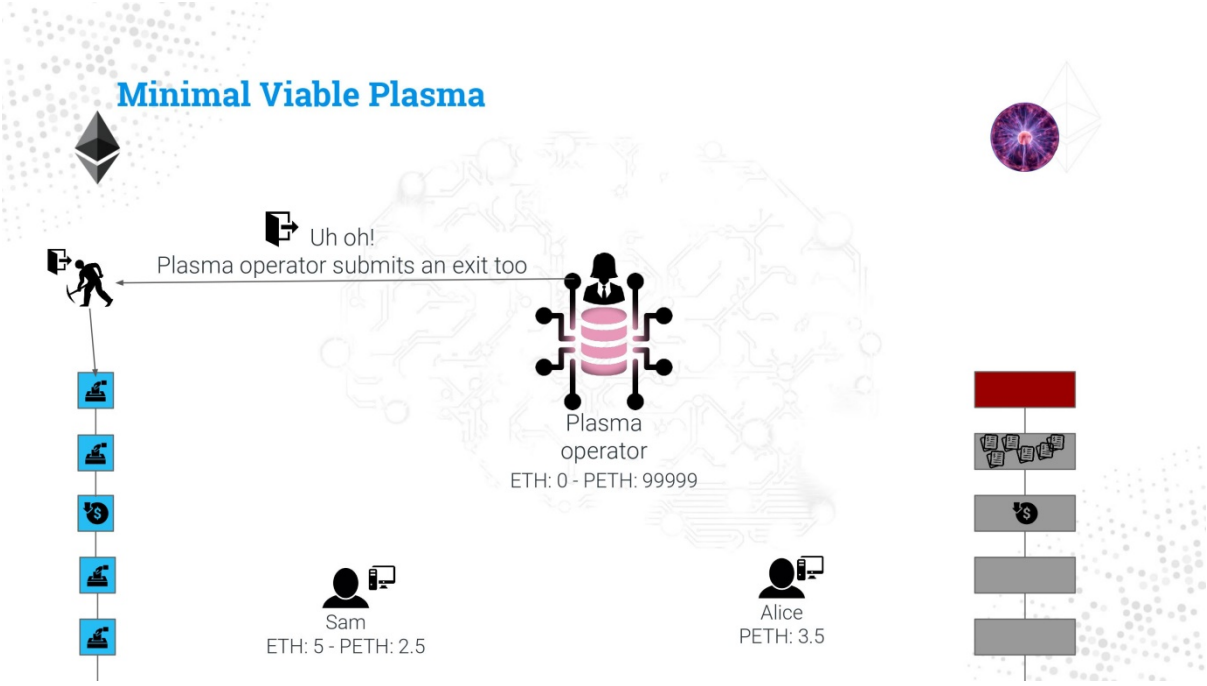

Minimal Viable Plasma
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

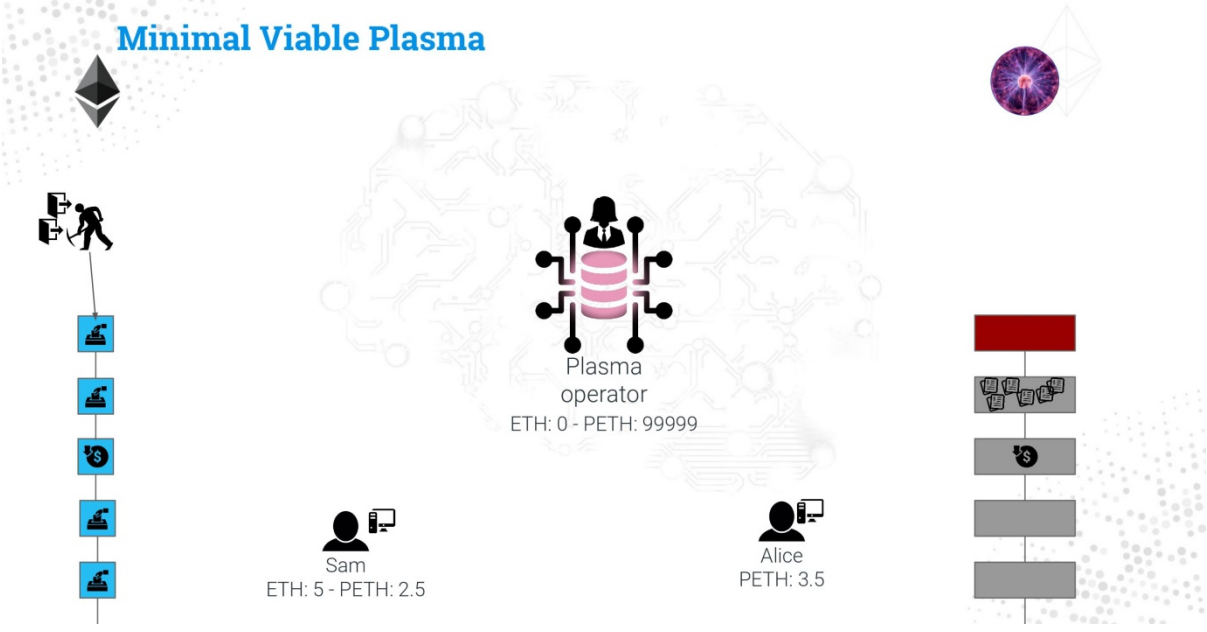

Minimal Viable Plasma
Oh nose!
An invalid block is confirmed!
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

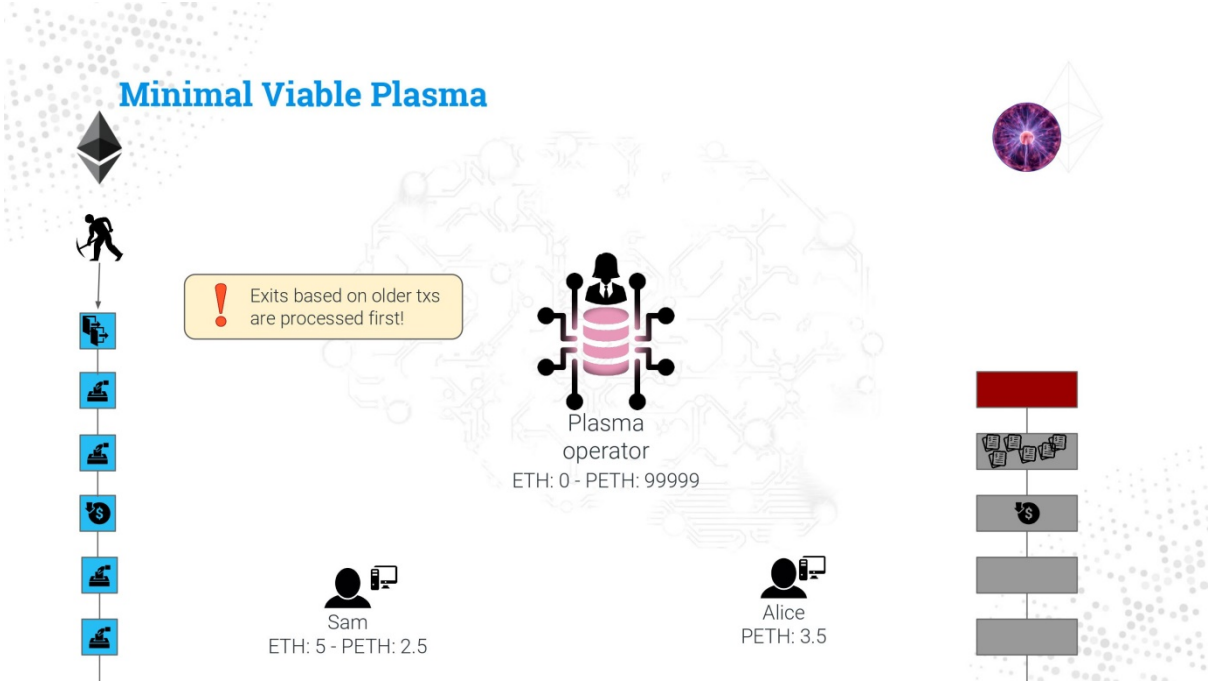

Minimal Viable Plasma
Plasma
operator
ETH: 0 - PETH: 99999
Clients notice bad behavior!
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

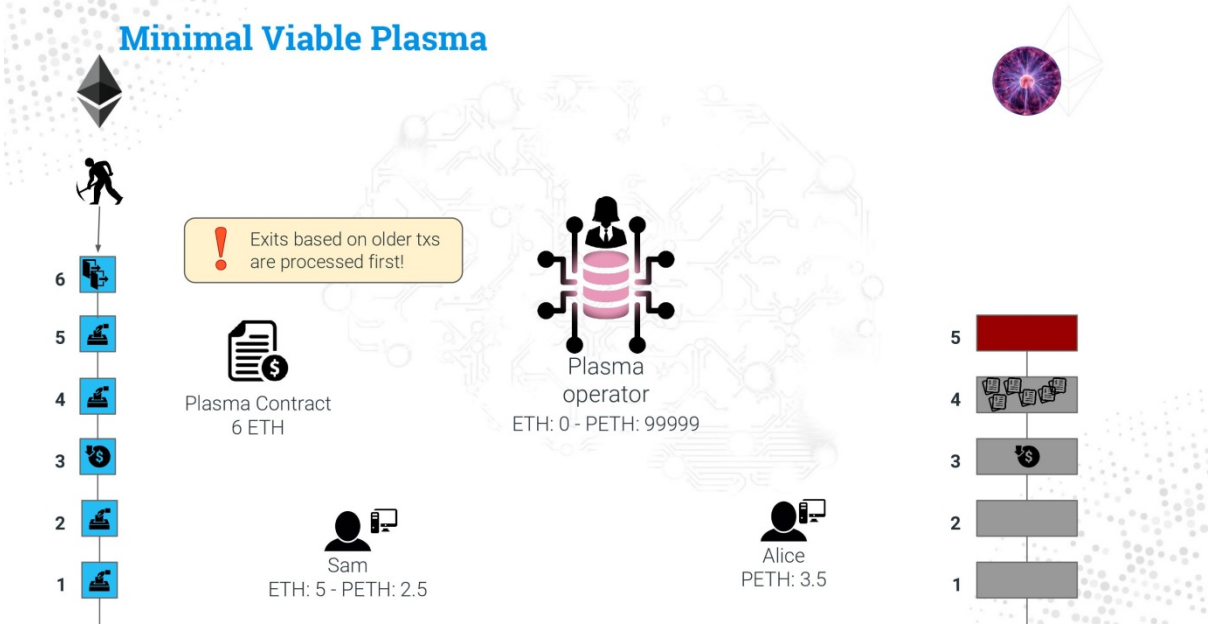

Minimal Viable Plasma
Sam & Alice submit
exit transactions
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

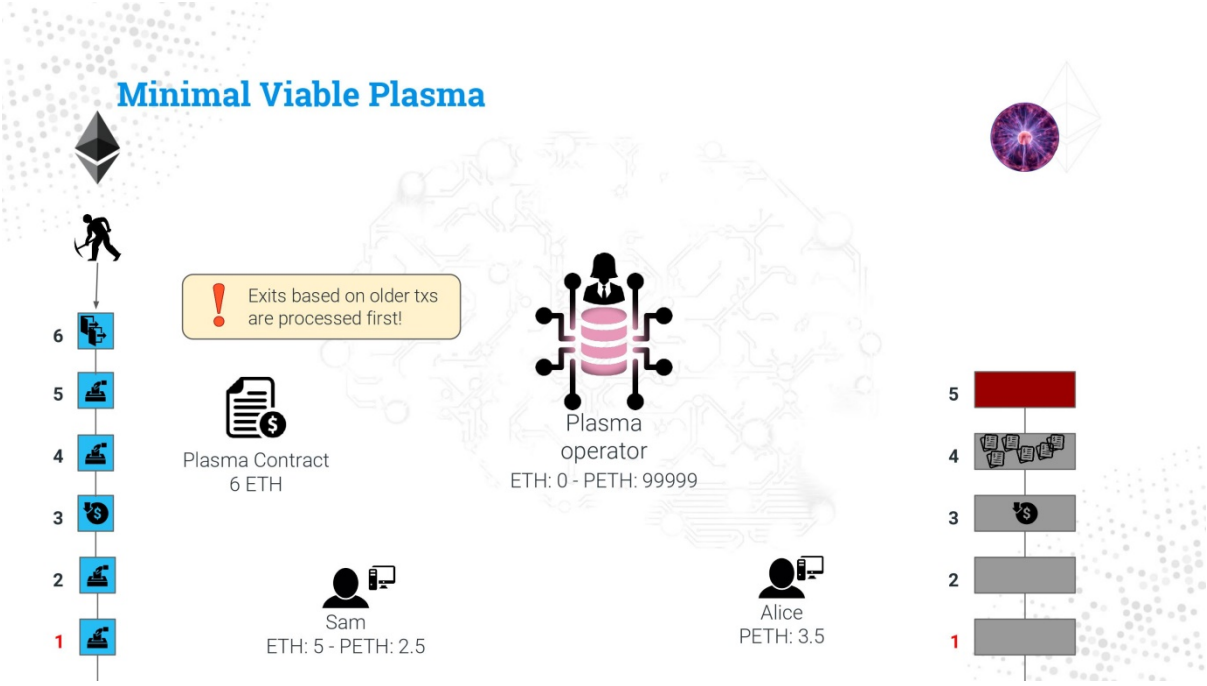

Minimal Viable Plasma
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

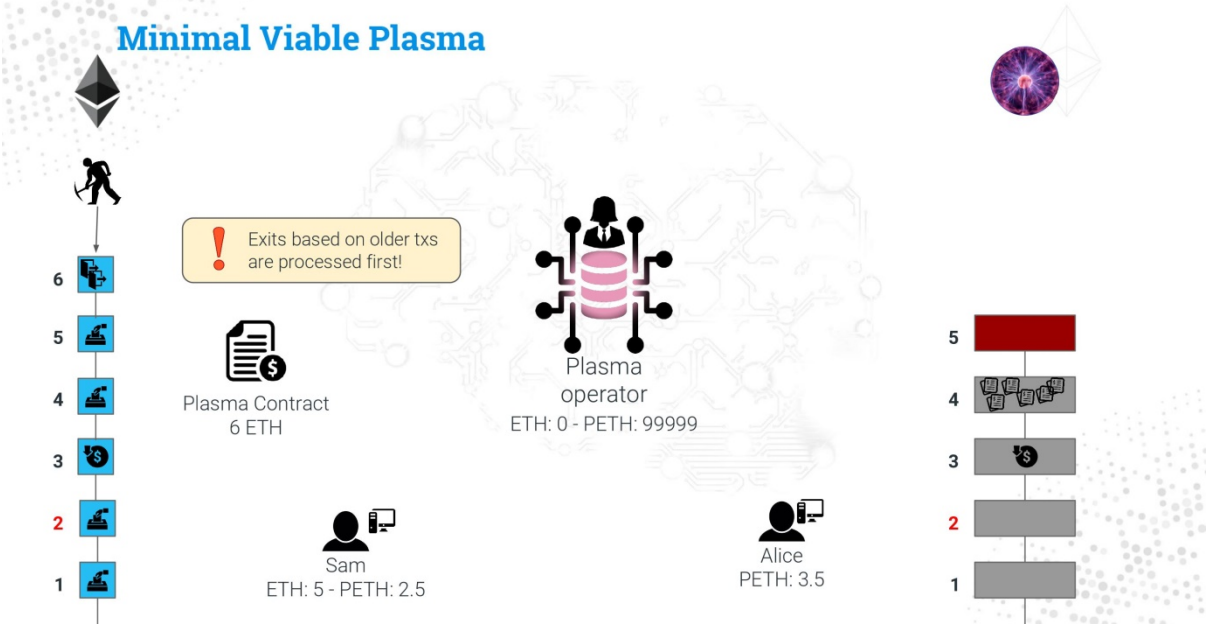

Minimal Viable Plasma
Uh oh!
Plasma operator submits an exit too
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

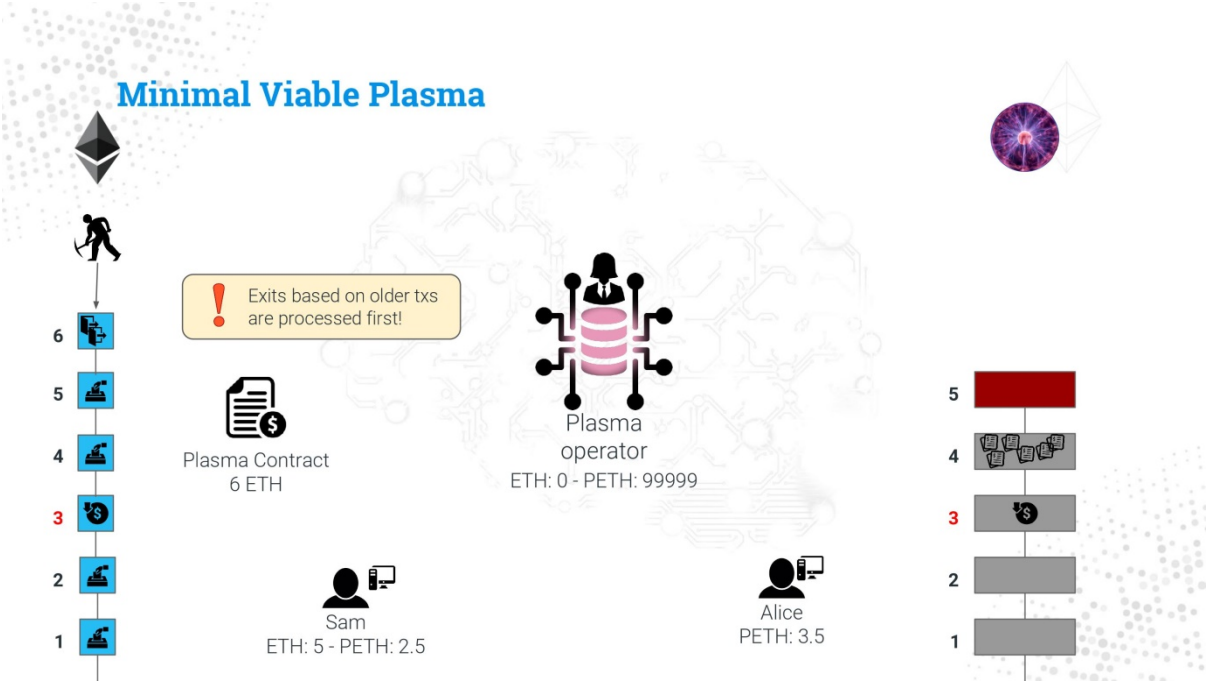

Minimal Viable Plasma
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

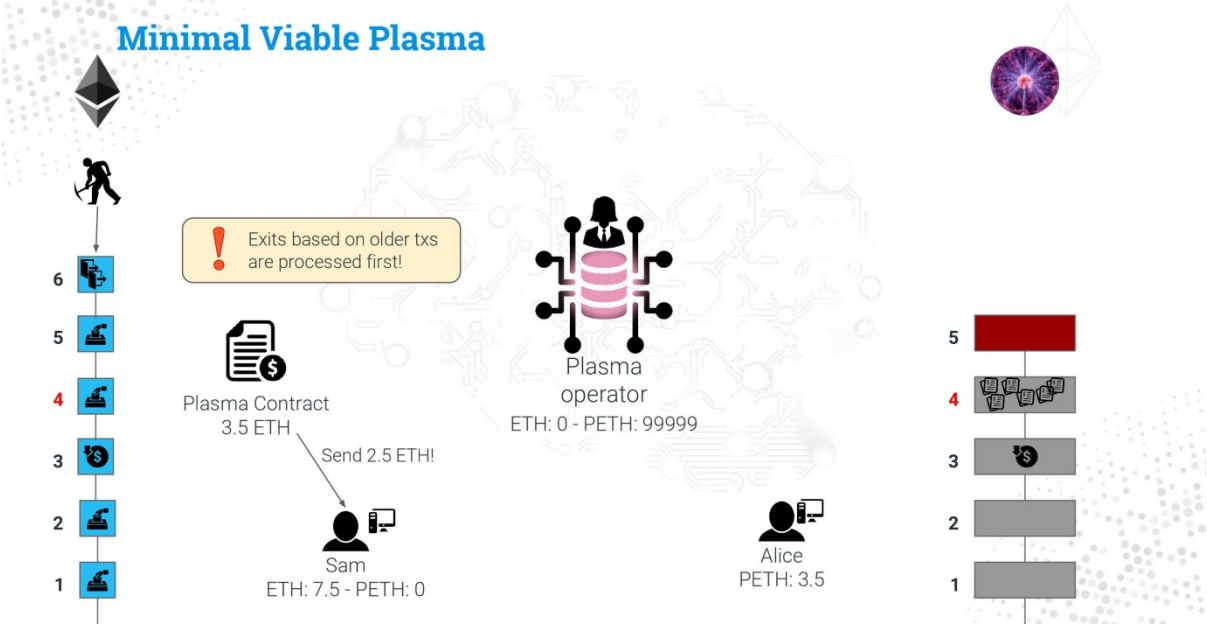

Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5

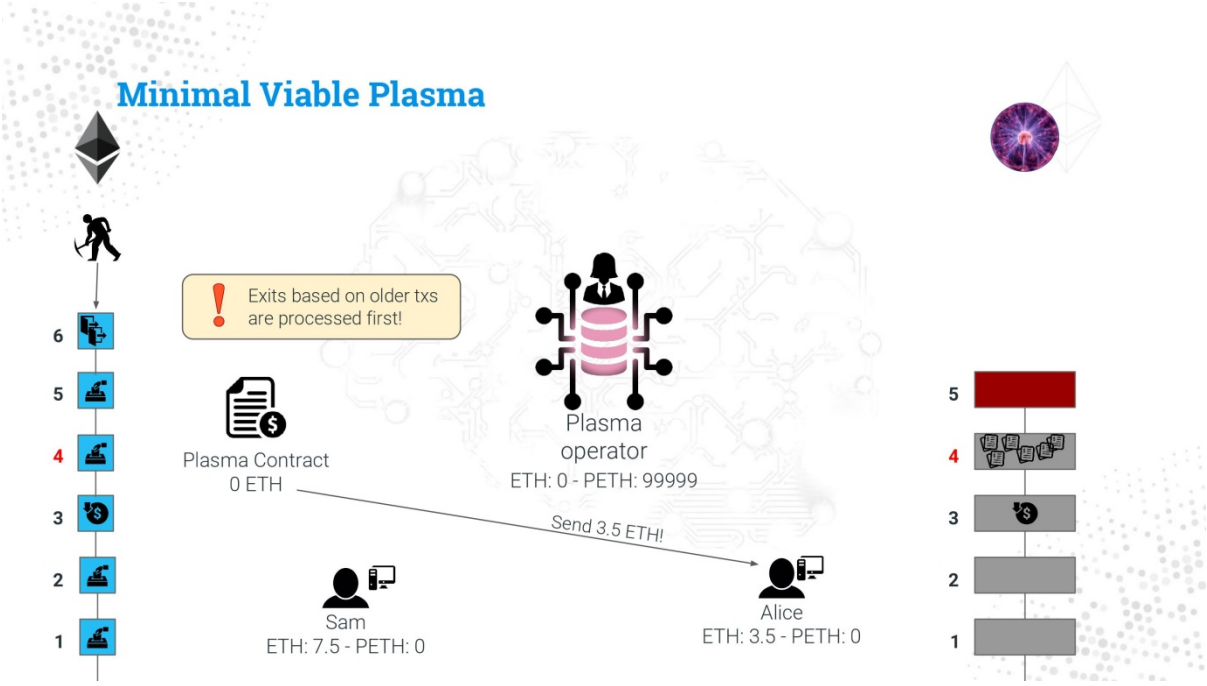

Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma Contract
6 ETH
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5
6
5
4
3
2
1

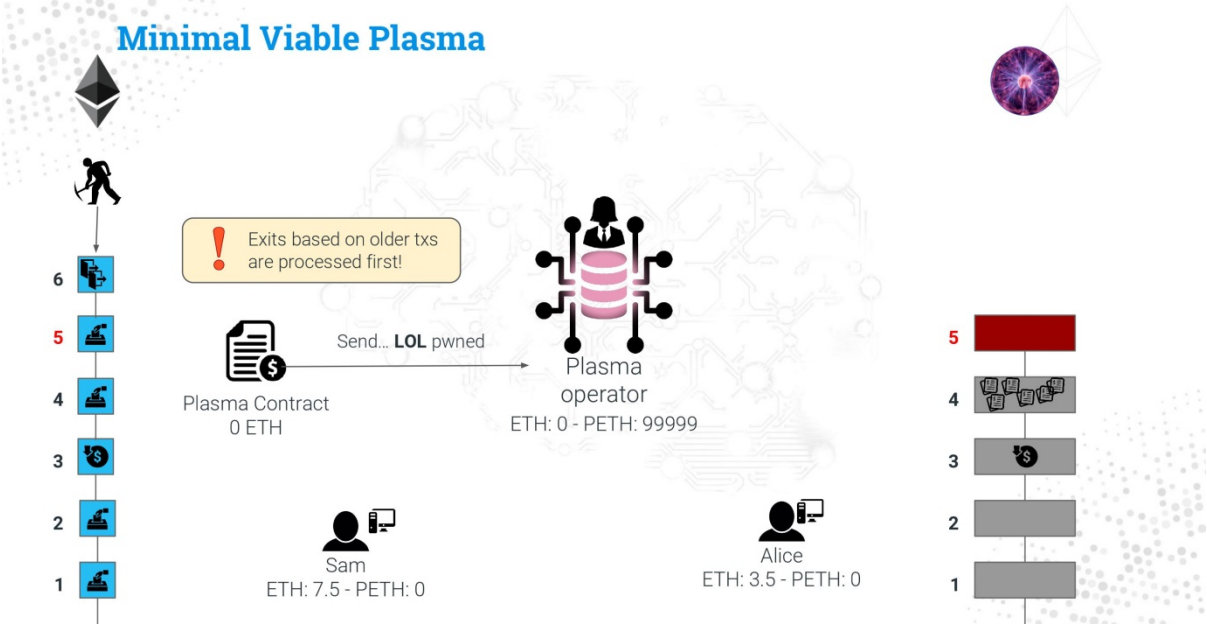

Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma Contract
6 ETH
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5
6
5
4
3
2
1

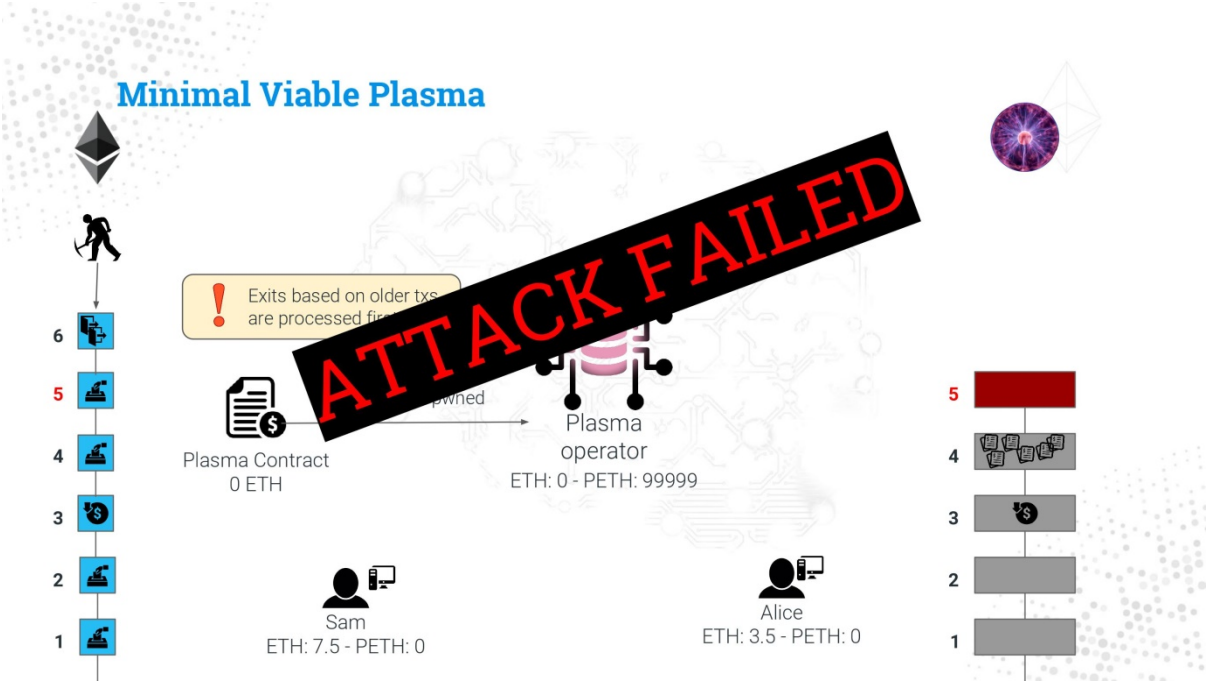

Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma Contract
6 ETH
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5
6
5
4
3
2
1

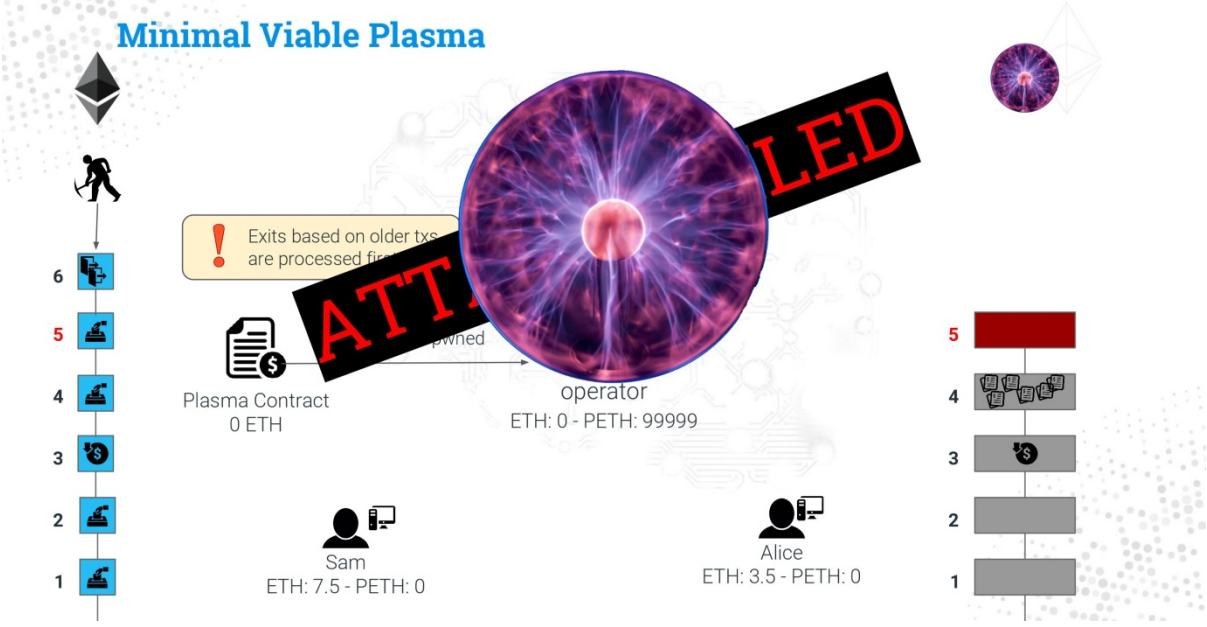

Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma Contract
6 ETH
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 5 - PETH: 2.5
Alice
PETH: 3.5
6
5
4
3
2
1


Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma Contract
3.5 ETH
Send 2.5 ETH!
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 7.5 - PETH: 0
Alice
PETH: 3.5
6
5
4
3
2
1


Minimal Viable Plasma
Exits based on older txs are processed first!
Plasma Contract
0 ETH
Plasma operator
ETH: 0 - PETH: 99999
Send 3.5 ETH!
Sam
ETH: 7.5 - PETH: 0
Alice
ETH: 3.5 - PETH: 0
6
5
4
3
2
1


Minimal Viable Plasma
Exits based on older txs are processed first!
Send... LOL pwned
Plasma Contract
0 ETH
Plasma operator
ETH: 0 - PETH: 99999
Sam
ETH: 7.5 - PETH: 0
Alice
ETH: 3.5 - PETH: 0
6
5
4
3
2
1


Minimal Viable Plasma
ATTACK FAILED
Exits based on older txs
are processed fi
Plasma Contract
0 ETH
Plasma
operator
ETH: 0 - PETH: 99999
Sam
ETH: 7.5 - PETH: 0
Alice
ETH: 3.5 - PETH: 0
6
5
4
3
2
1


Minimal Viable Plasma
LED
Exits based on older txs
are processed fi
Plasma Contract
0 ETH
operator
ETH: 0 - PETH: 99999
Sam
ETH: 7.5 - PETH: 0
Alice
ETH: 3.5 - PETH: 0
6
5
4
3
2
1

Important Design Pattern: Constraints

Important Design Pattern: Constraints

- Trust is established by…
  - Limiting possible actions
  - Imposing costs for bad behavior

Final Takeaways

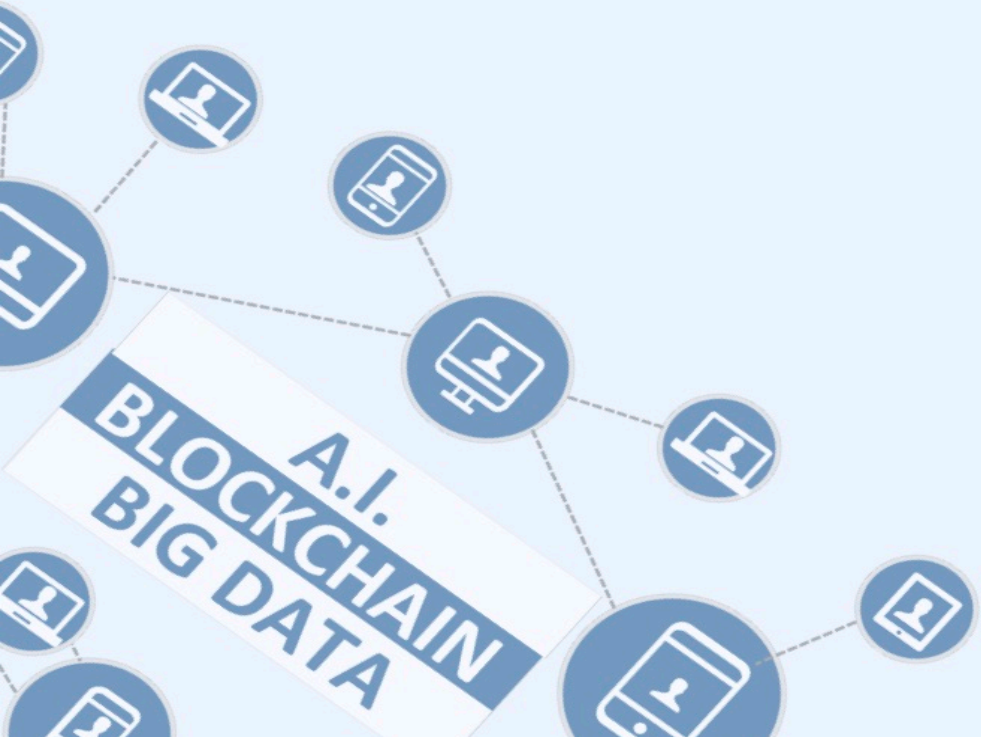
- Store minimal information on chain
  - Plasma avoids storing intermediate state
    - Only stores incoming & outgoing ETH balance
- Threat of recourse can be enough to prevent bad behavior

7강

Blockchain and Innovative Nation

전 하 진 위원장

(한국블록체인협회)



강의 동영상 URL

1 부: https://youtu.be/WPLivTGRYoY

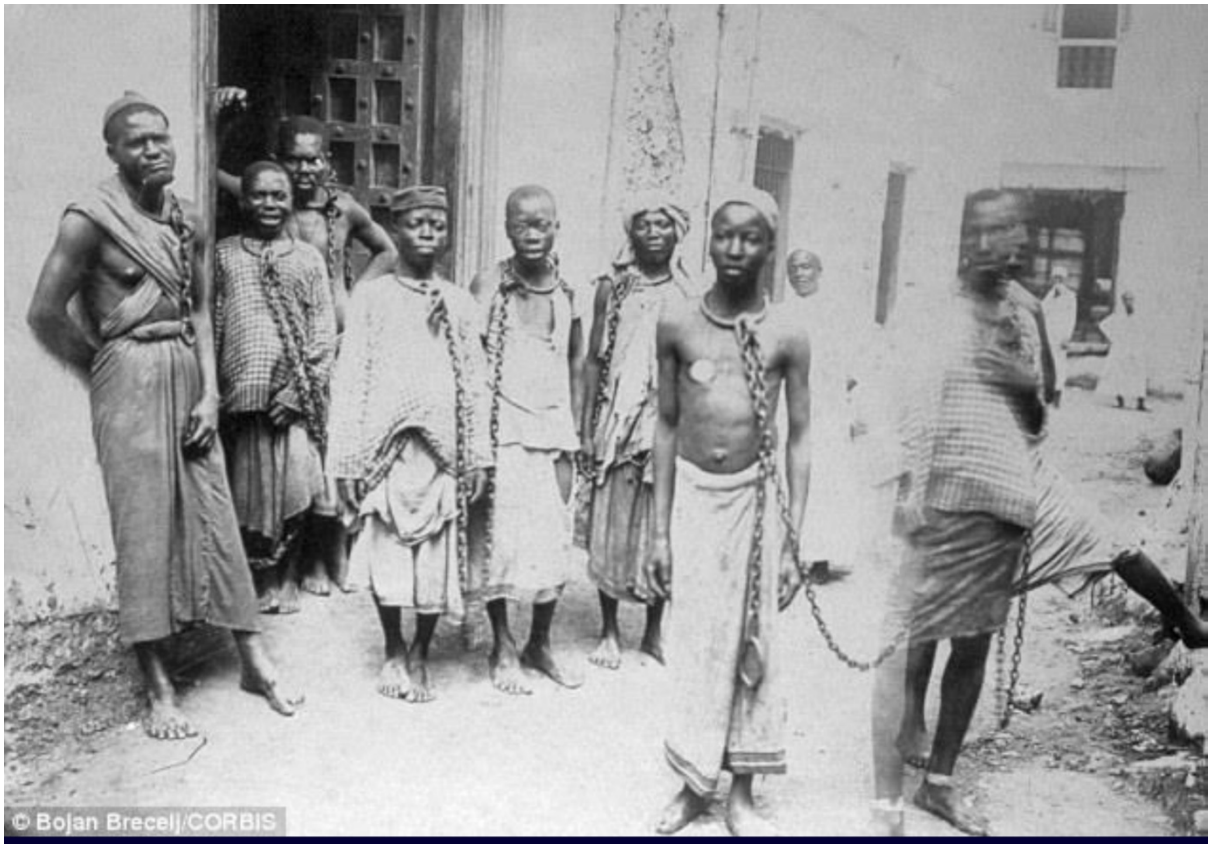
2 부: https://youtu.be/tQTn6z-97tU

Blockchain & Innovative Nation

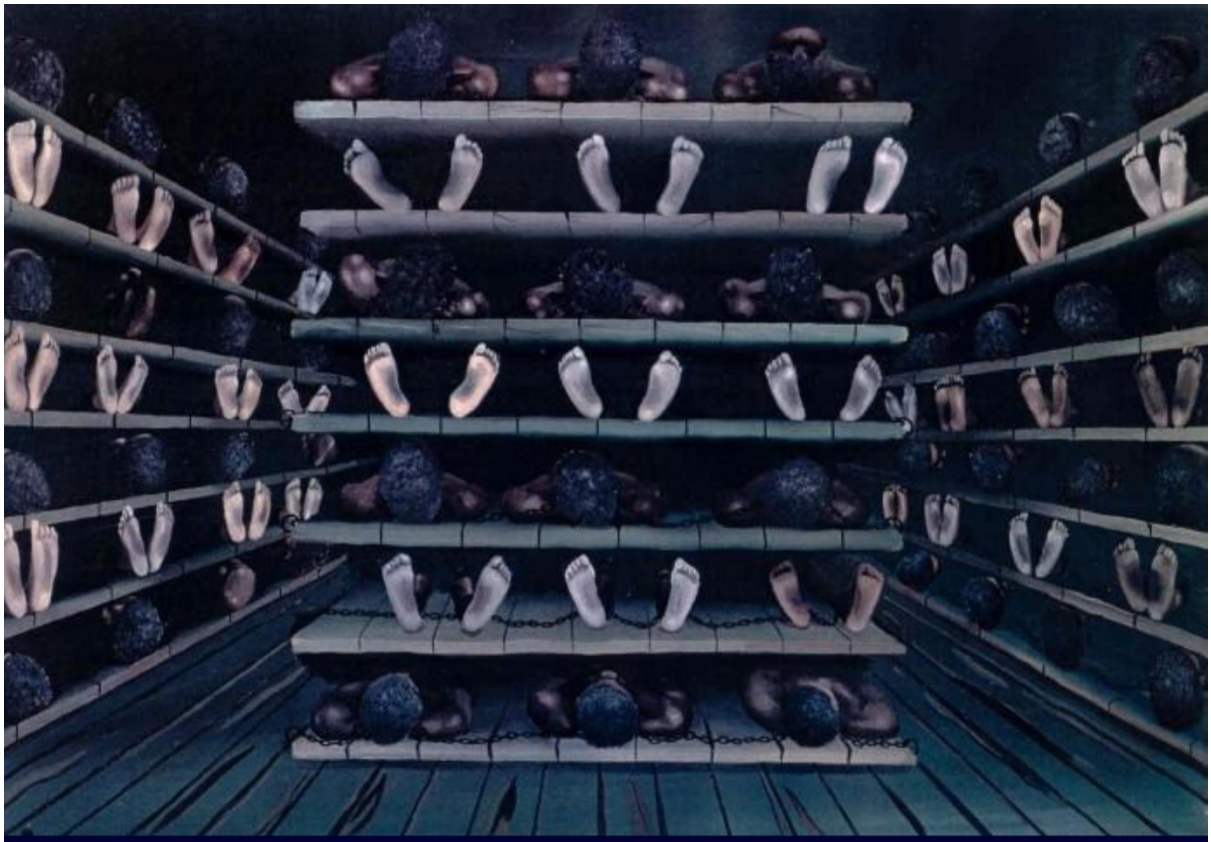
전 하 진

hajin@hajin.com

How has human civilization changed?



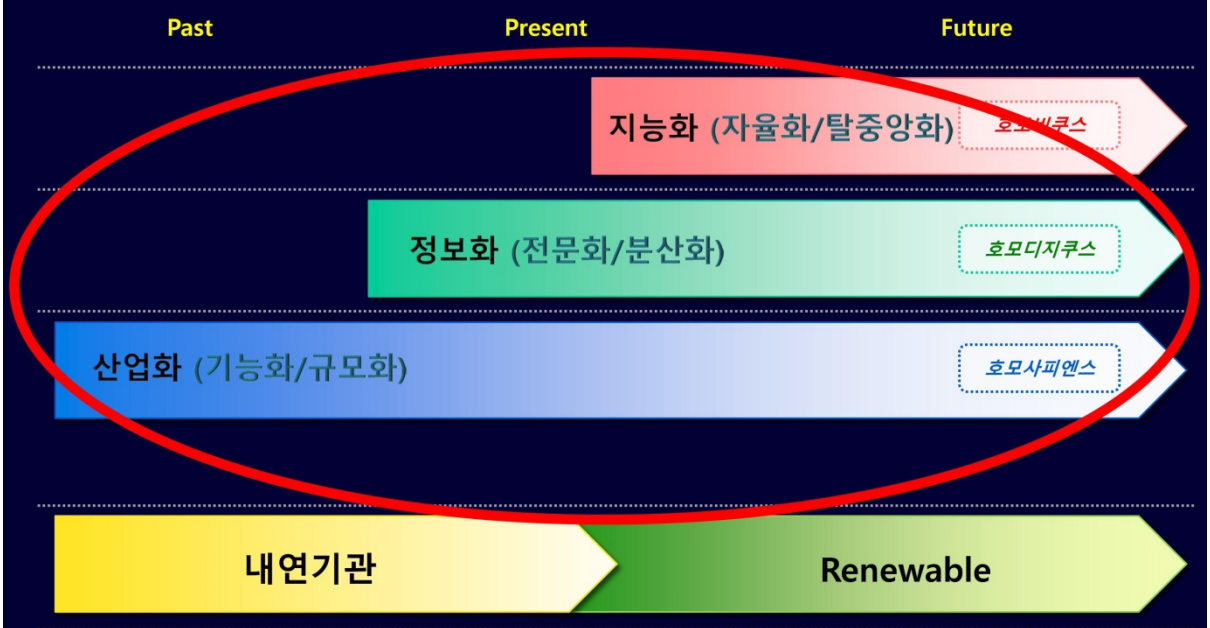
Siti hajin@hajin.com



Siti hajin@hajin.com

Siti hajin@hajin.com

Changes in human civilization

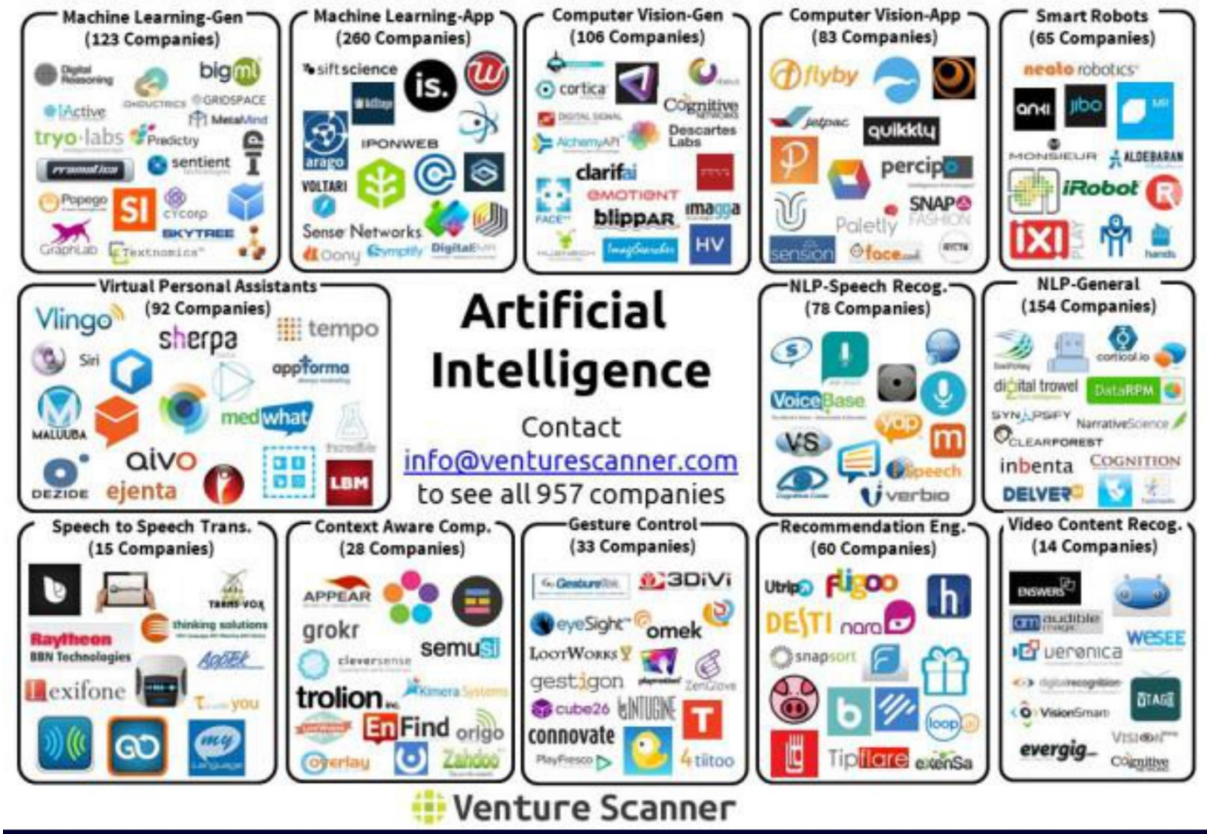


Siti hajin@hajin.com

GETTY IMAGES
Siti
hajin@hajin.com

money slave
Siti
hajin@hajin.com

Siti hajin@hajin.com

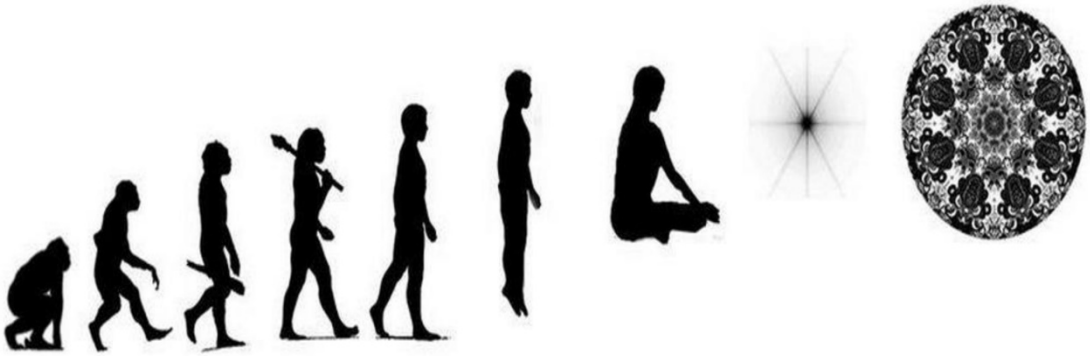


Siti hajin@hajin.com

Siti

hajin@hajin.com

What's Next?



Siti

hajin@hajin.com

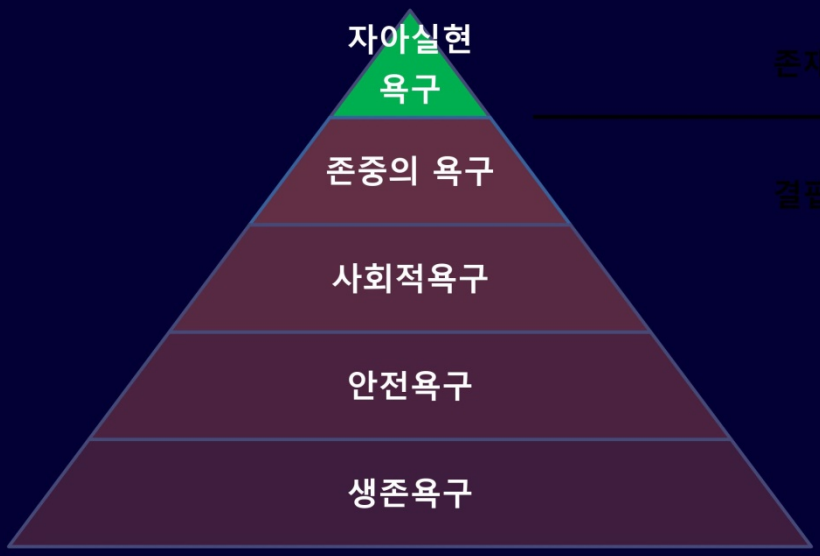
비만, 기아 그리고 기후변화로 멸종의 길로 갈 것인가?

Or

특이점을 극복하고 새로운 인류가 될 것인가?

Intellectual Society (知性社會)

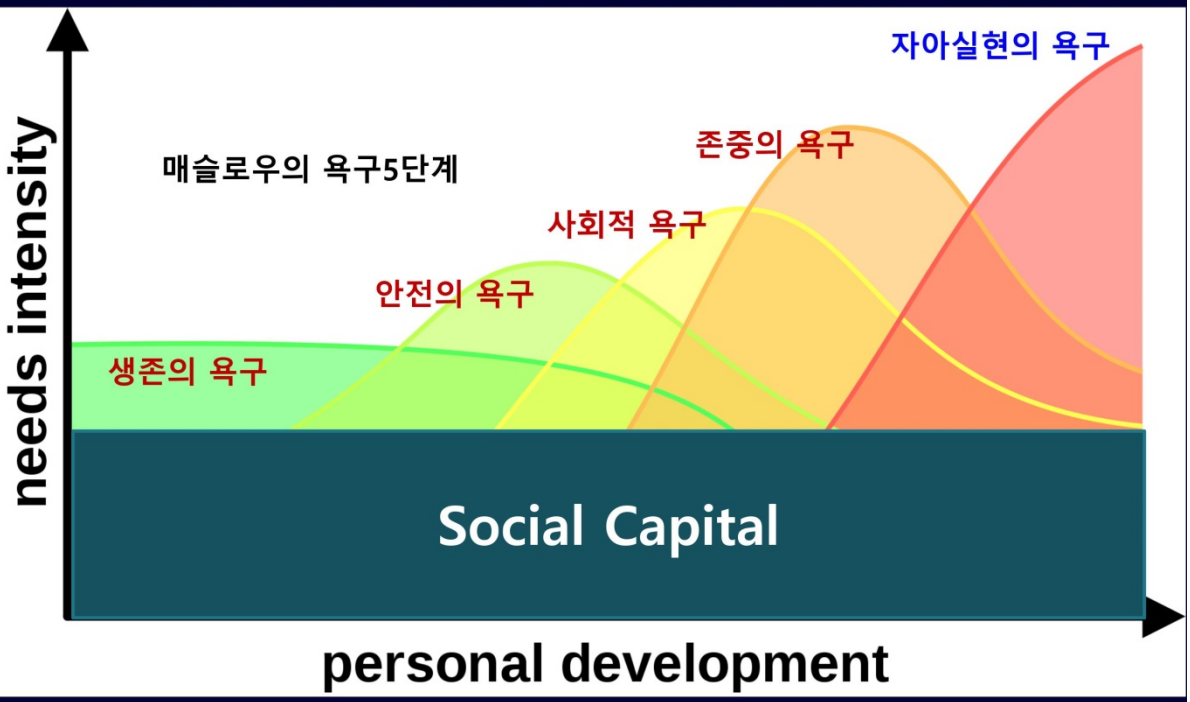
매슬로의 인간욕구 5단계



Siti

hajin@hajin.com

인간의 고도화



Siti

hajin@hajin.com

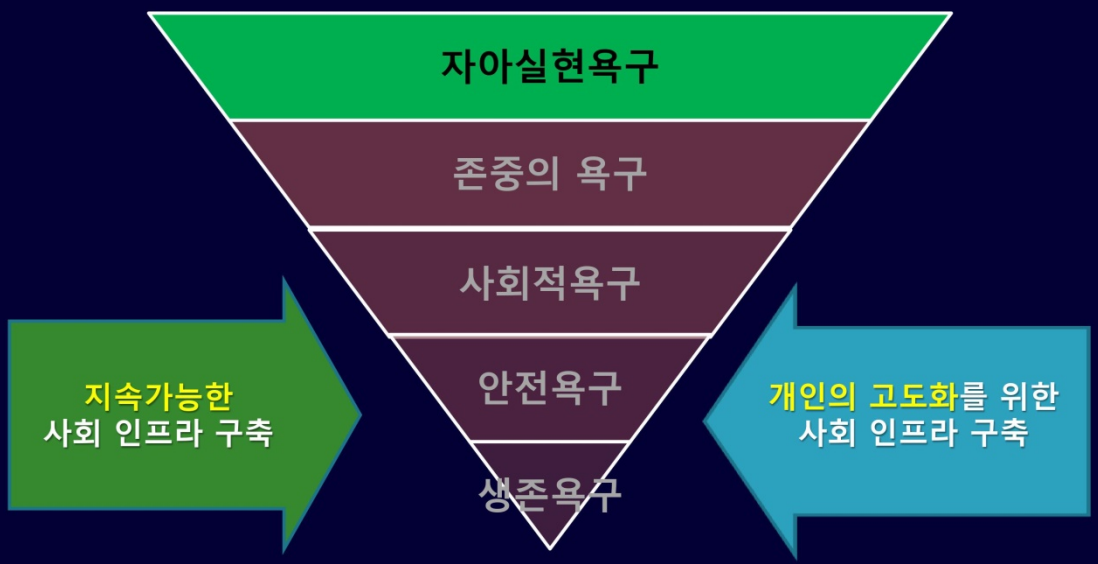
Intellectual Society

가치의 고도화	BlockChain ...
지능노예	AI, Big Data, ...
감각노예	Sensor, Network, ...
근력노예	Engine, ...
환경의 고도화	ESS, Clean Energy ...

Siti

hajin@hajin.com

Intellectual Society



Siti

hajin@hajin.com

Intellectual Society

가치의 고도화 | BlockChain ...

- 비전, 의지 등이 중요한 변수
- 절대적 시간 투자가 필요
- 일과 놀이의 혼재

- 지속가능성이 중요한 변수
- 스마트기술에 의한 최적화
- 자급자족 기반 마련이 중요

환경의 고도화 | ESS, Clean Energy ...

Siti hajin@hajin.com

知性 '답 없는 물음'을 끊임없이 되물으며, 자연과 인류에 기여하고자 하는 의지다.

知慧 '말로 드러나지 않는 것', '경험'으로부터 배우는 것이다.

知能 '답이 있는 물음'에 대해 재빠르게 답을 찾아내는 능력이다.

知識 '말로 드러나는 것'이며, '책'으로부터 배우는 것이다.

Siti hajin@hajin.com

지성은 세상에 대한 사랑과 책임을 지는 주인의 모습이다.

기계가 엄청난 지식을 가지고 빠르게 정답을 외친다고, 지성을 가질 수는 없다.

지성은 답이 없는 질문을 통해 세상의 문제를 해결하고 기여하고자 끊임없이 노력하는 과정이다.

또한 지성은 집단적 교류를 통해 불가능해 보이는 인류의 문제를 해결한다.

지성이야 말로 인간욕구의 마지막 단계인 자아실현을 위한 원동력이라고 할 수 있다.

Siti

hajin@hajin.com

Intellectual Society

고도화된 개인의 가치를 중심의 **새로운 경제시스템**

각자의 개성을 강화하는 **지아실현 교육**

자아실현을 위한 자급자족 기반의 **새로운 주거환경** (SiTi)

블록체인과 4차 산업혁명 기술

Siti

hajin@hajin.com

New economic system

Money-Oriented Society

Siti

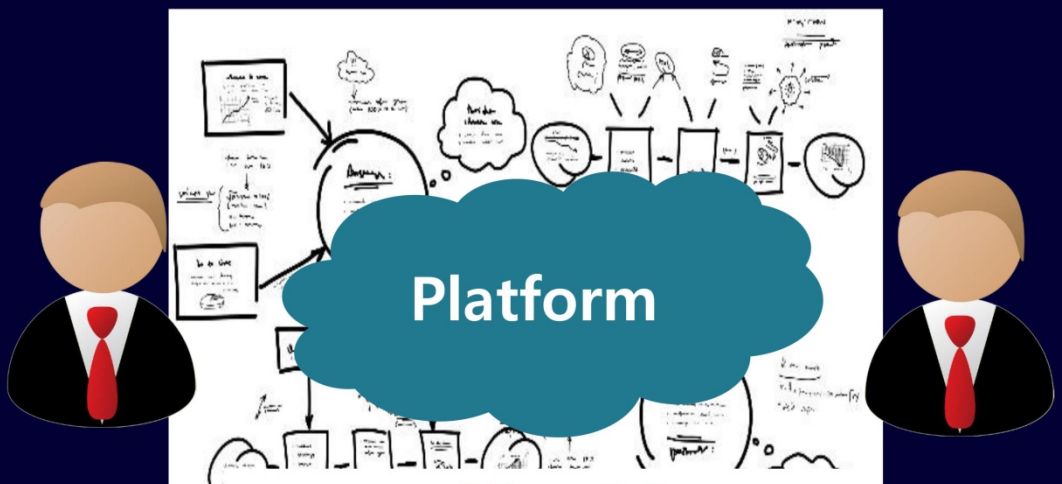
hajin@hajin.com

Money-Unused Society

Siti

hajin@hajin.com

Intellectual Society



Personal Value

Personal Value

- Micro Job
- Micro Transaction
- Barter System
- Programmable Economy

Siti

hajin@hajin.com

What is the next Tech

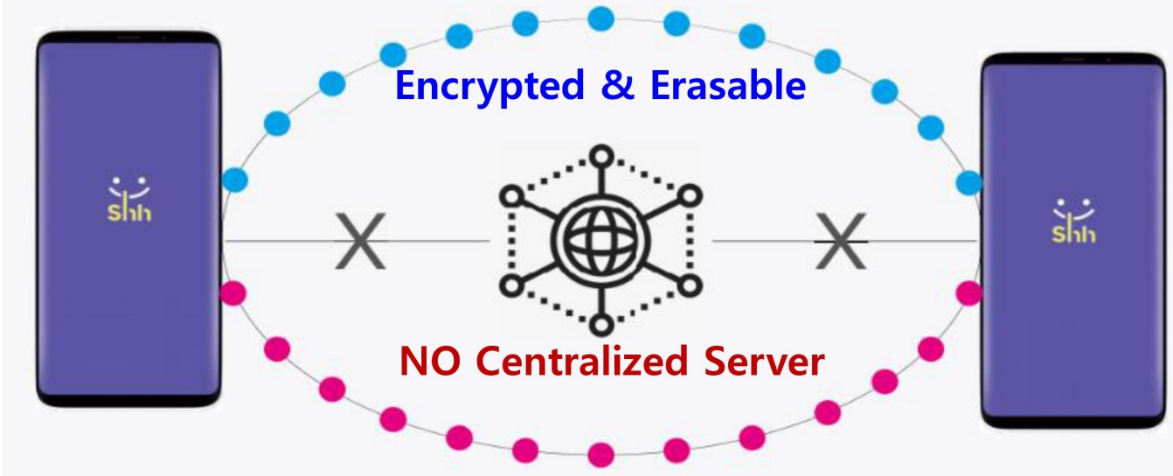
- Value of Internet
- Blockchain Messenger
- Atomic Swap
- Decentralized Database
- Programmable Money

Siti hajin@hajin.com

Blockchain Messenger

Shh Messenger

PAXNet



Siti hajin@hajin.com

Shh Messenger

PAXNet

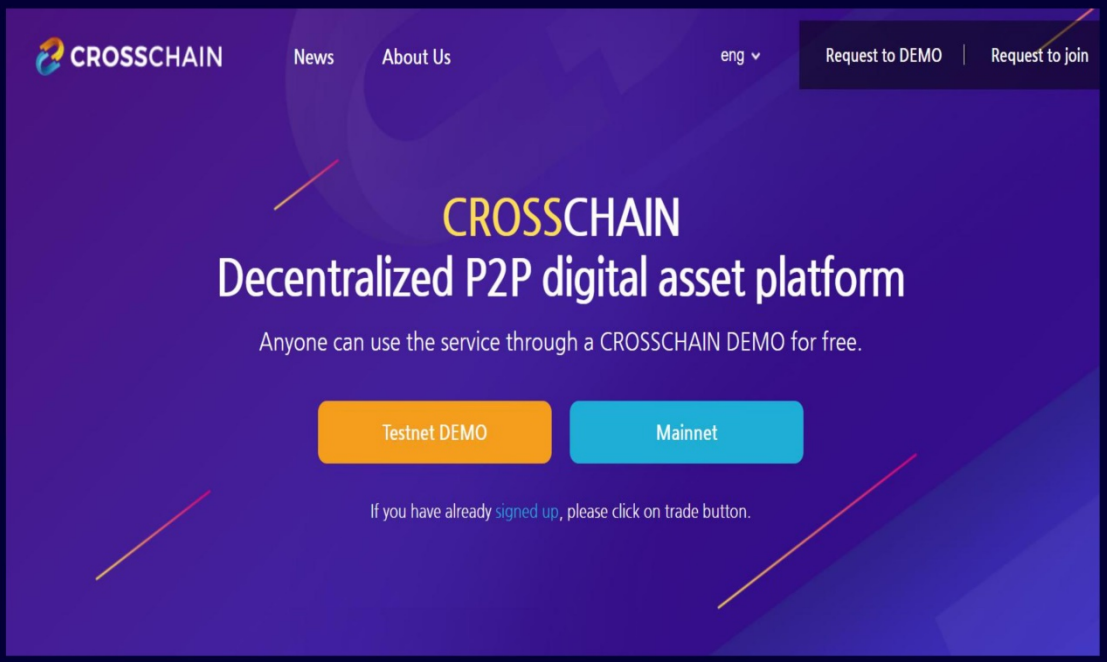
1. No Central Server
2. Permenant Deletes
3. OCaml Language Used
4. Encrypted Videos & Photos

5. Secret Actions
6. Limited View Points
7. Screen Capture disabled
8. Changing Other's profile photos

Siti

hajin@hajin.com

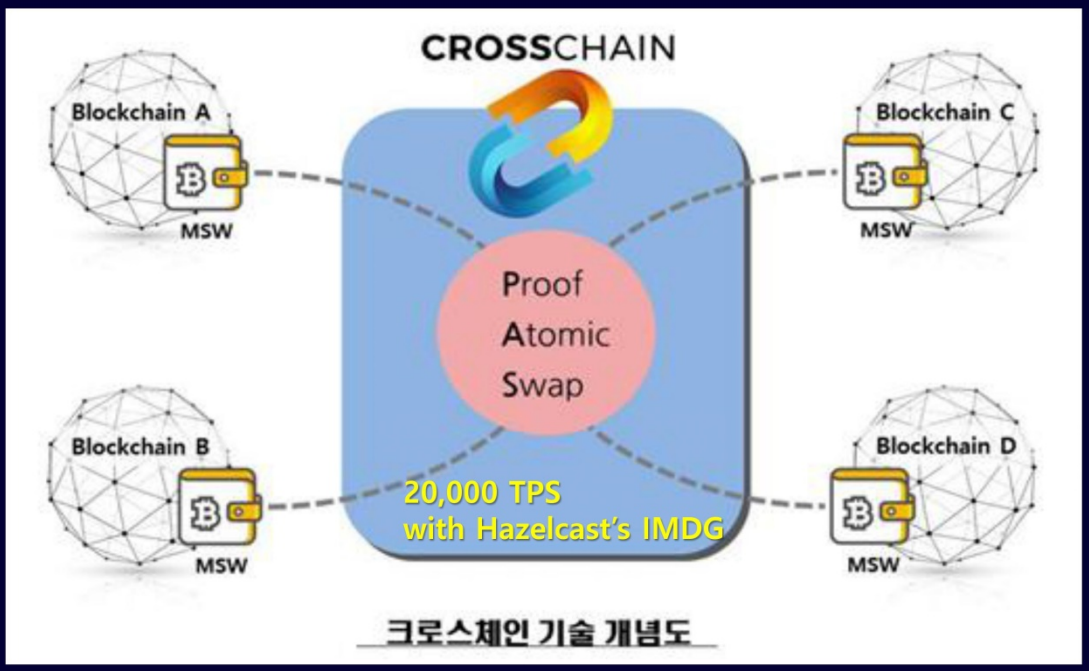
Atomic Swap



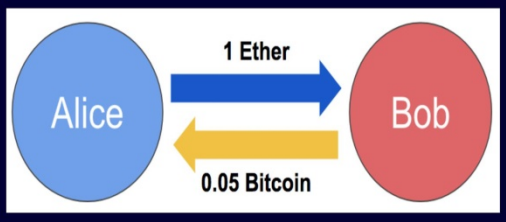
Siti

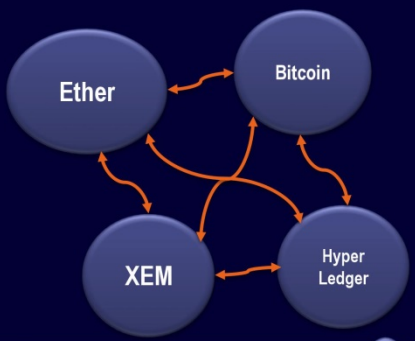
hajin@hajin.com

Atomic Swap



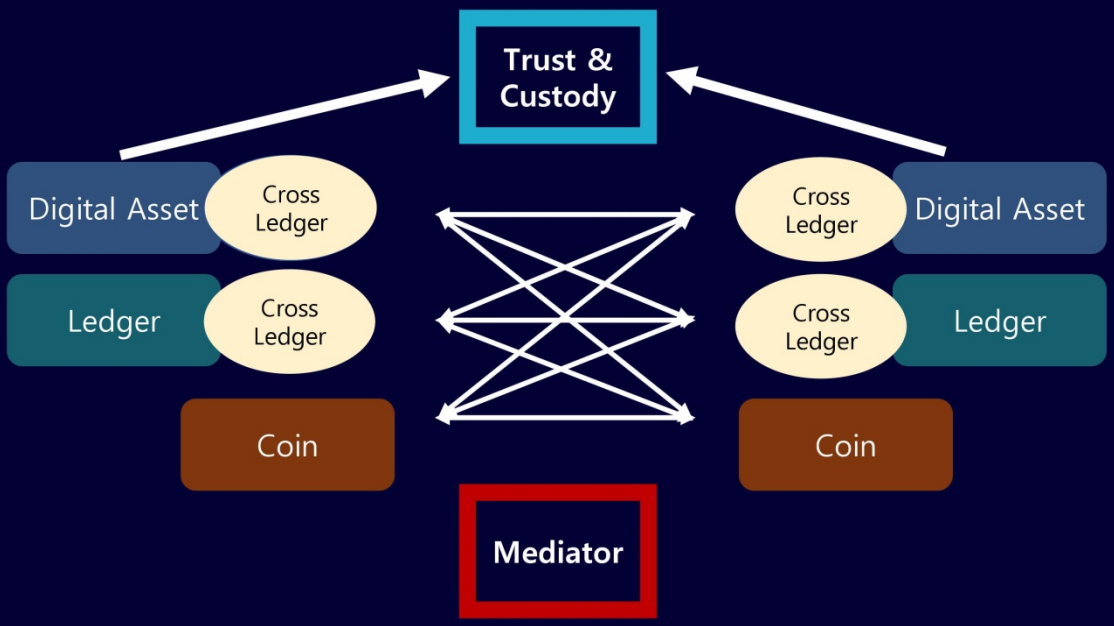
Atomic Swap





- No Double Spending Transaction
- Value evaluation between related parties.
- Very Low Transaction Fee
- Perfect **P2P Barter Transaction**

CrossChain Eco System



Decentralized Database

BaaSid™

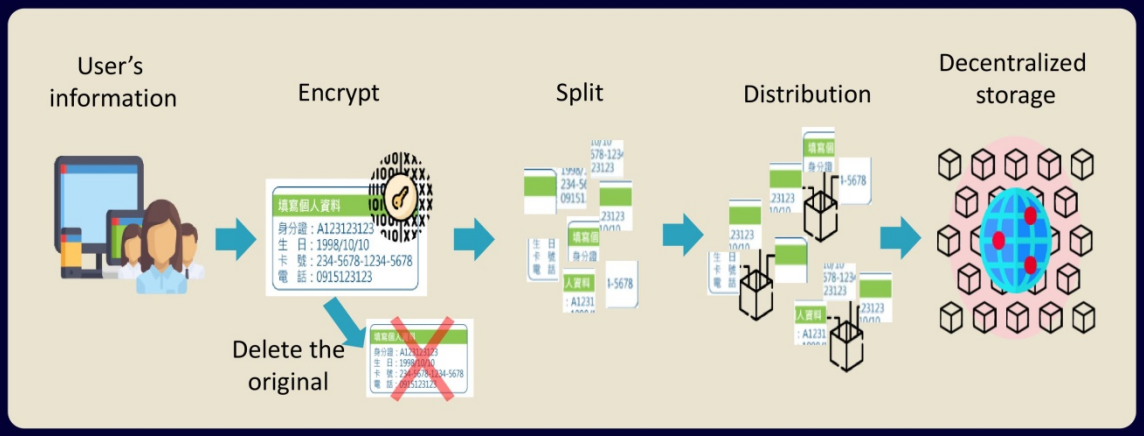
The world's first decentralized security verification blockchain application

BaaSid.com

Siti

hajin@hajin.com

BaaSid De-identification Protection



- Eliminate the possibility of data restoration
- Eliminate the possibility of re-identification of data

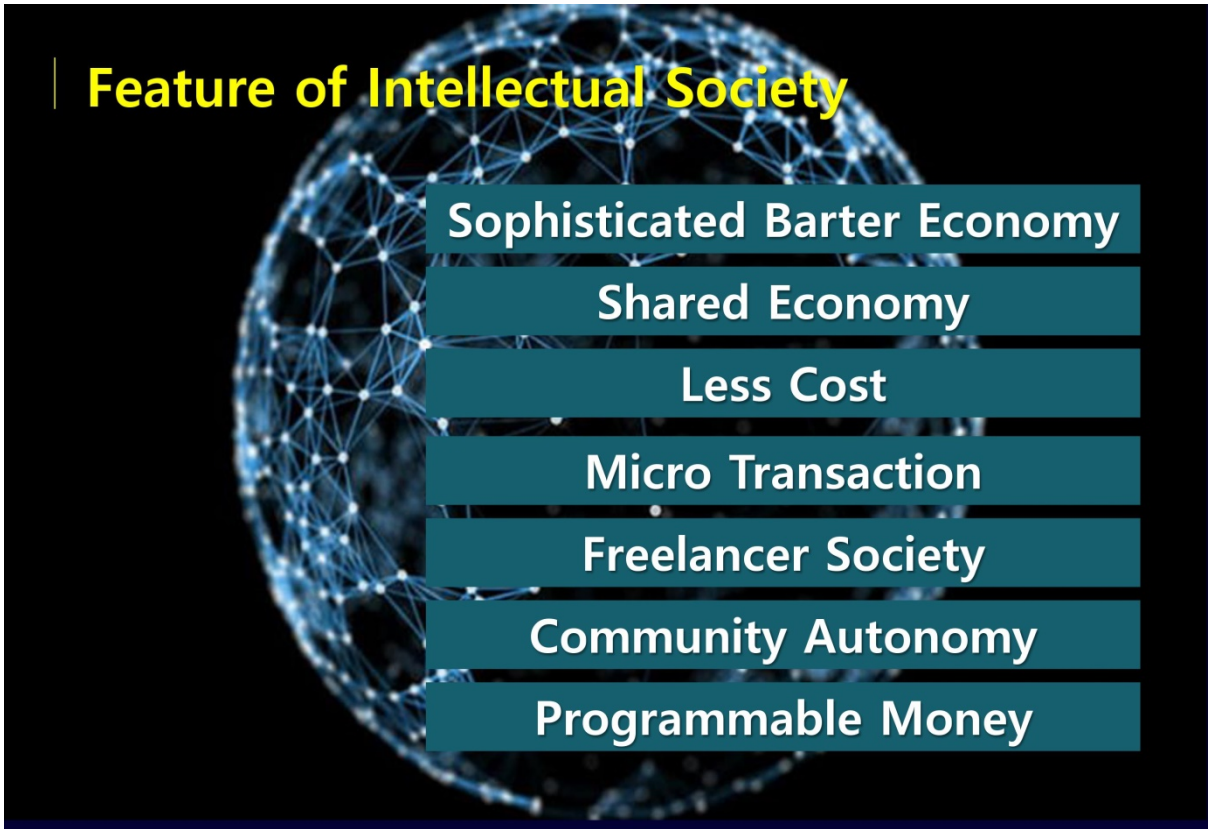
Siti

hajin@hajin.com

Feature of BaaSid

Siti

hajin@hajin.com


Feature of Intellectual Society
Sophisticated Barter Economy
Shared Economy
Less Cost
Micro Transaction
Freelancer Society
Community Autonomy
Programmable Money
Siti
hajin@hajin.com

WISA
World Intellectual Society Alliance
Siti
hajin@hajin.com

비전) 자연과 공존하며 인류공영에 이바지 한다.

육성) 지성인을 위한 새로운 교육 및 경제시스템을 구축한다

협업) 기존 질서가 새로운 질서를 지원하도록 해야 한다.

안정) 모든 사람들의 기본생활 안정을 최우선시해야 한다.

제도) 집단지성에 의한 플랫폼 거버넌스를 창조해야 한다.

Siti

hajin@hajin.com

Intellectual

Smart Human Siti

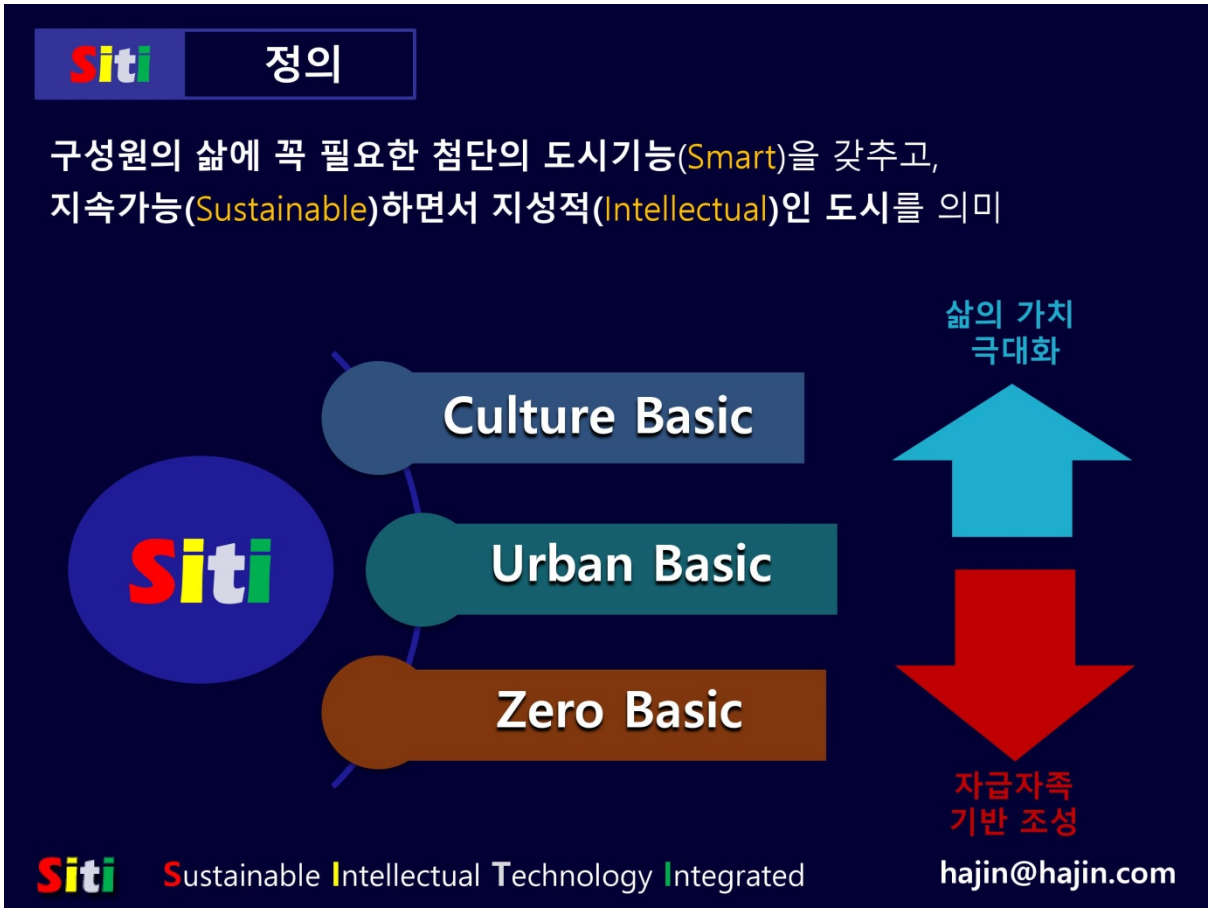
Siti hajin@hajin.com

기존 도시의 문제점

- 물, 에너지 등 자급자족 기반 취약
- 공해, 교통, 주거, 안전 등의 문제
- 직주 근접이 어렵고 높은 생활비 부담
- 공동체 붕괴로 행복지수 저하

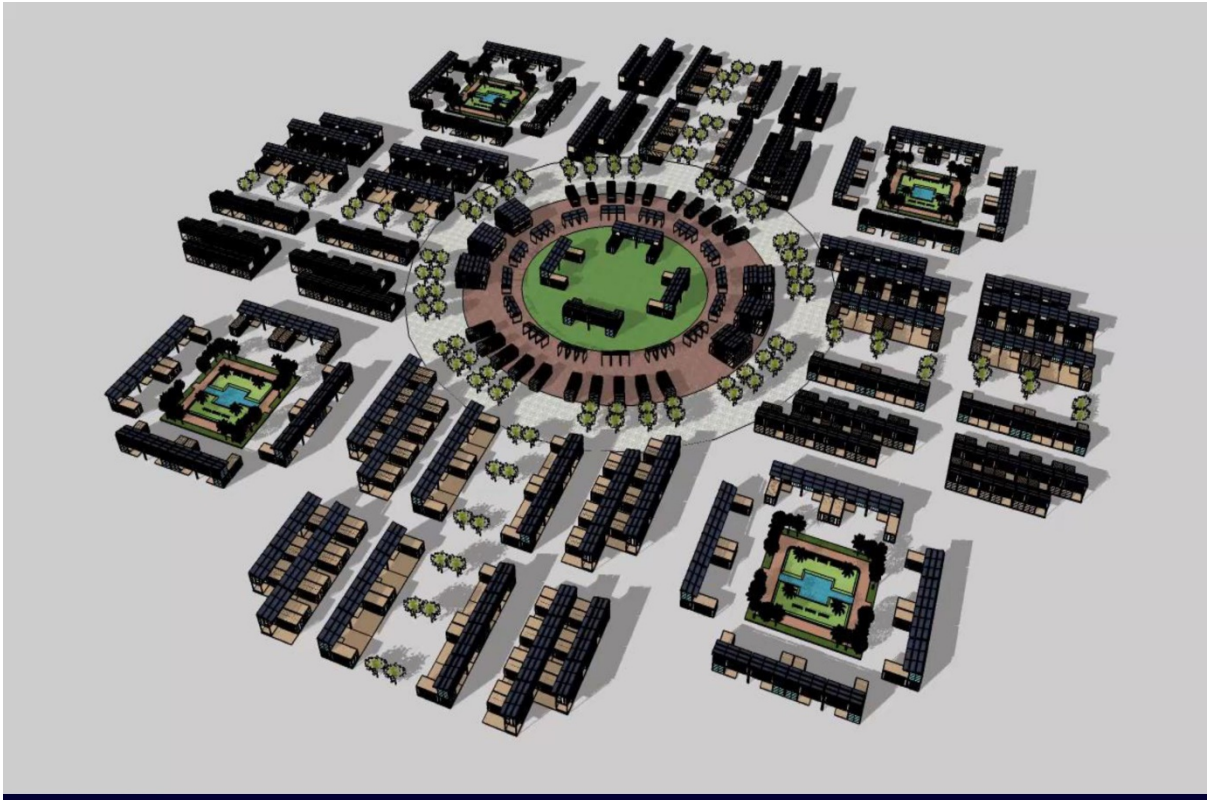
Siti hajin@hajin.com

삶과 주거환경의 미래!
첨단자족도시 Siti
The Future of Human Life and Residential Environment! The High-Tech Self-Sufficient City
자급자족 기반이 마련되고
자아실현을 위한 일과 공동체가 있는
Siti Sustainable Intelligent Technology Integrated
hajin@hajin.com


Siti 정의
구성원의 삶에 꼭 필요한 첨단의 도시기능(Smart)을 갖추고,
지속가능(Sustainable)하면서 지성적(Intellectual)인 도시를 의미
삶의 가치
극대화
Culture Basic
Siti
Urban Basic
Zero Basic
자급자족
기반 조성
Siti Sustainable Intellectual Technology Integrated
hajin@hajin.com

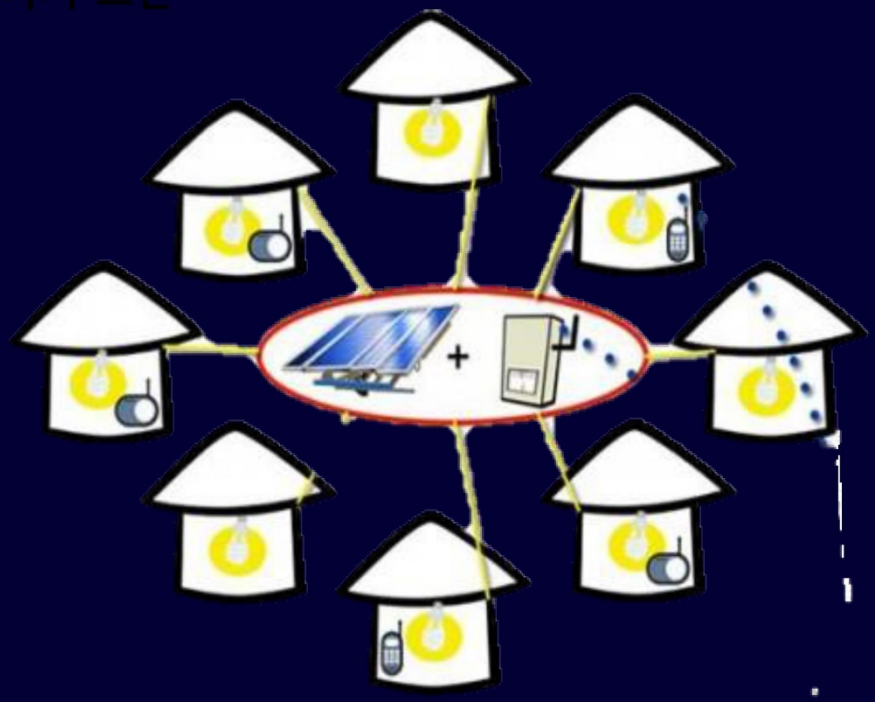
BLOCKCHAIN
Internet
ESS
Siti
hajin@hajin.com

Siti
hajin@hajin.com



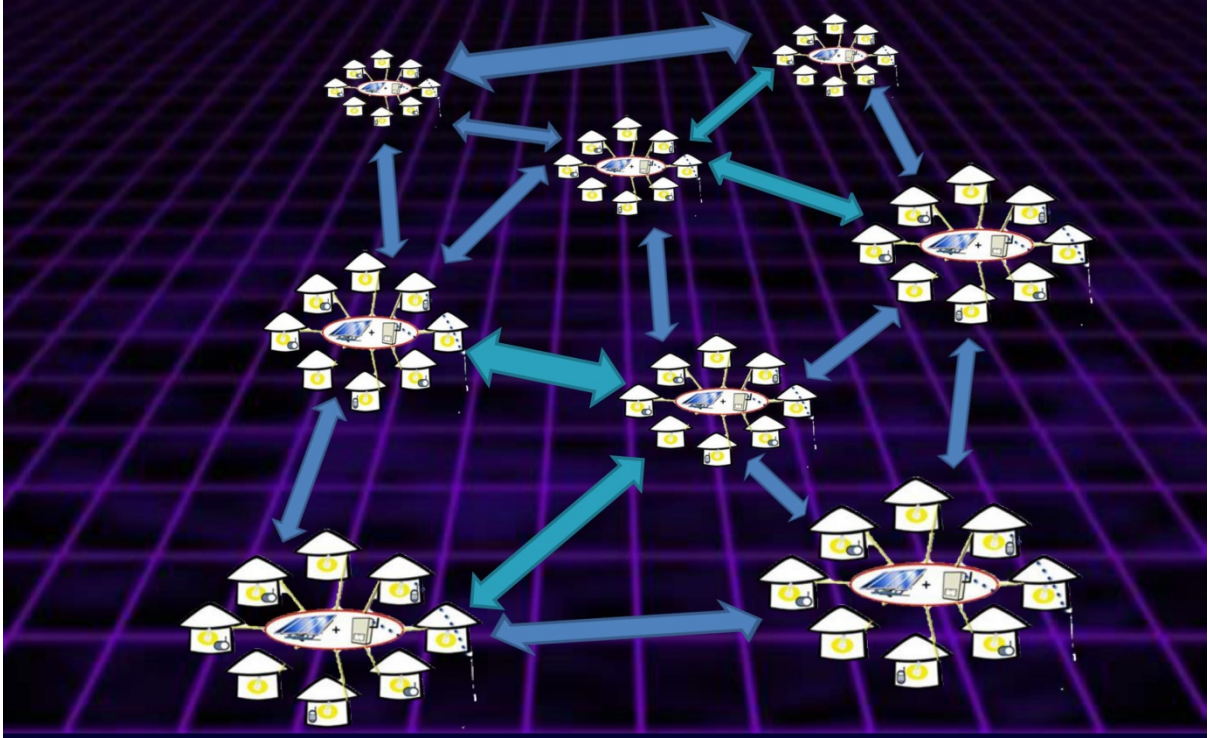
Siti hajin@hajin.com

잉여가치 교환



Siti hajin@hajin.com

잉여가치 교환



Siti hajin@hajin.com

Zero Basic

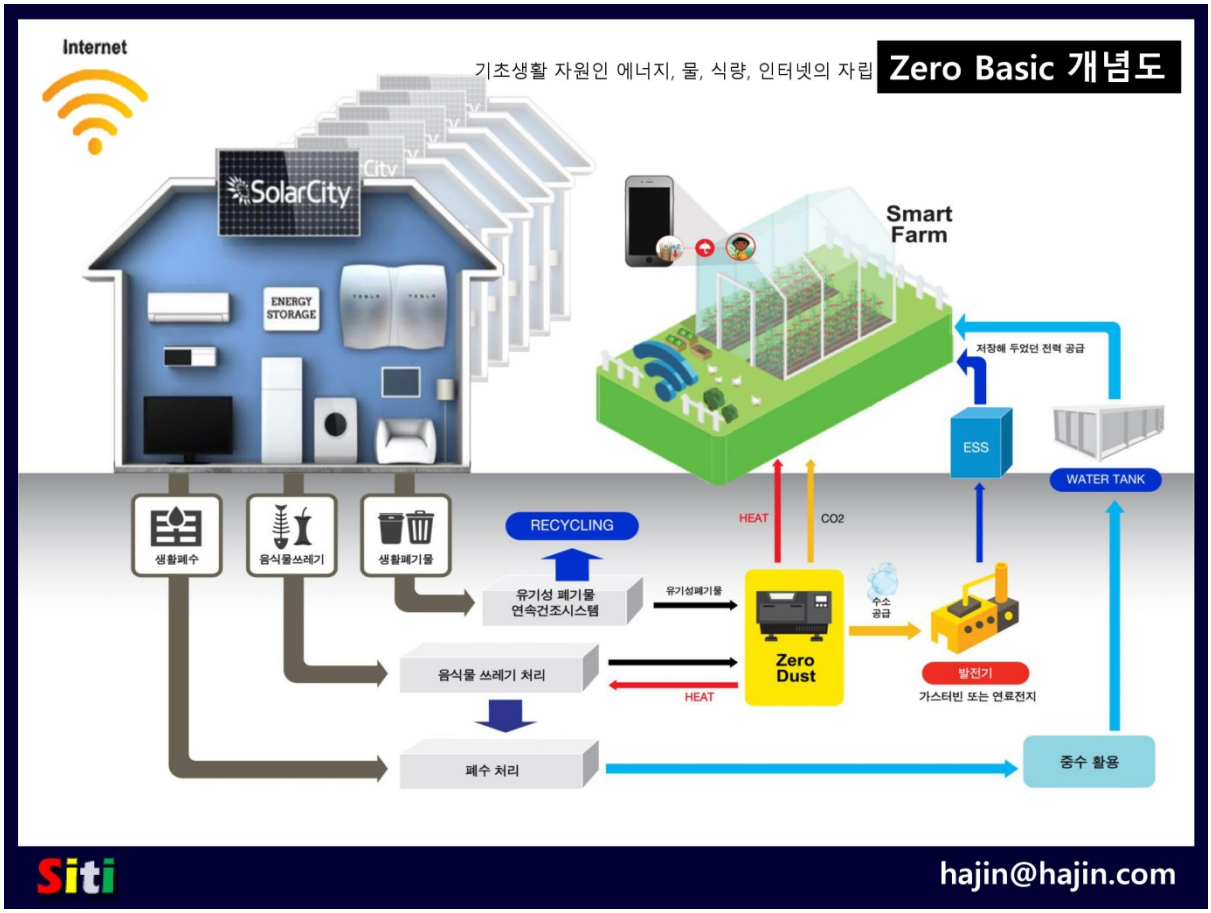
- 최소의 비용으로 자급자족 기반 마련
- 투자비 + 운영비 를 최소화

Zero Basic

Water | Energy | Food | Zero Waste | Internet

신재생에너지, 스마트 팜, 담수화, 인터넷 등의 기반 기술에 의한

Siti hajin@hajin.com


Internet
기초생활 자원인 에너지, 물, 식량, 인터넷의 자립
Zero Basic 개념도
SolarCity
ENERGY STORAGE
Smart Farm
저장해 두었던 전력 공급
ESS
WATER TANK
생활폐수
음식물쓰레기
생활폐기물
RECYCLING
HEAT
CO2
유기성 폐기물 연속건조시스템
유기성폐기물
수소 공급
Zero Dust
발전기
가스터빈 또는 연료전지
음식물 쓰레기 처리
HEAT
폐수 처리
중수 활용
Siti
hajin@hajin.com

Siti
hajin@hajin.com

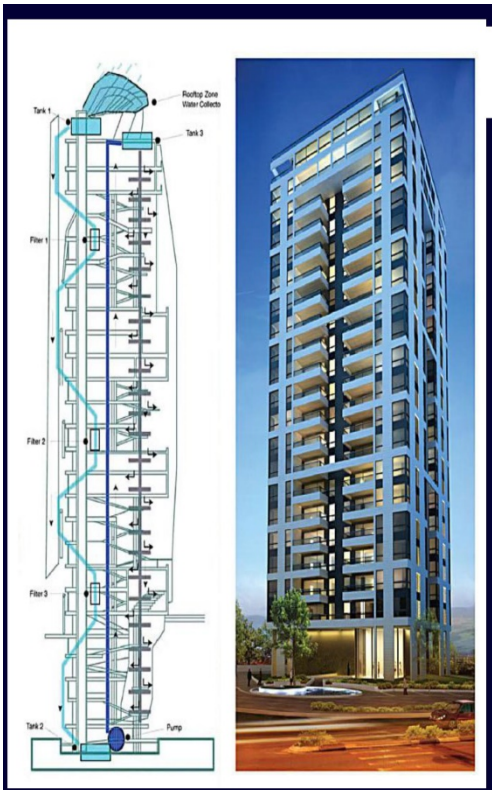
유엔개발계획(UNDP)보고서에 따르면 전 세계 도시 농부의 수는 8억 명. 2013년 기준 세계인구의 11%정도다. 이 중 6억 명은 자체 소비를 위해 도시에서 농사를 짓는다.

5㎡ 규모 발코니에서 1년간 식료품 83㎏을 수확하고 있는 영국의 도시농부 마크 스미스의 도시텃밭

Siti hajin@hajin.com

Siti hajin@hajin.com

Siti hajin@hajin.com



watergen

온도26.7도, 60% 습도에서 하루에 3,000리터 생산

350Wh/liter, 약 2-4센트/리터 소요

Siti hajin@hajin.com

Siti hajin@hajin.com

Urban Basic

- 도시 기능을 내재화 (인터넷 기반의 원격 서비스)
- IoT 기반의 스마트시티 구현 (비용 최소화)

Urban Basic

교육 | 의료 | 제조 | 교통 | 안전

인공지능, 드론, 3D프린터, IoT, 빅데이터, 등 각종 기반 기술에 의한

Siti hajin@hajin.com

Siti hajin@hajin.com

미국의 신생 대학이자 교육 스타트업, 미네르바스쿨 :

합격률 1.9%. 학생은 306명에 불과, 전 세계 167개국 1만6000여 명의 지원,
미 하버드대(5.2%), 스탠퍼드대(4.7%)보다 더 '바늘구멍'이다.

Siti hajin@hajin.com

healthspot
healthspot
station
Siti
hajin@hajin.com

Leah Smith
5' 6"
110
120
75
69
101°
99
Dr. Jenkins
Siti
hajin@hajin.com

Siti hajin@hajin.com

Culture Basic

- 자아실현을 위한 비즈니스 필요
- 행복을 위한 공동체 및 활동 (품앗이, 나눔, 공유경제)

Culture Basic

Business | Community | Sharing

품앗이, 플랫폼, 공유 경제, 나눔 등의 문화를 통한

Siti hajin@hajin.com

Business
Community
Siti
hajin@hajin.com

Sharing(품앗이)
Siti
hajin@hajin.com

Co-Work space
Siti
hajin@hajin.com

Co-Dining
Siti
hajin@hajin.com

Siti hajin@hajin.com

Siti hajin@hajin.com

M-ZERO FARM & GARDEN

M-ZERO Farm

양질의 토양에서 우리의 종자를 유기농법으로 재배하는 M-ZERO Farm
ICT 기술을 적용하여 성장 모니터링 및 알림 서비스 제공

M-ZERO Garden

식용 작물을 활용한 디자인 가드닝으로 경관의 미를 더하다.
모듈 구조로 다양한 구조, 장소에 적용 가능

특허청 (주)엠제로랩 kista 한국지식재산전략원 20

Siti hajin@hajin.com

Siti hajin@hajin.com

Siti Factor

Community building for self-actualization

Culture Basic

Business | Community | Sharing

Urban Basic

교육 | 의료 | 산업 | 교통 | 안전

Zero Basic

Water | Energy | Food | Waste | Internet

Siti hajin@hajin.com

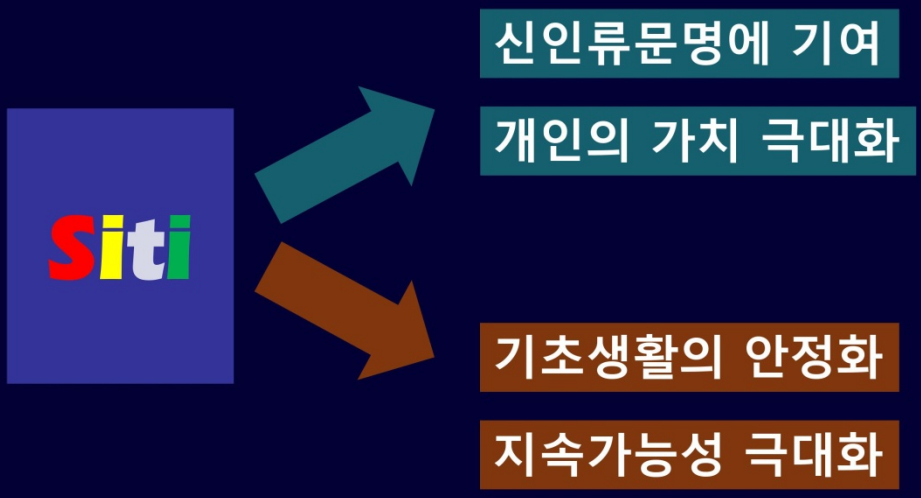
Siti 종류

- Tourist Siti
- Maker Siti
- Blockchain Siti
- Sports Siti
- Corporate Siti
- Artist Siti
- Campus Siti
- Farm Siti

Siti

hajin@hajin.com

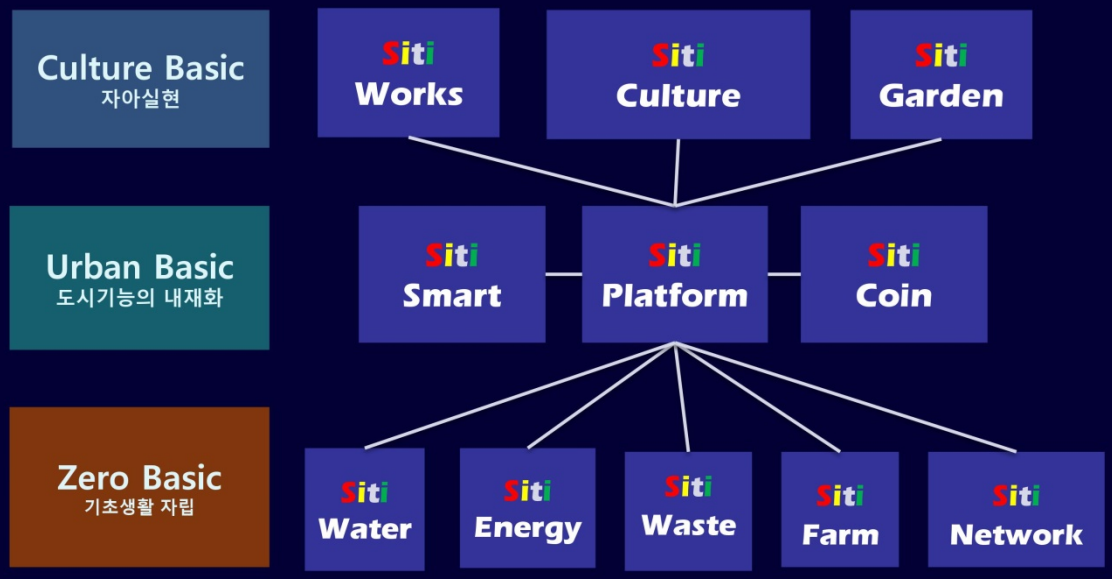
Siti 기대효과



Siti

hajin@hajin.com

Siti Business



Siti

hajin@hajin.com

How to make the Siti

Siti

hajin@hajin.com

Siti 고려사항

Culture Basic
자아실현

- 어떤 구성원이 사는 도시인가?
- 자아실현을 위해 필요한 것은?
- Siti 의 주수익원은 무엇인가?

- **자아실현**
- **공동체 활성화**
- **직주근접**
- **기초생활의 안정**

Urban Basic
도시기능의 내재화

- 기존의 도시기능을 융합하고 최적화
- 최고 수준의 서비스

Zero Basic
기초생활 자립

- 기초비용의 최소화
- 도시기반의 통합화

Siti

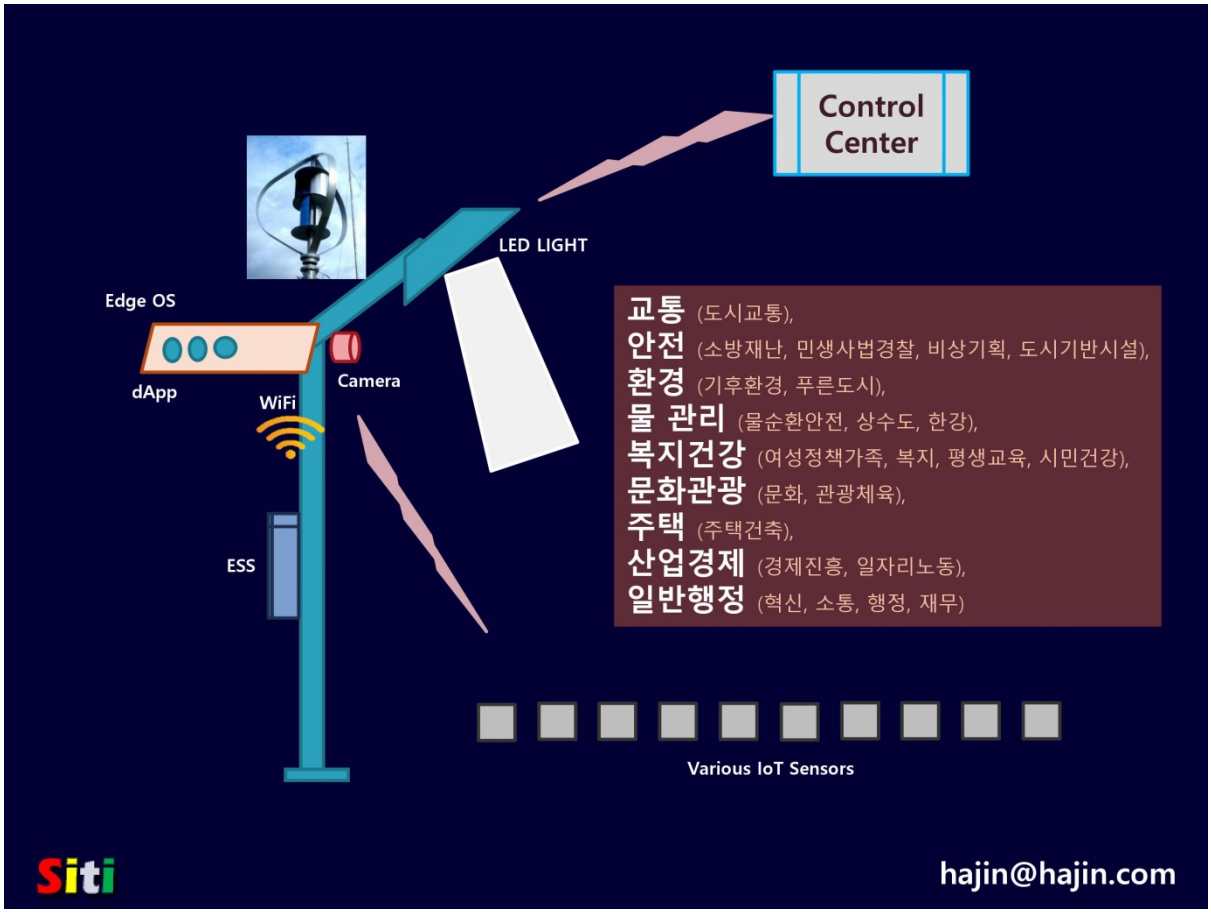
hajin@hajin.com

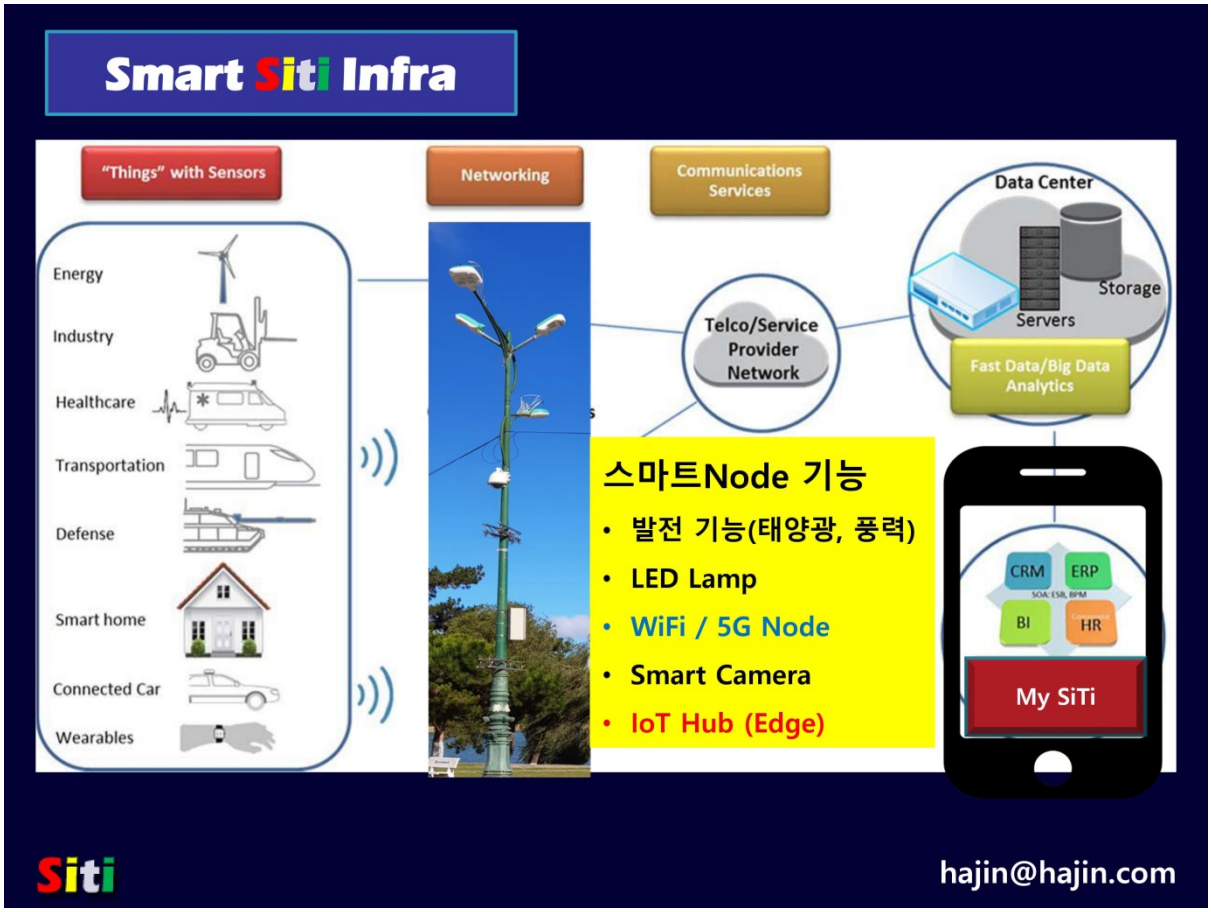
Smart Human Siti

구성원들의 **행복한 삶**을 위한 요소들만
선별적으로 채택한 최소비용의 최적화도시를 지향

Siti

hajin@hajin.com


Control Center
LED LIGHT
Edge OS
dApp
WiFi
Camera
ESS
교통 (도시교통),
안전 (소방재난, 민생사법경찰, 비상기획, 도시기반시설),
환경 (기후환경, 푸른도시),
물 관리 (물순환안전, 상수도, 한강),
복지건강 (여성정책가족, 복지, 평생교육, 시민건강),
문화관광 (문화, 관광체육),
주택 (주택건축),
산업경제 (경제진흥, 일자리노동),
일반행정 (혁신, 소통, 행정, 재무)
Various IoT Sensors
Siti
hajin@hajin.com


Smart Siti Infra
"Things" with Sensors
Networking
Communications Services
Data Center
Storage
Servers
Fast Data/Big Data Analytics
Telco/Service Provider Network
Energy
Industry
Healthcare
Transportation
Defense
Smart home
Connected Car
Wearables
스마트Node 기능
• 발전 기능(태양광, 풍력)
• LED Lamp
• WiFi / 5G Node
• Smart Camera
• IoT Hub (Edge)
CRM
ERP
BI
HR
My SiTi
Siti
hajin@hajin.com

Pocket Siti

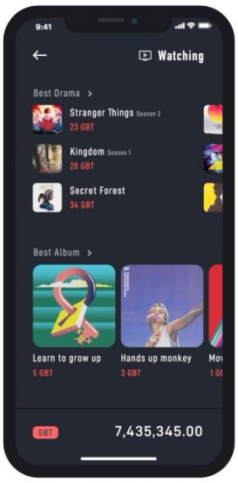
주민광장 | 벼룩시장 | 구인/구직 | 타임뱅크

보관소 | 동호회 | 주민센터 | 공유센터

지역화폐 | 투표시스템 | 빅데이터 | 블록체인 | 인공지능 | IoT

Siti

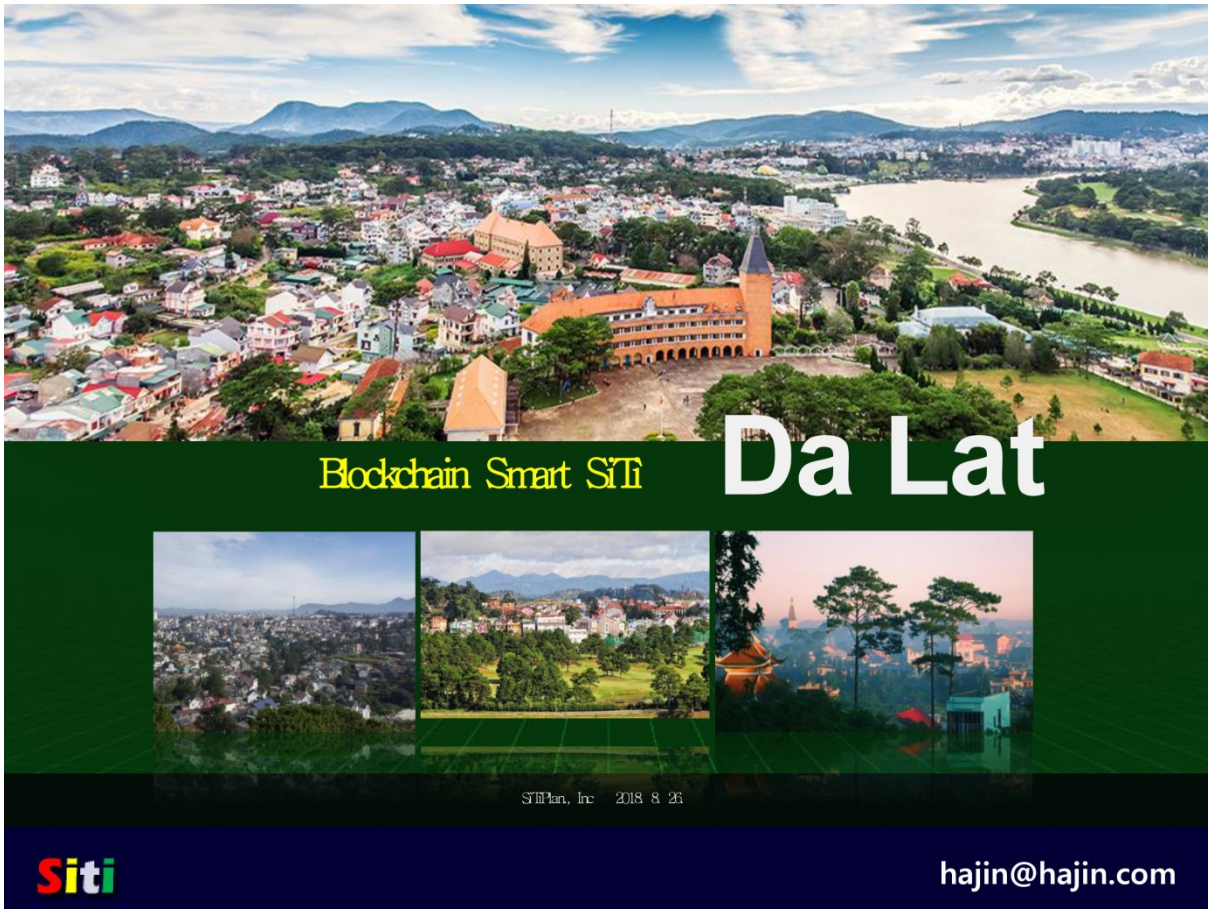
hajin@hajin.com



Pilot Project

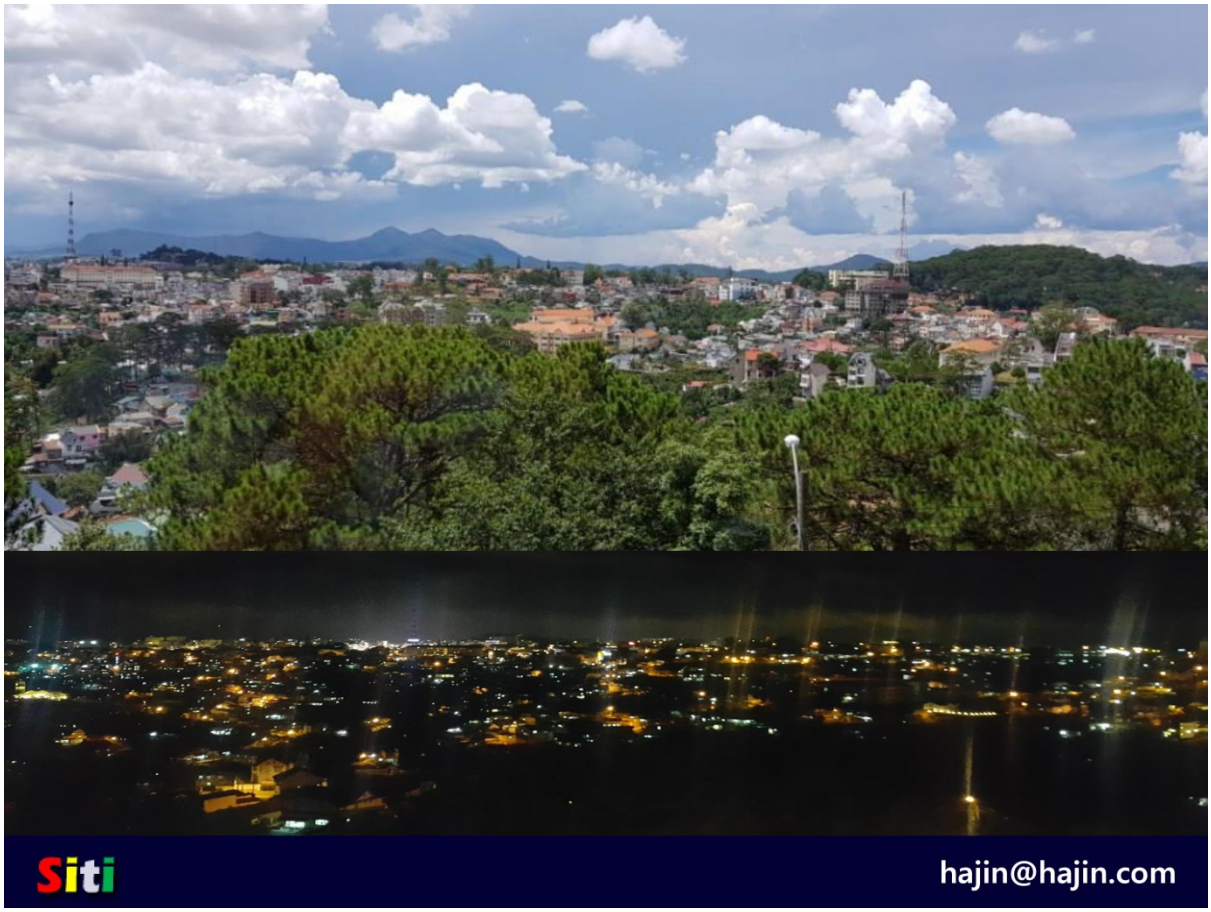
Siti

hajin@hajin.com


Blockchain Smart SiTi
Da Lat
SiTiFan, Inc 2018. 8. 26
Siti
hajin@hajin.com

다낭
Đà Nẵng
태국
어번 래
차따아니
나콘라차시마
부리람
베트남
방콕
Pleiku
시엠레아프
꾸이년
Tp. Qui Nhơn
파타야
라용
캄보디아
짠타부리
나짱
Tp. Nha Trang
뜨랏
프놈펜
200Km
달랏
Tp. Đà Lạt
호치민
Hồ Chí Minh
1500M 고지대라
항상 봄인 기후 및 청정지역
붕따우
Tp. Vũng Tàu
껀터
Cần Thơ
타이 만
Google
Siti
hajin@hajin.com

International Tourist & Academy City Dalat
▪ 컨벤션, 의료시설, 메이커스와 오피스빌딩, 레지던스호텔, 공연장, 그리고 블록체인대학, 국제 초중고등학교, 문화예술대학, IT대학 단기연수와 타운하우스 등이 있는 외국인이 방문하고 싶어하는 명품 도시
Luxury Agricultural City Dalat
(ex 세계 Coffee의 명품 주요 원산지)
▪ 커피 파크를 도시에 품고 있어 현재 5백만에 이르는 관광객에게 놀거리 즐길거리, 먹거리를 제공하는 다양한 엔터테인먼트가 있는 고급 관광지
Asia Blockchain Mecca Dalat
▪ 싱가포르, 마닐라, 홍콩, 방콕 등 주변 도시 중심에 있는 달랏, IT분야의 사람들이 모여 컨퍼런스도 하고 또 여러 기업들이 연구하는 비즈니스 도시
Beijing
Incheon
Tokyo
New Delhi
Manila
Bangkok
Da Lat
Kuala Lumpu
Singapore
Jakarta
Canberra
Siti
hajin@hajin.com


Siti
hajin@hajin.com

Siti
hajin@hajin.com

Siti
hajin@hajin.com

HỘI THẢO LẦN THỨ 4
THẢO LUẬN VỀ THỦ TỤC THU HỒI, BỒI THƯỜNG ĐẤT
VÀ CHẾ ĐỘ ĐẤT CÔNG CỦA HÀN QUỐC VÀ VIỆT NAM
제 4차 국제학술회의
(사)한국감정평가학회
제4차 국제학술회의
주 최 : (사)한국감정평가학회, 한국감정평가사협회, 베트남 달랏시
2019. 1. 17 ~ 1. 21
베트남 달랏
Siti
hajin@hajin.com

ĐẢNG CỘNG SẢN VIỆT NAM QUANG VINH MUÔN NĂM
Siti
hajin@hajin.com

Siti hajin@hajin.com

Siti hajin@hajin.com

Siti hajin@hajin.com

Dalat Blockchain Based Smart Town & Foreign Residence Village Masterplan

Project Masterplan by PLANNING KOREA

Siti hajin@hajin.com

Masterplan
Dalat Blockchain Based Smart City
Phase3
Phase2
Phase1
Culture Basic
블록체인 캠퍼스 & 오피스
Culture Basic
Music Street
Urban Basic
Smart Security,
Makers Lab
Residence Area
Culture Basic
호텔 & Convention
Urban Basic
학교, 병원, 상업시설
Culture Basic
Condo (AirBnB)
Zero Basic
Waste to Energy
Zero Basic
Micro Grid
Culture Basic
Token Economy
Project Masterplan by PLANNING KOREA
Siti
hajin@hajin.com

Masterplan
Foreign Residence Village
Shopping Street & Small Houses
Dalat coffee specialty shops.
Korean and Vietnamese restaurants.
Commercial & residential complex
Dalat Coffee House
Project Masterplan by PLANNING KOREA
Siti
hajin@hajin.com

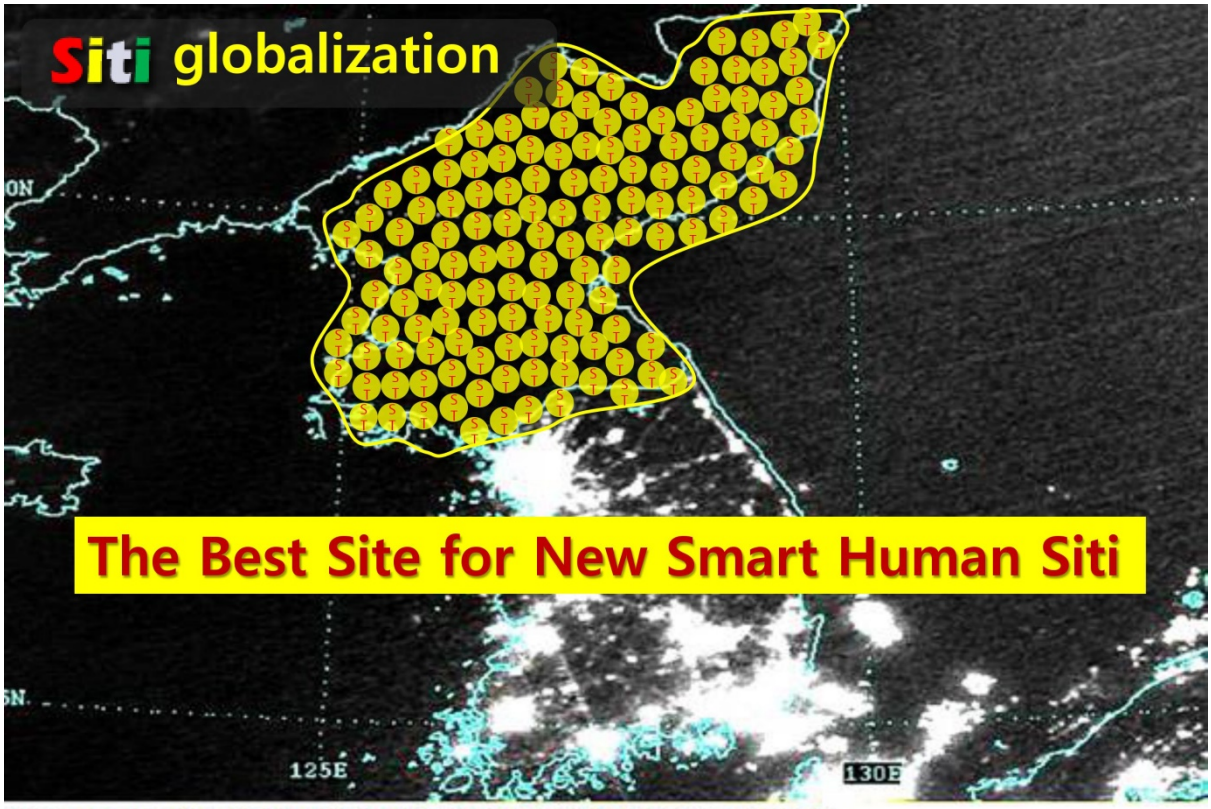
Masterplan
Family Resort
Terrace House
Project Masterplan by PLANNING KOREA
Siti
hajin@hajin.com

Masterplan
Blockchain Campus
Project Masterplan by PLANNING KOREA
Siti
hajin@hajin.com

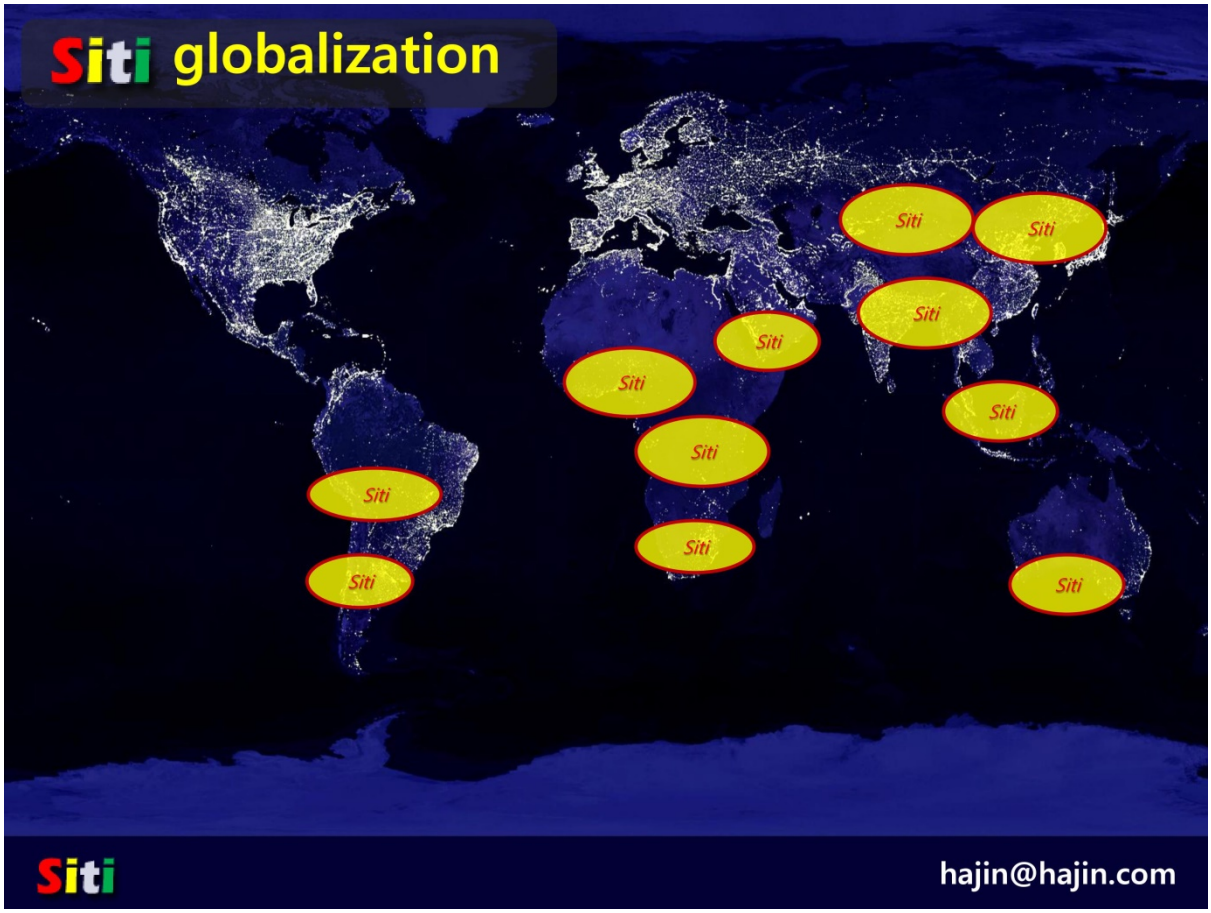
Siti hajin@hajin.com

Siti hajin@hajin.com

Wish list



NASA / The Korean Peninsula at night (Note presence of electricity in South Korea)


Siti globalization
Siti
Siti
Siti
Siti
Siti
Siti
Siti
Siti
Siti
Siti
Siti
Siti
hajin@hajin.com

한국스마트휴먼테크협회
KOREA SMART HUMAN TECHNOLOGY ASSOCIATION
Siti
hajin@hajin.com

▲ 1997년~2018년 – **전세계 58개국**, **314개 도시 공연** 기록
▲ 제주 난타호텔 오픈
▲ 중국 광저우 전용관 개관
▲ 영국 에딘버러 프린지 페스티벌 참가
▲ 아시아 최초 브로드웨이 공연 (뉴 빅토리아 극장)
▲ 아시아 최초 뉴욕 오프 브로드웨이 전용관 설립
▲ 서울 호암아트홀 초연

Siti hajin@hajin.com

Smart Human City

Siti

▲ 2020년~2040년 – **전세계 ??개국**, **???개 도시 건설**
▲ 2020년 베트남 달랏에 스마트 Siti 건설
▲ 2021년 카자흐스탄 슈켄트에 스마트 Siti 건설
▲ Siti가 만들어 낸 일자리 ???
▲ Siti가 줄여낸 탄소감축량 ???
▲ Siti가 만들어낸 행복지수 증가율 ???

Siti hajin@hajin.com

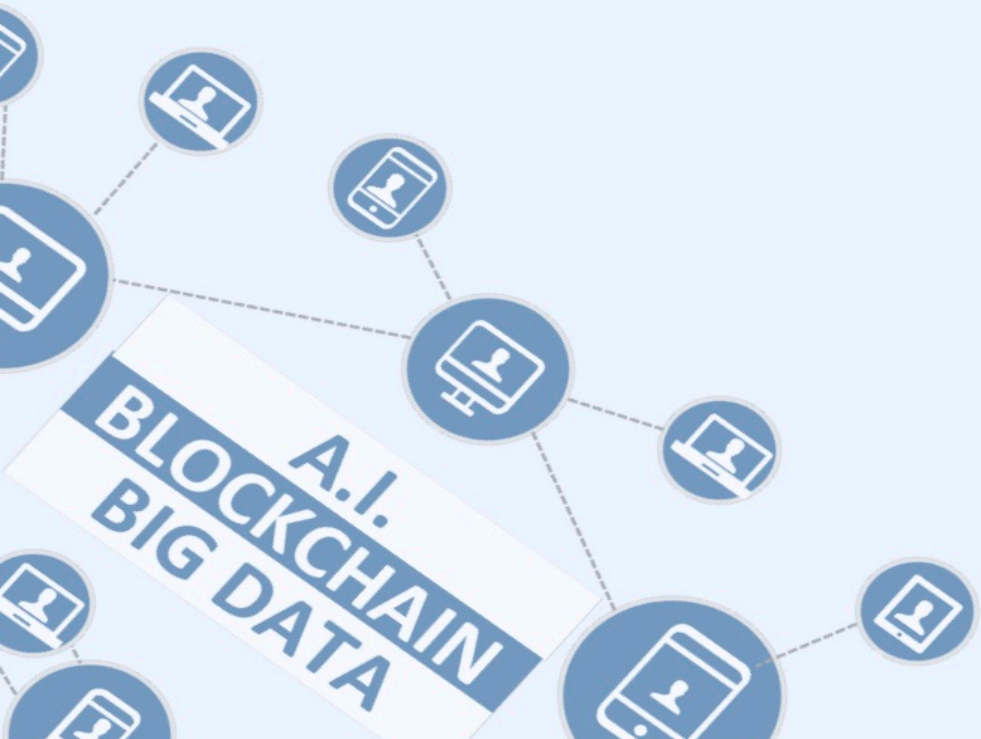
Cảm ơn bạn.
谢谢
Aitäh
Thank you
Danke.
.תודה
Grazie
감사합니다
Merci
ขอขอบคุณ
ありがとうございます。
hajin@hajin.com

8강

Crypto Economy 설계

장 중 혁 이사

(주식회사 아톰릭스컨설팅)



강의 동영상 URL

1 부: https://youtu.be/PMxT94JFXno

2 부: https://youtu.be/IqCdE4sLLEA

3 부: https://youtu.be/l_Kd157Xwml

Crypto Economy 설계란 무엇인가?

May 2019

ATOMRIGS CONSULTING

ATOMRIGS CONSULTING

Company Overview

ATOMRIGS CONSULTING

Crypto Project Builder

- 2018.10.2 설립
- Ethereum Project Builder
- Crypto Custody, L2 Scaling solution, 기타 암호화폐 프로젝트

Crypto Experts

정우현 (Atomrigs)
Co-founder
Managing Partner
CEO

장중혁
Co-founder
Managing Partner

Finance Experts

황현철, Ph.D
Co-founder
Managing Partner

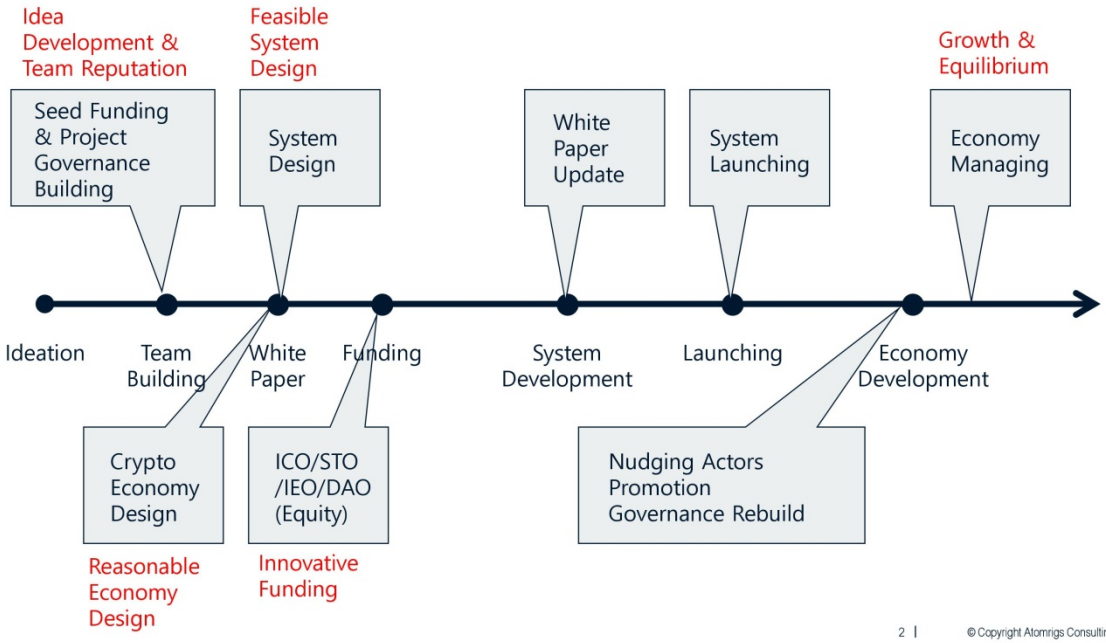
배경일, Ph.D
Co-founder
Managing Partner

Partners

ENTERPRISE ETHEREUM ALLIANCE · Onther Inc. · infobank · IoTrust Delivering Trusted Connectivity · QCA · GAMEPER

© Copyright Atomrigs Consulting Inc. 2018

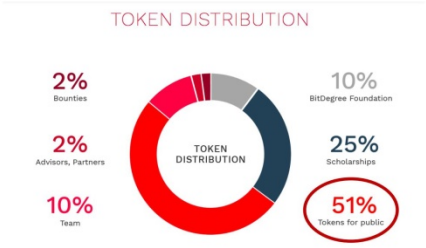
Lifecycle of Blockchain & Crypto Project



 © Copyright Atomrigs Consulting Inc. 2018

ICO/IEO/DAO

Planning



Donation & Reward

Off-chain → **IEO**

Reward Plan : Reward Rate, Lock-up

Anti-Scam Mechanism

On-chain → **DAO**

Reward Plan : ERC20

Anti-Scam Mechanism : ERC20

 © Copyright Atomrigs Consulting Inc. 2018

STO : Security Token Offering

참고 자료 : [증권형 토큰 시리즈] 제1편 증권형 토큰이란 무엇이고, 우리는 왜 증권형 토큰을 파헤치게 되었는가, *디사이퍼 미디엄*, http://bitly.kr/cXpFP

 © Copyright Atomrigs Consulting Inc. 2018

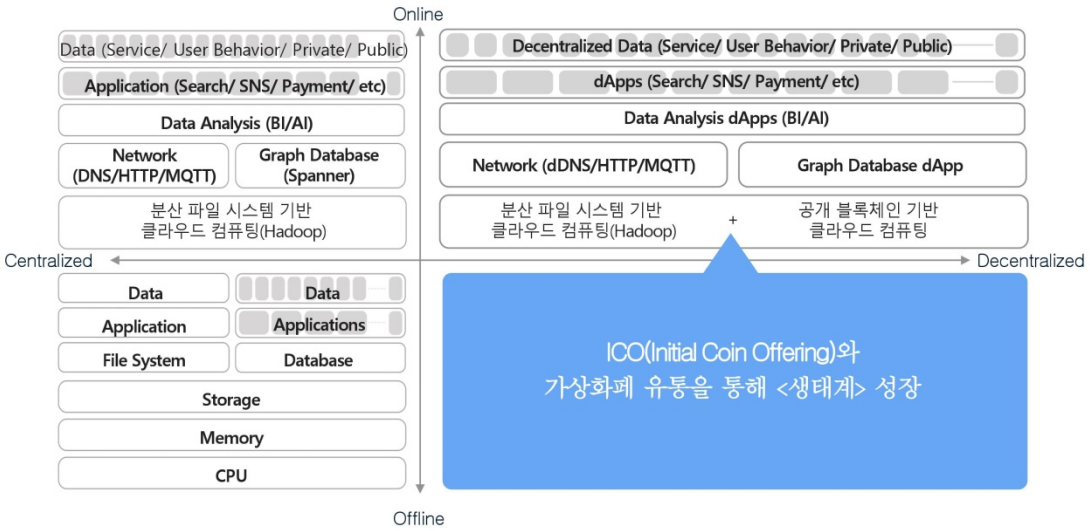
How to raise fund for blockchain project?

 © Copyright Atomrigs Consulting Inc. 2018

비트코인이 던진 두 개의 메시지, 그리고 이더리움

메시지 1 : '신뢰할 수 있는 온라인 탈중앙 컴퓨팅'이 가능하다

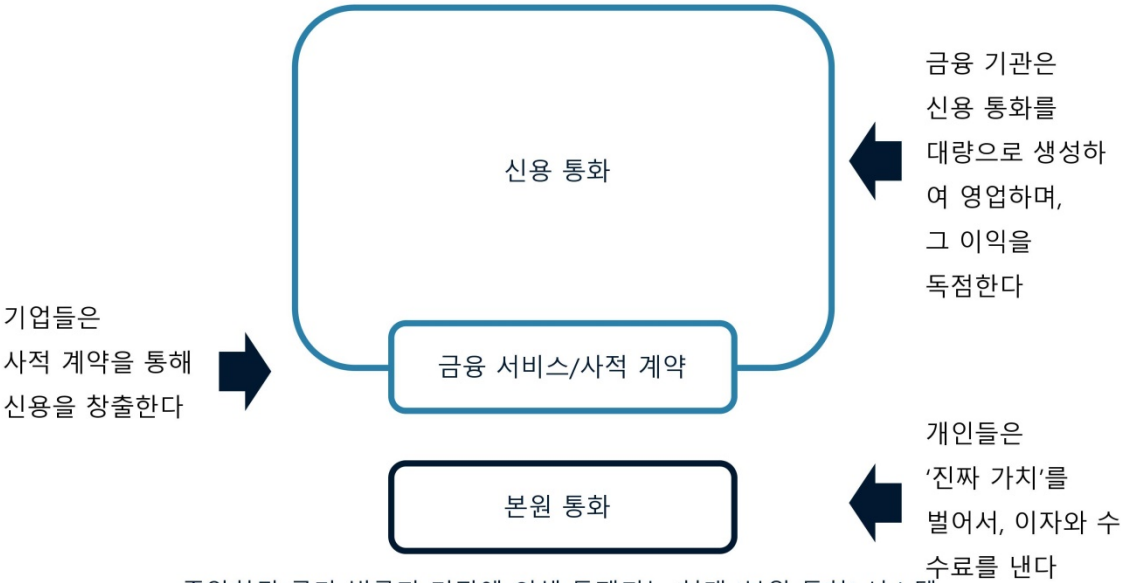
비트코인은 공개 블록체인 기반의 데이터 컴퓨팅이 어떻게 가능한가를 보여줌으로써, '중앙화된 온라인 컴퓨팅'의 대안으로서의 '**탈중앙화된 온라인 컴퓨팅**'의 가능성을 제시
이더리움은 이 측면을 진화시키려는 공개 블록체인 프로젝트



 © Copyright Atomrigs Consulting Inc. 2018

메시지 2 : 온라인 탈중앙 컴퓨팅을 기초로 '대안적 화폐 시스템'을 만들 수 있다

중앙화된 금융기관에 의해 지배되는 '신용통화' 시스템



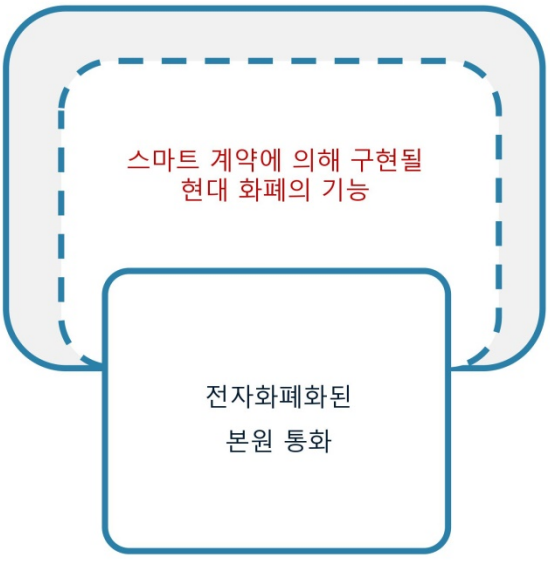
중앙화된 국가 법률과 기관에 의해 통제되는 현대 '본원 통화' 시스템

 © Copyright Atomrigs Consulting Inc. 2018

이더리움의 대안적 화폐이론

비트코인은 현대적 '신용 통화'의 기능성을 대체하기에는 너무 기능이 부족하며,
'실행 가능한 프로그램 코드를 포함한 전자화폐 기능'인 '스마트 계약'으로 이를 해결할 수 있다

'스마트 계약'이라는 새로운 기술을 포함하는 전자화폐 시스템을 이용한다면, 신용통화의 상당부분이 대체될 것!



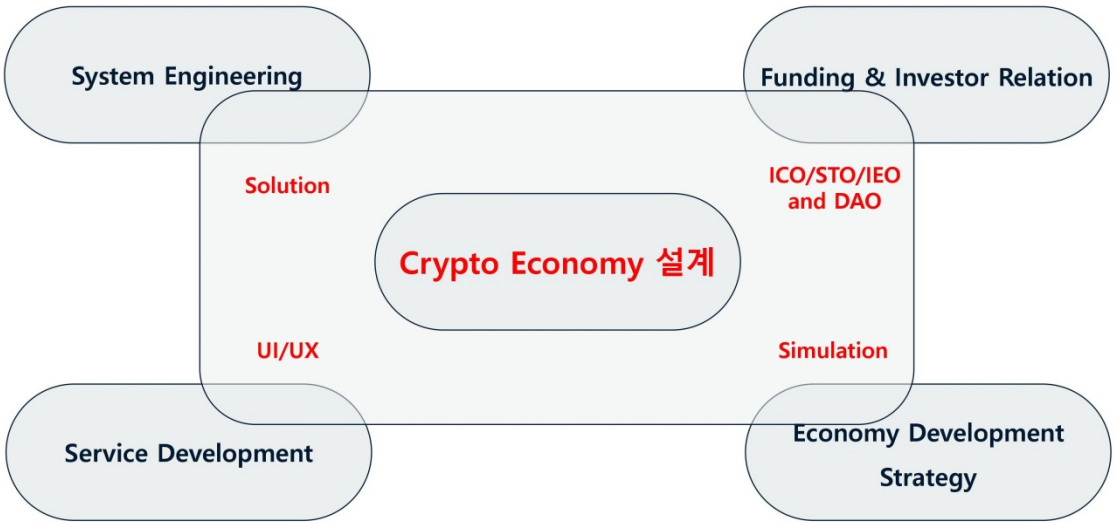
알고리즘에 의해 통제되는 '암호화폐' 시스템

 © Copyright Atomrigs Consulting Inc. 2018

What is Crypto Economy Engineering

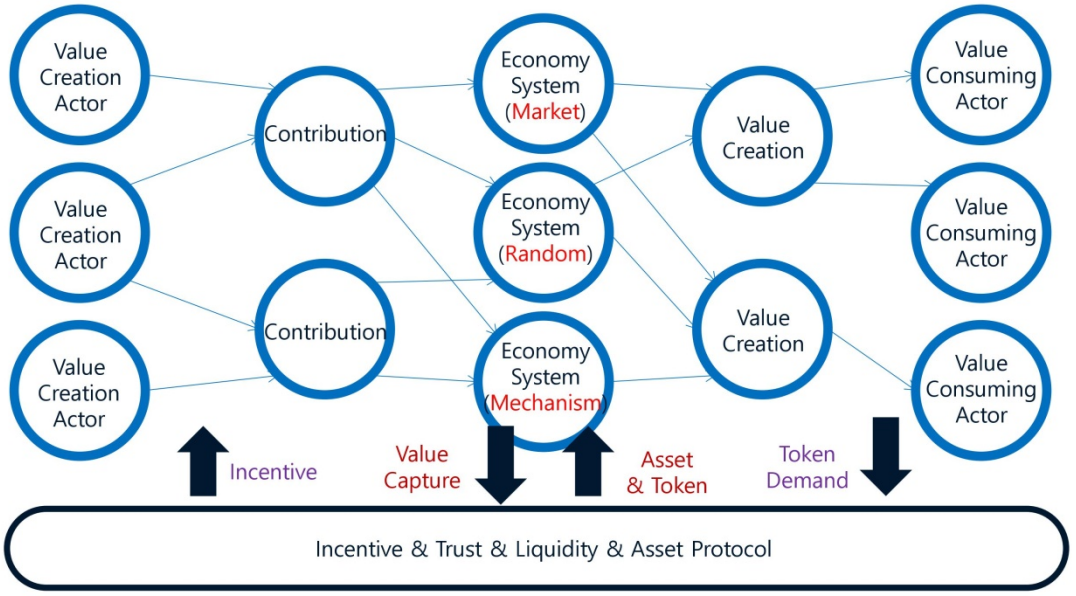
ATOMRIGS CONSULTING

Job Definition of Crypto Economist



 © Copyright Atomrigs Consulting Inc. 2018

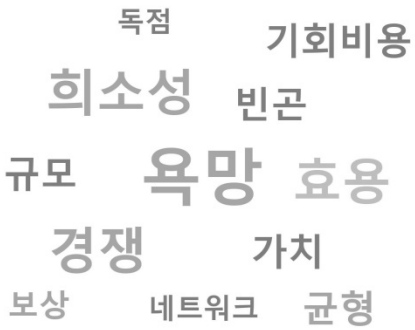
What is Crypto Economy?



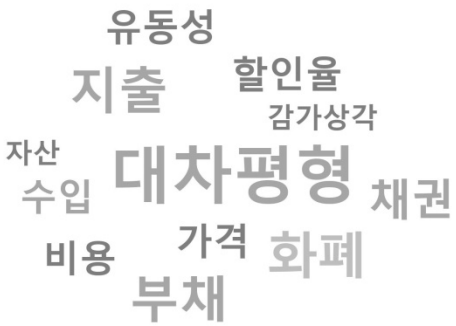
 © Copyright Atomrigs Consulting Inc. 2018

Crypto Economics

Economic Space



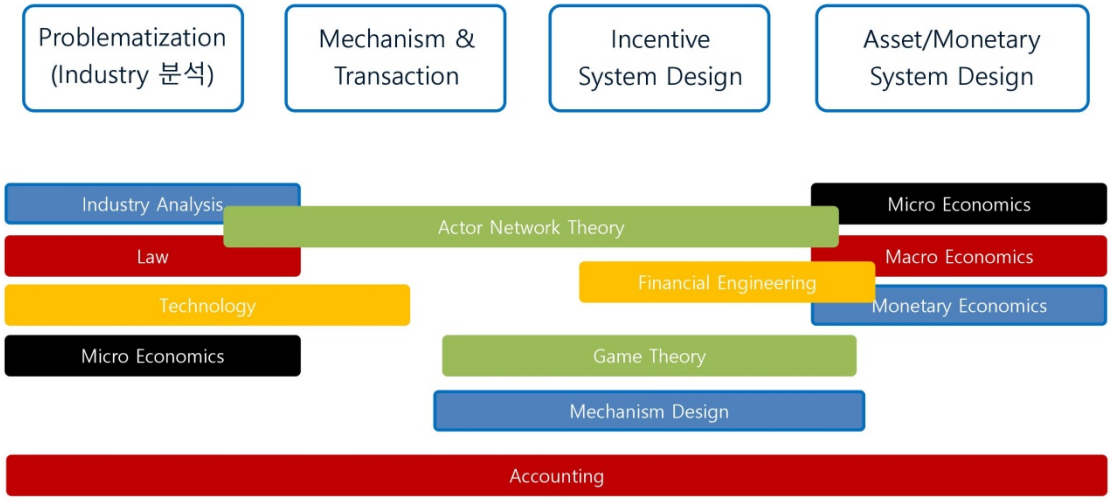
Accounting Space



 © Copyright Atomrigs Consulting Inc. 2018

ATOMRIGS CONSULTING

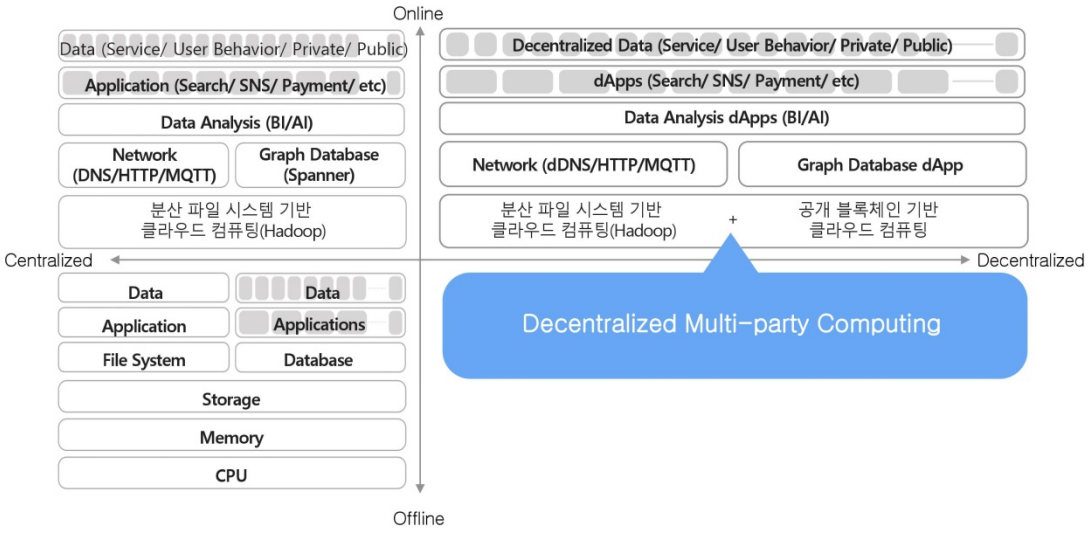
Methodology for Crypto Economy Design



 © Copyright Atomrigs Consulting Inc. 2018

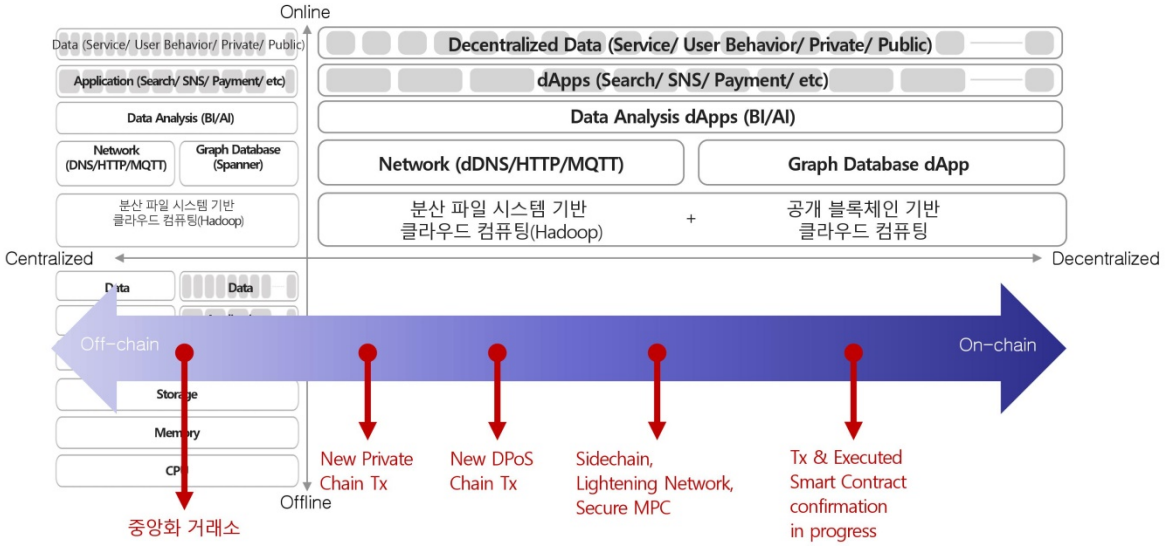
On-chain vs. Off-chain

History of Computing



 © Copyright Atomrigs Consulting Inc. 2018

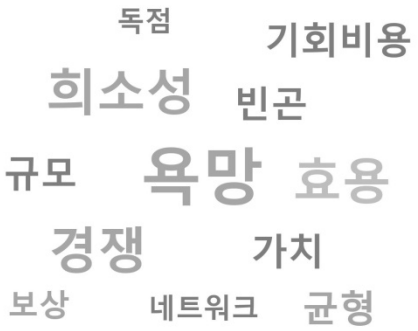
What is 'On-chain'?



 © Copyright Atomrigs Consulting Inc. 2018

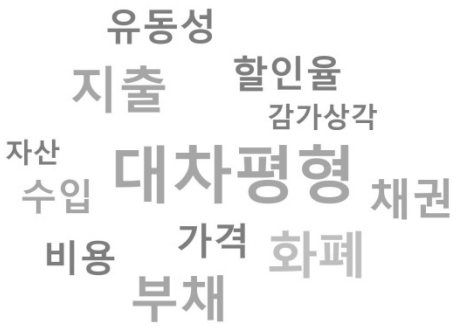
What is ‘On-chain’?

경제적 공간



Off-chain

회계적 공간



On-chain

 © Copyright Atomrigs Consulting Inc. 2018

What is ‘On-chain’?

Bitcoin

Ethereum

 © Copyright Atomrigs Consulting Inc. 2018

ATOMRIGS CONSULTING

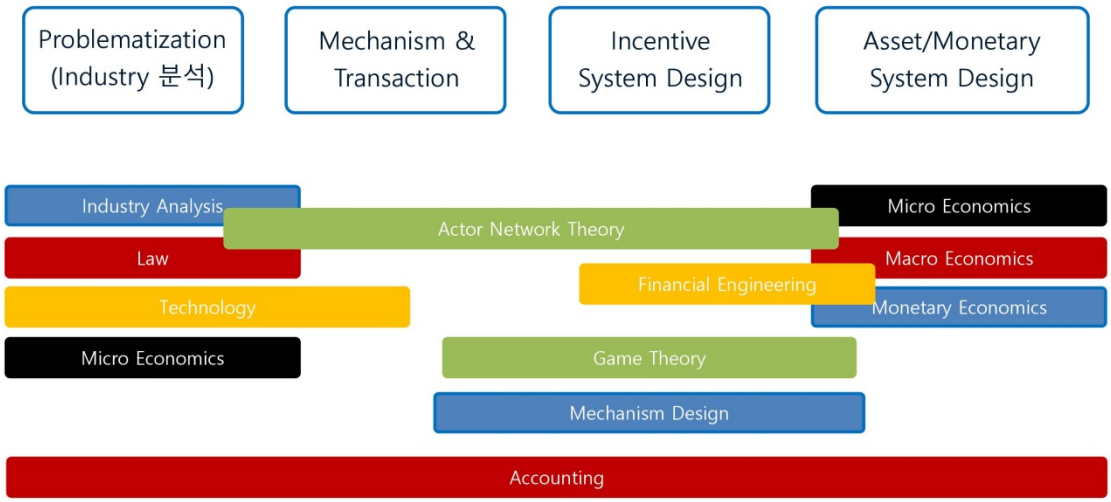
Meaning of 'on-chain' in Crypto Economy Design

	Goods	Contract	Conditions	Enforcement	Payment
Transaction Type 1 (크립토 키티)	On-chain	On-chain	On-chain	On-chain	On-chain
Transaction Type 2 (Augur)	On-chain	On-chain	Off-chain	On-chain	On-chain
Transaction Type 3 (Commerce)	Off-chain	On-chain	Off-chain	Off-chain	On-chain

 © Copyright Atomrigs Consulting Inc. 2018

Crypto Economy Design

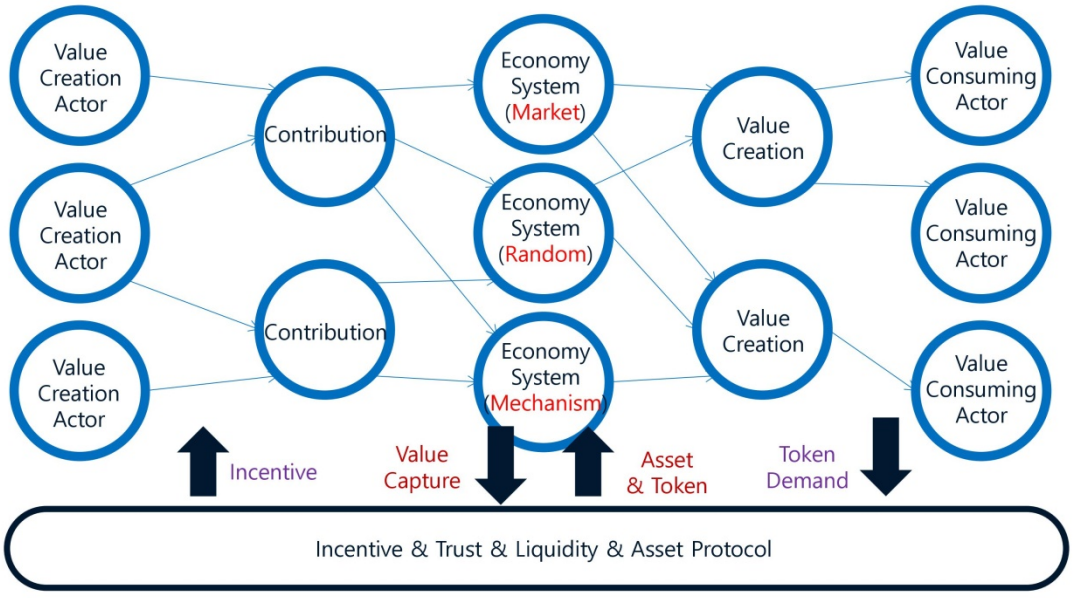
Crypto Economy Design



Economic Problem Off-chain, Re-define On-chain, by Incentive system On-chain, Nudging Actors supplying suitable contributions

 © Copyright Atomrigs Consulting Inc. 2018

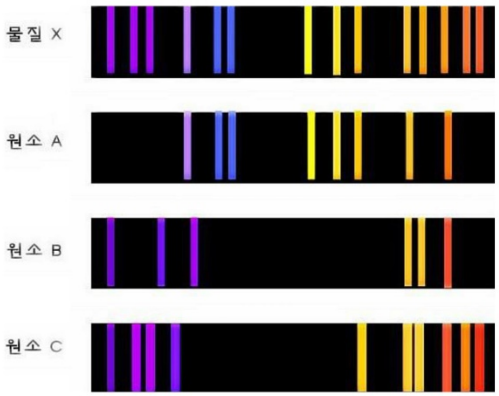
Crypto Economy Design



 © Copyright Atomrigs Consulting Inc. 2018

분석적 설계 vs. 패턴 기반 설계

현재의 크립토 이코노미 설계는 대개 '다른 프로젝트 설계 요소 중 설득력이 있고 자기 프로젝트가 가치를 전달하려는 방식과 유사한 설계 요소들을 조합'하는 방식인 '패턴 기반 설계'로 이루어짐
분석적 설계는 이코노미 구성 요소를 '트랜잭션' 단위로 분해하여, 트랜잭션 생성에 대한 '보상 시스템'을 설계하여 이코노미가 '가치'를 생성하고 '지속'하는데 필요한 '화폐-자산' 균형을 설계



물질 X를 만들려면 원소A, 원소B, 원소C가 필요

사그라다 파밀리아 성당 : 가우디가 고딕과 아르누보, 이슬람 양식, 카탈루냐 모더니즘을 결합하여 설계

© Copyright Atomrigs Consulting Inc. 2018

Industry Analysis for Crypto Economy Design

Goals of Analysis

- Definition of Value
- Missing Value of Legacy
- Scale & Volume of Demand
- Who is competitors?

 © Copyright Atomrigs Consulting Inc. 2018

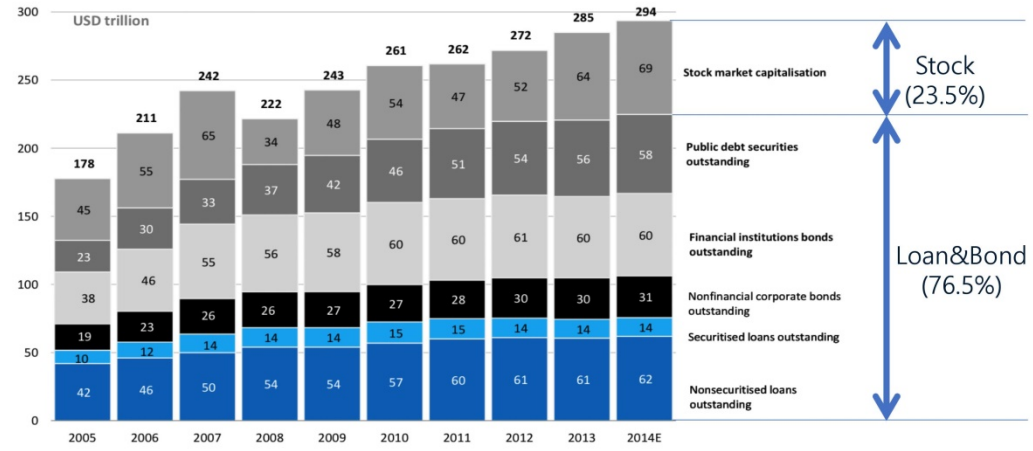
Goals of Analysis

- Who is Contributor supplying essential value?
- The contributor's specialty
- How to make the contribution on-chain

 © Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN(decentralized Credit Union Network)

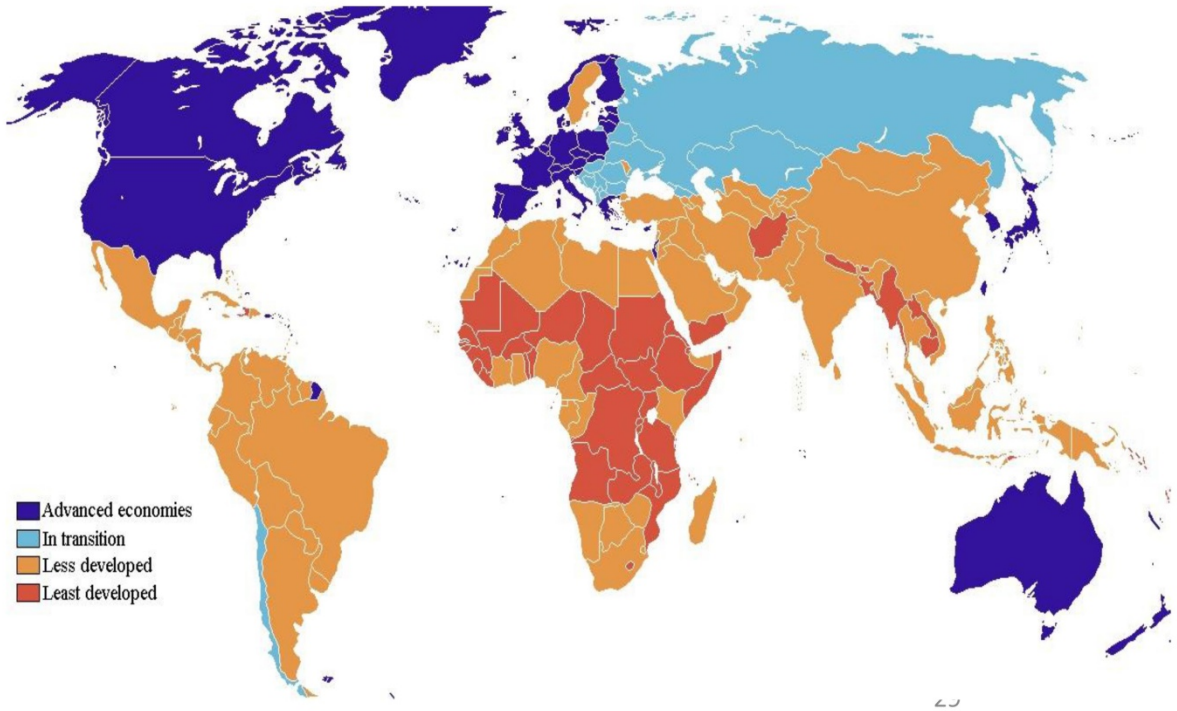
Scale & Volume of Demand



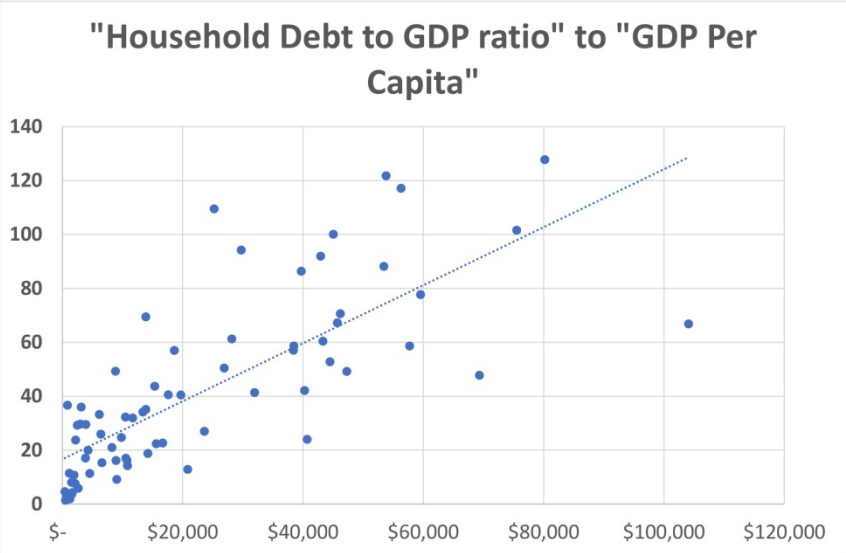
Source: McKinsey Global Institute, Haver, BIS, Deutsche Bank estimates

 © Copyright Atomrigs Consulting Inc. 2018

개인 연소득 3,000~15,000달러 사이의 세계 인구는 약 35억 명



개인당 소득이 높을 수록 소득 대비 부채의 비중은 높아짐



30

ATOMRIGS CONSULTING

사례 : dCUN(decentralized Credit Union Network)

Missing Value of Legacy

고금리, 집단 보증 등
대출 상품 설계

Loan 디폴트 위험

높은 조달 비용

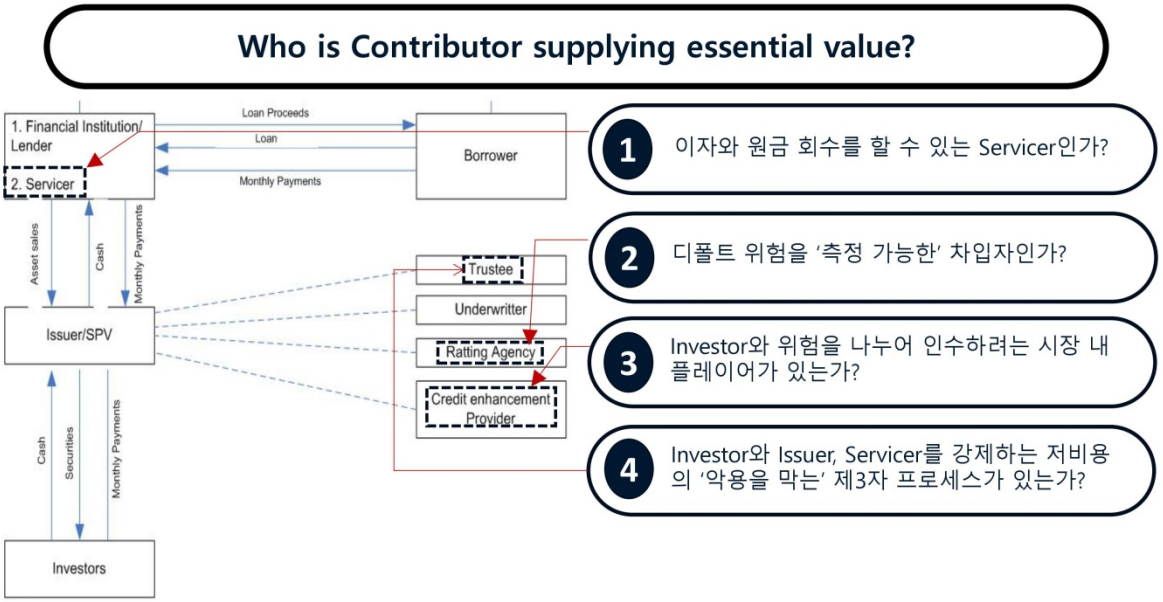
환 위험 + 기관 디폴트 위험

대출금융기관

Borrower ← Loan → Non-securitized ← Loan → Lender

31 | © Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN(decentralized Credit Union Network)



32 | © Copyright Atomrigs Consulting Inc. 2018

Transaction Analysis, Mechanism Design & Incentive system

Transformation of value, Off-chain to On-chain

Re-define value

What is essential contribution

How to drive the contribution on-chain

 © Copyright Atomrigs Consulting Inc. 2018

Transaction Analysis : Journalizing(分介)

What is essential contribution

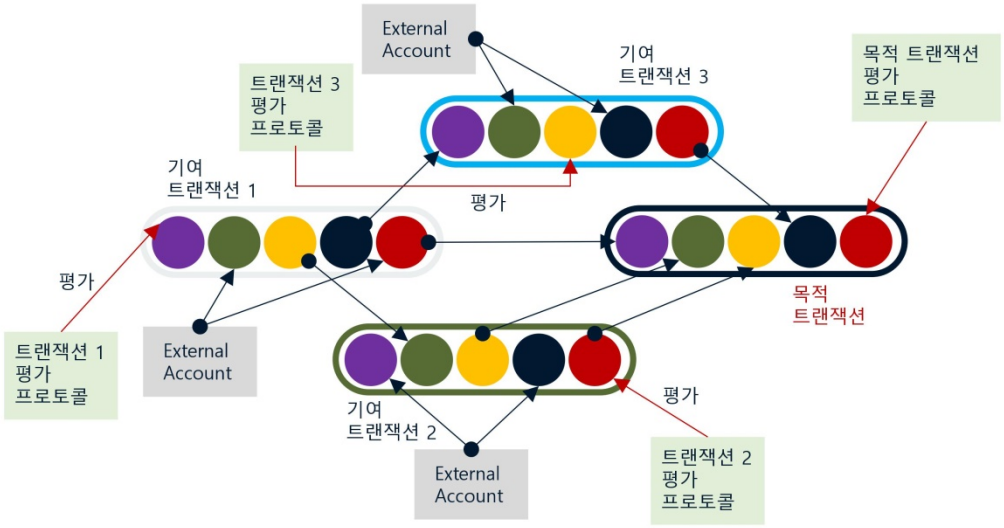
4월 1일: 현금 5,000만원을 출자하여 영업을 시작.
4월 2일: 상품을 현금으로 매입. 매입 가격은 500만원.
4월 4일: 영업용 가구를 현금으로 구입. 구입 가격은 150만원.
4월 7일: 상품을 판매하고 대금은 현금으로 받음. 상품의 원가는 50만원이고 매출 가격은 60만원.

날짜	차변	금액	대변	금액
4월 01일	현금	50,000,000	자본금	50,000,000
4월 02일	상품	5,000,000	현금	5,000,000
4월 04일	비품	1,500,000	현금	1,500,000
4월 05일	현금	600,000	상품	500,000

 © Copyright Atomrigs Consulting Inc. 2018

How to drive the contribution on-chain

크립토 이코노미는 트랜잭션들로 구성되며, 각 트랜잭션의 구성요소는 다른 트랜잭션의 산물이거나 기여행위(contribution)의 산물



ATOMRIGS CONSULTING

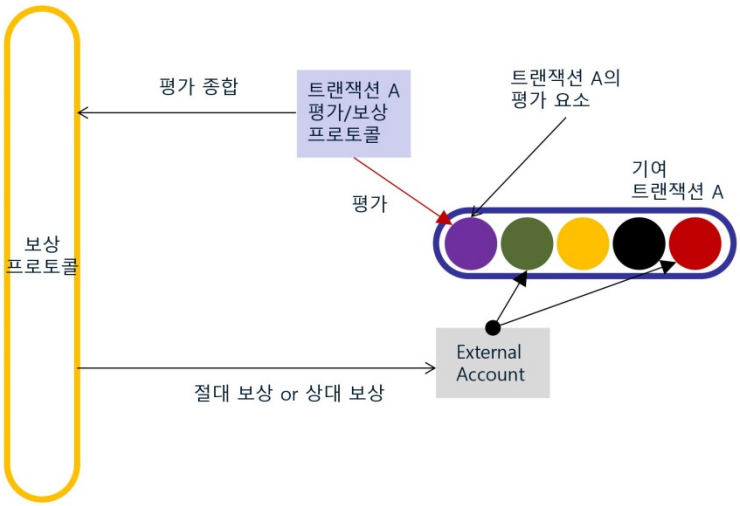
Problem solving On-chain

- 단일 기여자 인센티브 모델
- 복수 기여자에 의한 동일 기여 인센티브 모델
- 시장을 통한 의사결정
- 메카니즘 디자인을 통한 사회적 선택
- 보유형 인센티브 모델

© Copyright Atomrigs Consulting Inc. 2018

Problem solving On-chain

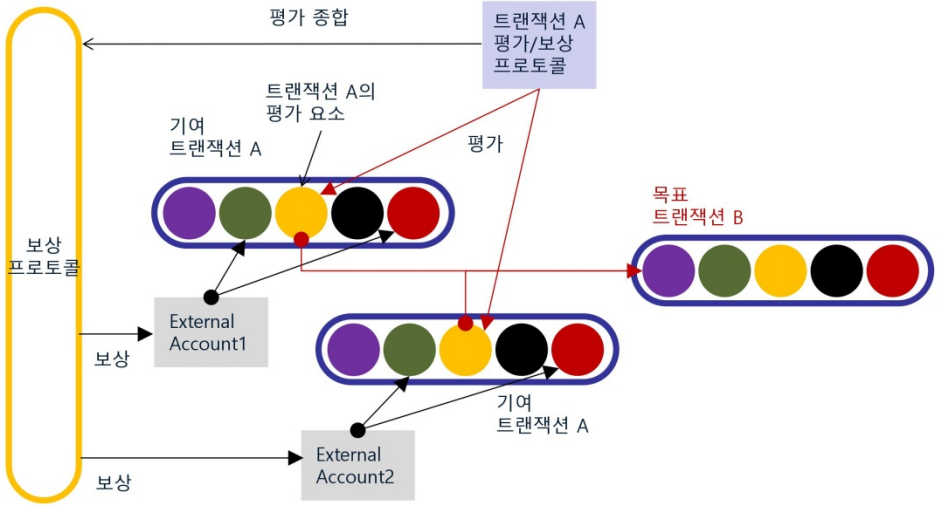
단일 기여자 인센티브 모델



 © Copyright Atomrigs Consulting Inc. 2018

Problem solving On-chain

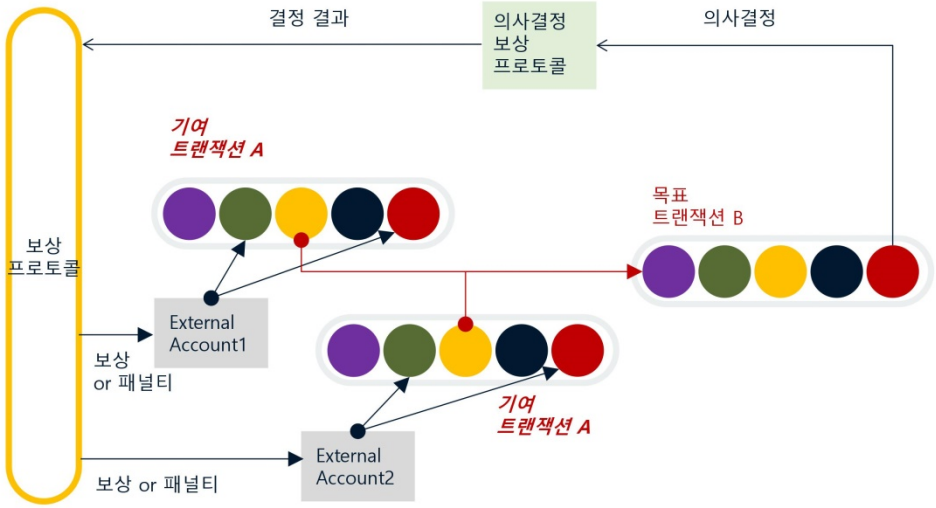
복수 기여자에 의한 동일 기여 인센티브 모델



 © Copyright Atomrigs Consulting Inc. 2018

Problem solving On-chain

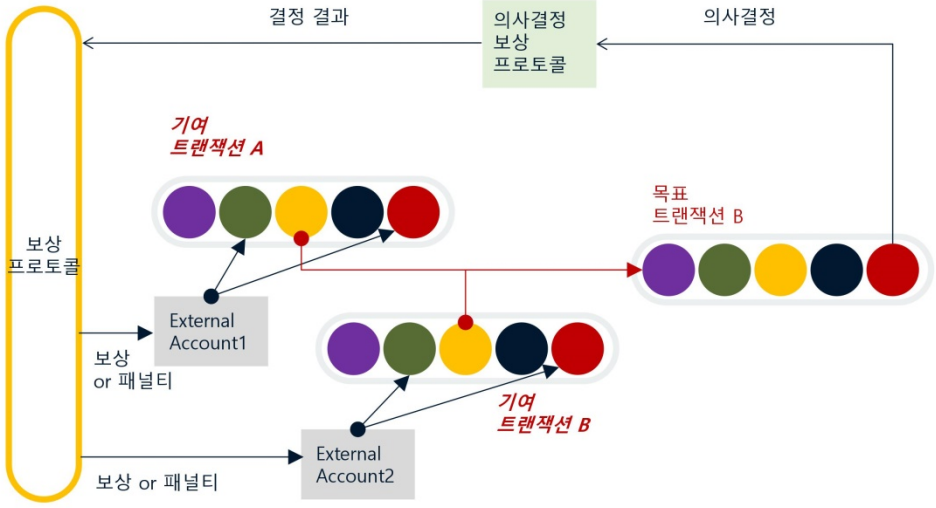
시장을 통한 의사결정



 © Copyright Atomrigs Consulting Inc. 2018

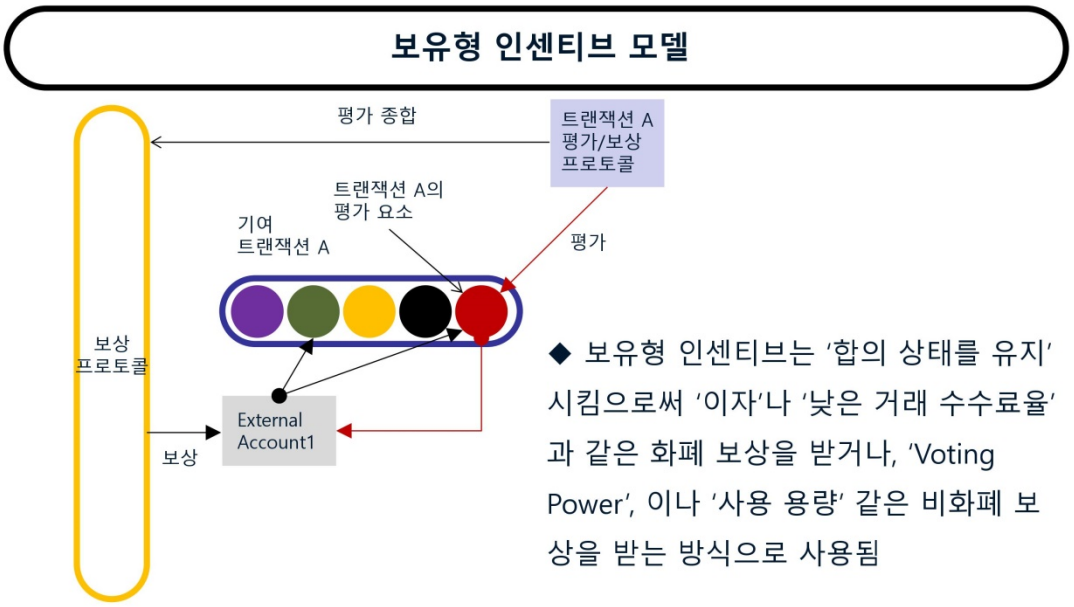
Problem solving On-chain

메카니즘 디자인을 통한 사회적 선택



 © Copyright Atomrigs Consulting Inc. 2018

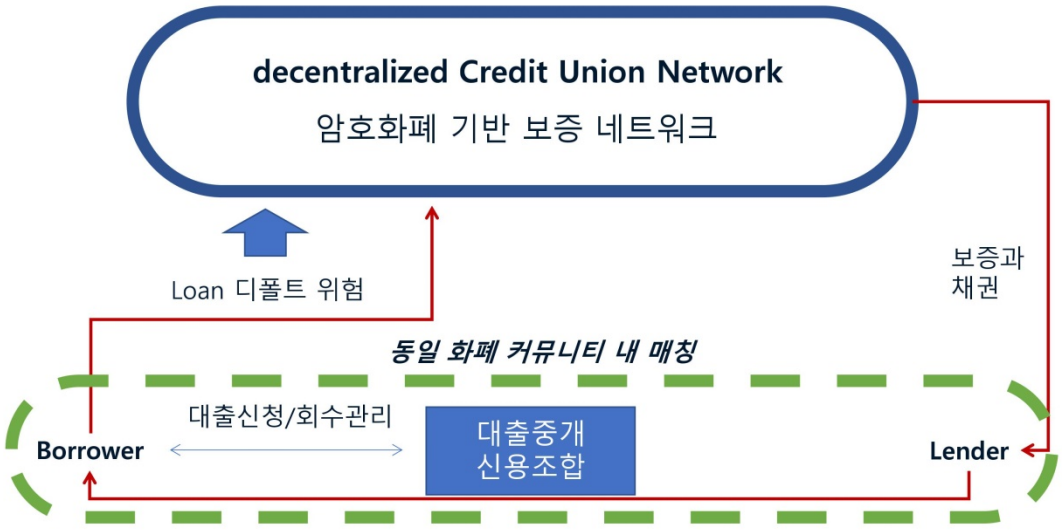
Problem solving On-chain



◆ 보유형 인센티브는 '합의 상태를 유지' 시킴으로써 '이자'나 '낮은 거래 수수료율' 과 같은 화폐 보상을 받거나, 'Voting Power', 이나 '사용 용량' 같은 비화폐 보상을 받는 방식으로 사용됨

 © Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN의 보증 메카니즘

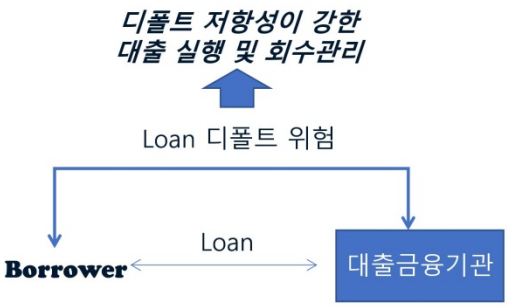


암호화폐를 매개로 한 P2P 대출

 © Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN의 필수 트랜잭션

'가치' 생산을 위한 '필수 트랜잭션'과 그 구성 요소인 '기여'는 무엇인가?

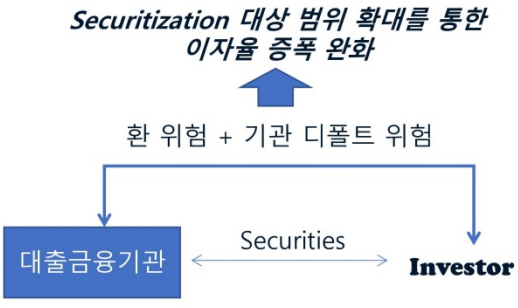


1. 디폴트 위험이 있는 차입자에 대한 대출 필터링
2. 디폴트를 방어하려는 이해 관계자의 존재
3. 디폴트 시, 강제로 작동하는 원금 회수 메카니즘
4. 인센티브 시스템을 악용하는 Abuser 차단

 © Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN의 필수 트랜잭션

'가치' 생산을 위한 '필수 트랜잭션'과 그 구성 요소인 '기여'는 무엇인가?



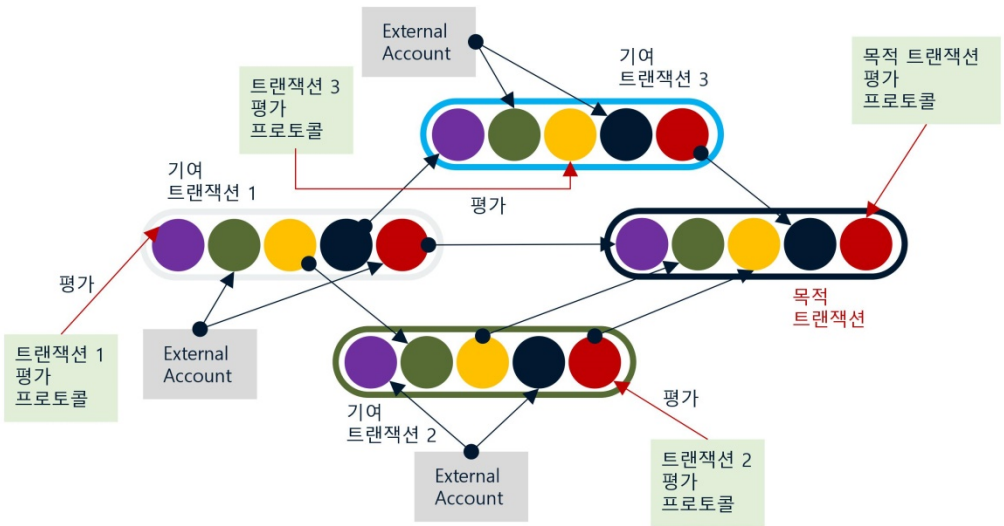
5. '차입자 정보 기반 신용 위험 측정'을 대체할 방법
6. '환 위험'을 인수할 수 있는 위험 인수자
7. 발행기관 상태에 독립적인 상환 및 청산 메카니즘
8. 글로벌하게 작동하는 securities 유통 메카니즘

 © Copyright Atomrigs Consulting Inc. 2018

Money & Asset

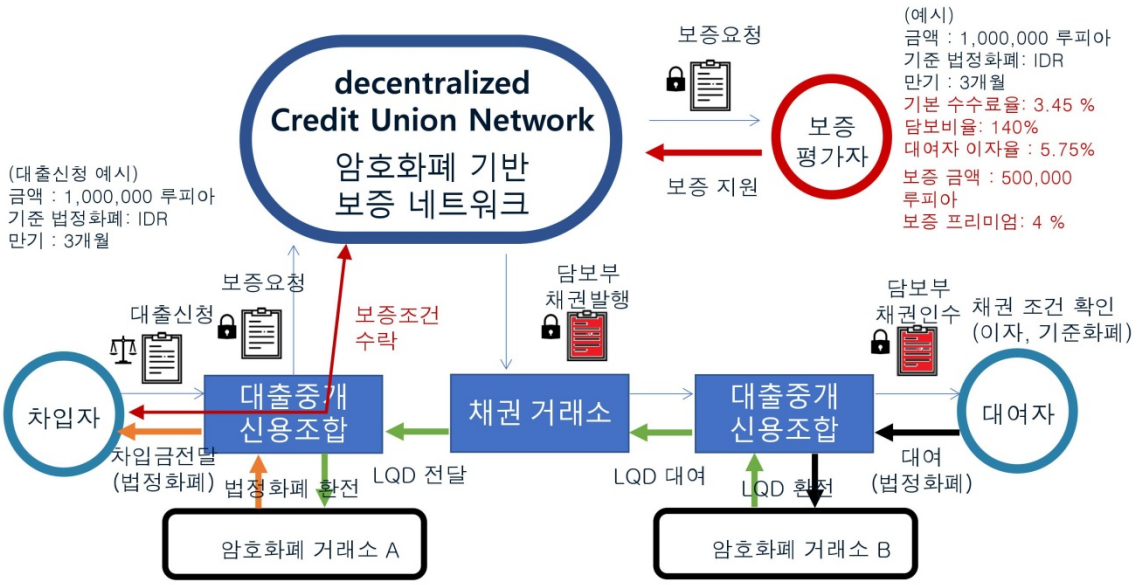
ATOMRIGS CONSULTING

Token is financial status from transaction by incentive system



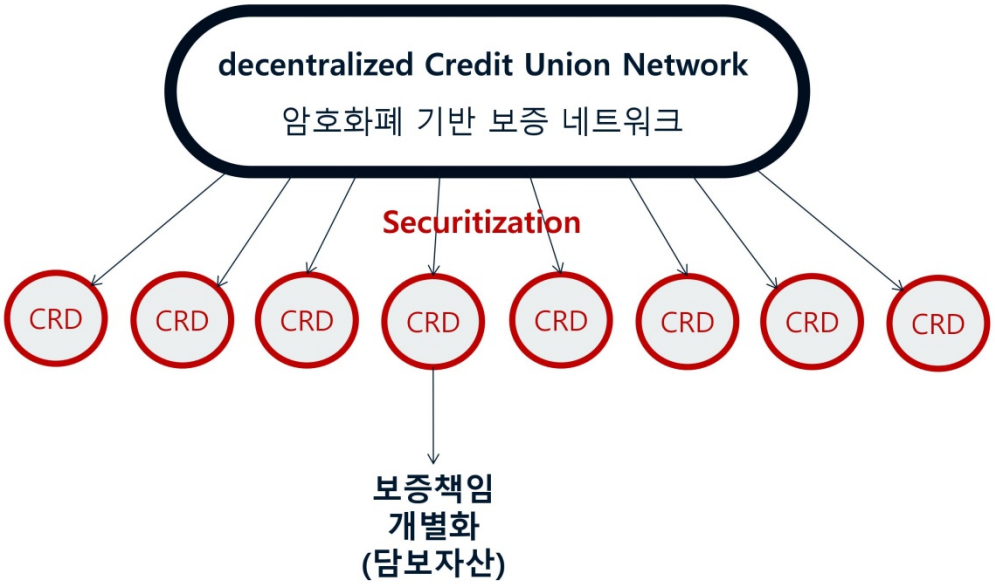
© Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN의 'Global Scale' 유동성 전달을 위한 토큰 LQD



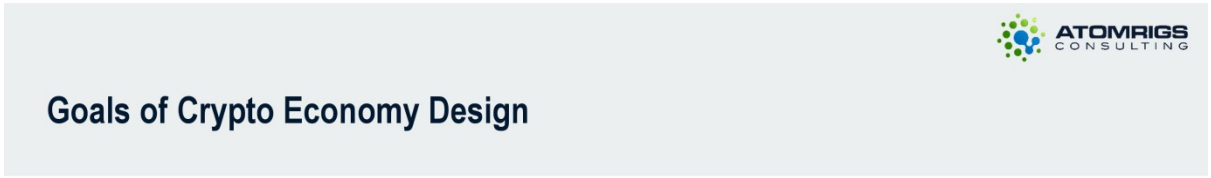
 © Copyright Atomrigs Consulting Inc. 2018

사례 : dCUN의 '기금에 의한 보증'을 '자산 담보화'하기 위한 토큰 CRD



 © Copyright Atomrigs Consulting Inc. 2018

Goals of Crypto Economy Design and Future works



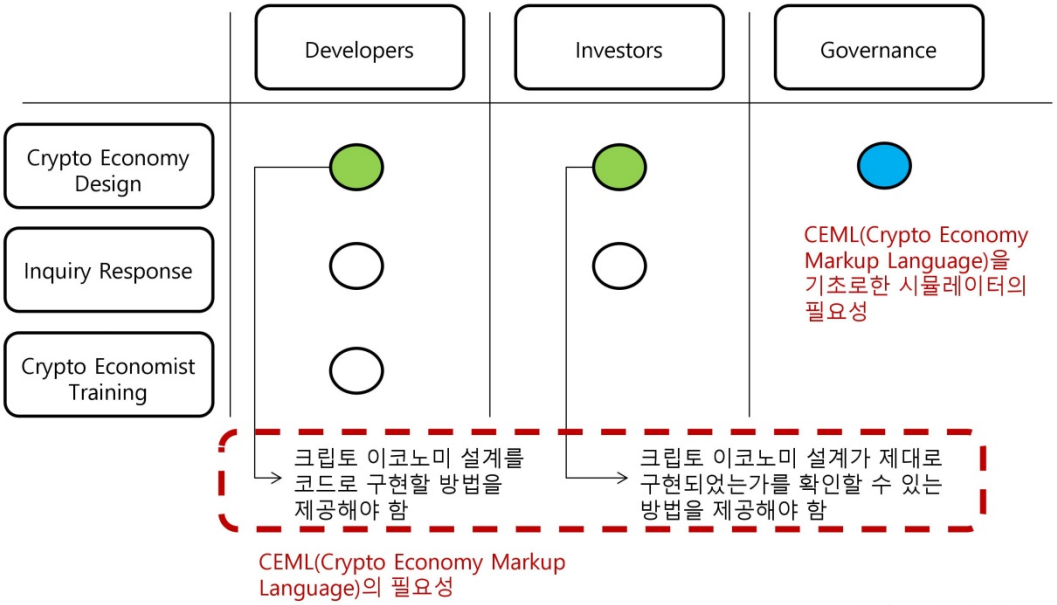
Who is Main Actor?

What is the mechanism creating intrinsic value of crypto token and asset?

What is on-chain? What is off-chain?

 © Copyright Atomrigs Consulting Inc. 2018

Future works



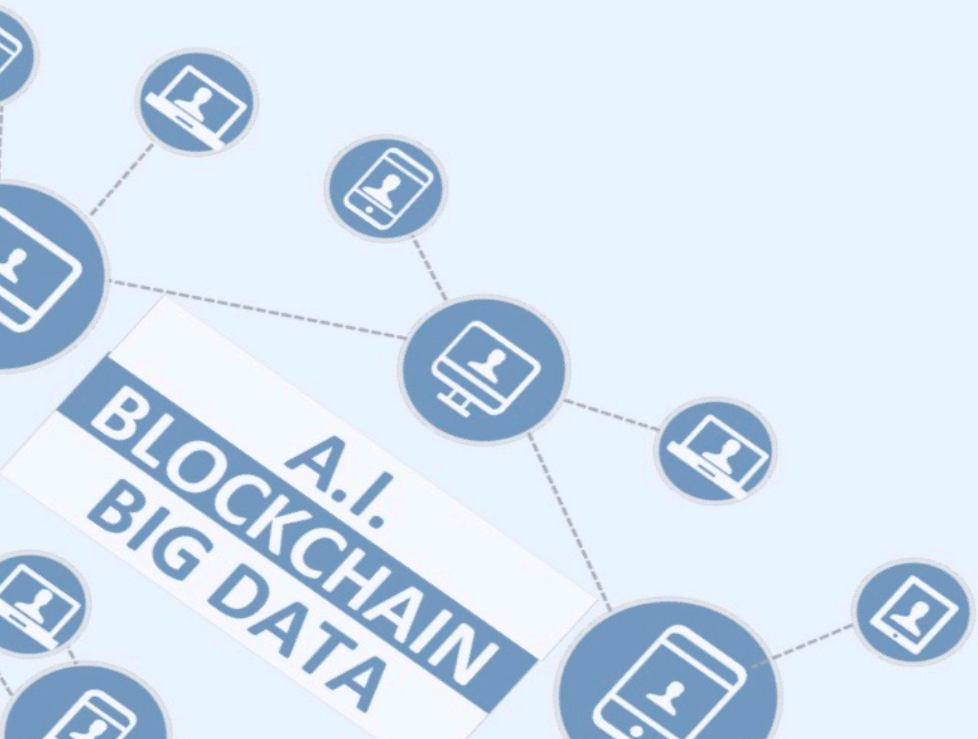
© Copyright Atomrigs Consulting Inc. 2018

9강

블록체인과 세계경제

오 정 근 회장

(한국금융ICT융합학회)



강의 동영상 URL

1 부: https://youtu.be/FMUp-_wdpSU

2 부: https://youtu.be/g0ELzCiHI-A

블록체인과 세계경제

2018. 5. 9

오정근
(한국금융ICT융합학회 회장)

약력

- 고려대 경제학 학사 석사
- 영국 맨체스터대 경제학 석사 박사

- 한국금융ICT융합학회 회장

- 前 한국은행 금융경제연구원 부원장
- 동남아중앙은행 조사국장
- 고려대 경제학과 교수
- 건국대 금융IT학과 특임교수
- 한국국제금융학회 회장
- 아시아금융학회 회장

목 차

- 블록체인과 거래효율성 신뢰성
- 블록체인과 암호화폐의 미래
- 급증하는 토큰시대 개화
- 디지털국가 디지털정당
- 암호화폐 동향과 규제 동향
- 디지털화폐와 디지털금융 시대
- 암호화폐와 부패방지, 포용금융
- 폭발적으로 늘어날 ICO
- 투자자보호
- 한국형 암호화폐공개(ICO) 가이드라인
- ICO 금지에 따른 블록체인 암호화폐 기업들의 탈한국러시와 국부유출
- 대응방안: 특구육성
- 외국의 혁신 사례

블록체인과 거래효율성 신뢰성(금융보안)

2009년 두 가지 문명사적 중요한 발명

- 애플사의 아이폰
  - 종래의 피쳐폰에 인터넷 기능 장착한 스마트폰 출현
  - 손안에 인터넷이 들어와 전세계가 시공을 초월해 언제 어디서든지 연결되는 네트워크 시대 진입

- 블록체인기반 비트코인
  - 네트워크 기반의 가상(암호, 디지털)화폐 출현
  - 블록체인 거래: 종래 가치의 거래=>신뢰의 거래

기존 중앙집중형 시스템

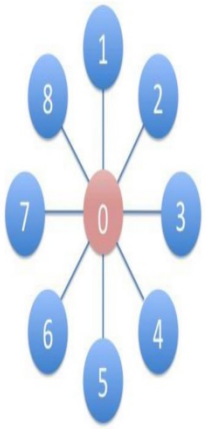
□ 기존 중앙집중형 시스템은 **원장(Ledger)**을 집중하여 관리하는 **신뢰할 수 있는 제3의 기관(TTP: Trusted Third Party)**을 설립하고 **해당 기관에 대한 신뢰**를 확보하는 방식으로 발전해 왔음

▪ 특정 기관이 원장을 조작 또는 개인정보를 유출하지 않을 뿐 아니라 시스템 오류 및 처리속도 저하를 예방하고, 해킹 등 외부로부터의 악의적인 공격 및 조작 시도를 방지할 수 있다는 신뢰가 중요

□ 신뢰할 수 있는 제3의 기관(TTP)을 설립하여 운영하는데 소요되는 **높은 사회적 비용**은 **금융산업 발전**의 **제약** 요인으로 작용할 수 있음

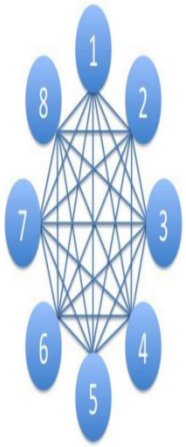
— 대규모 조직을 설립·운영하기 위한 비용은 이용자의 높은 수수료 부담 으로 전가

— 한편 규제 및 감독은 진입장벽으로 작용하여 혁신적인 신규 서비스 및 사업자의 진출을 제한



분산원장(Distributed Ledger) 기술

□ **분산원장(Distributed Ledger) 기술**은 거래정보를 기록한 **원장**을 특정 기관의 중앙 서버가 아닌 **P2P(Peer-to-Peer)네트워크**에 분산하여 참가자가 공동으로 기록하고 관리하는 기술을 의미함



클라이언트나 서버의 개념 없이 동등한 참가자(peer nodes)들이 클라이언트와 서버 의 역할을 동시에 수행하며 데이터나 주변 장치 등을 공유하는 방식으로 주로 음악, 영화 등의 파일을 공유하는 서비스 등에 활용

— 분산원장 기술에서는 모든 참여자가 거래내역이 기록된 원장 전체를 각각 보관하고 새로운 거래를 반영하여 갱신(update)하는 작업도 공동으로 수행

보안과 블록체인(Block chain)
분산형 전자금융 거래장부

블록체인은 거래 정보를 중앙서버에 저장하지 않고 네트워크 내 여러 컴퓨터에 분산해 저장하는 보안기술

블록체인은 거래에 참여하는 모든 사용자가 거래내역을 공유

거래할 때마다 이를 대조해 위조를 막는 분권화된 방식

거래 내역이 모든 거래주체에게 공유되기 때문에 공유된 정보를 모두 조작하기는 어렵고 별도 보안 프로그램 없이 강력한 보안 능력 보유

블록체인 작동원리

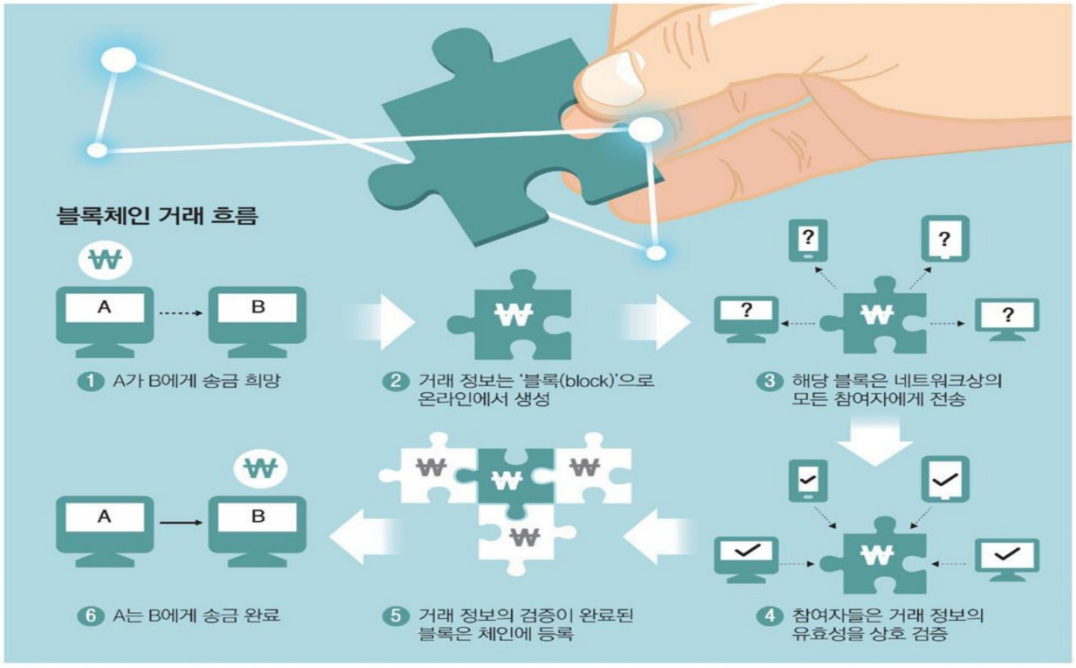
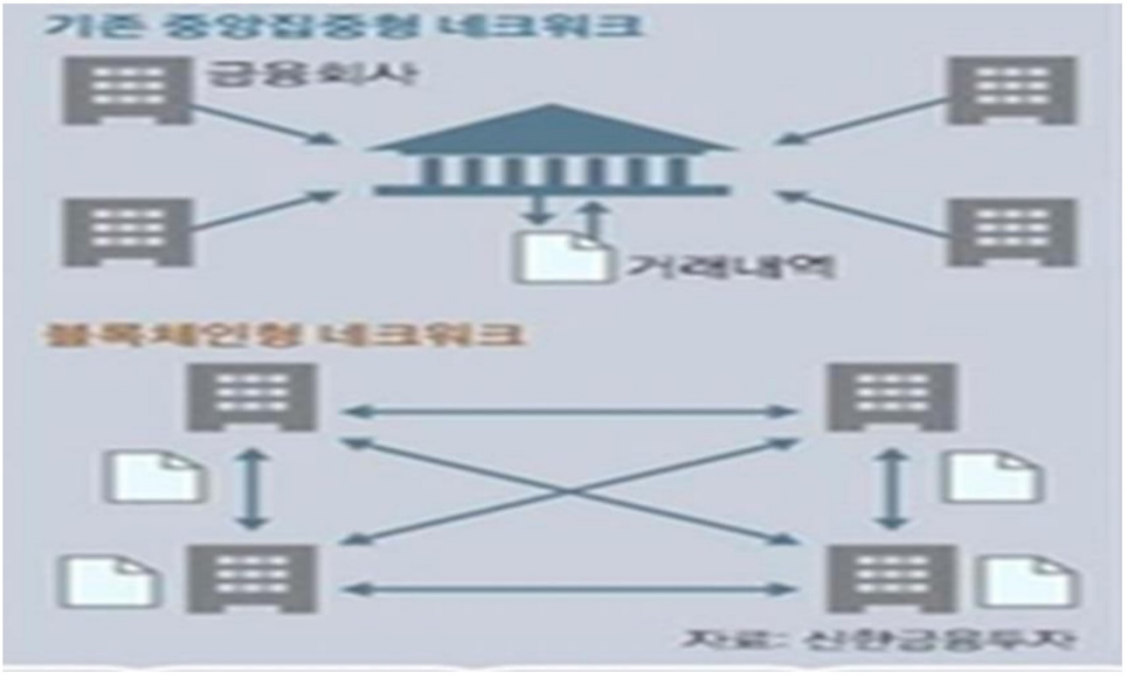
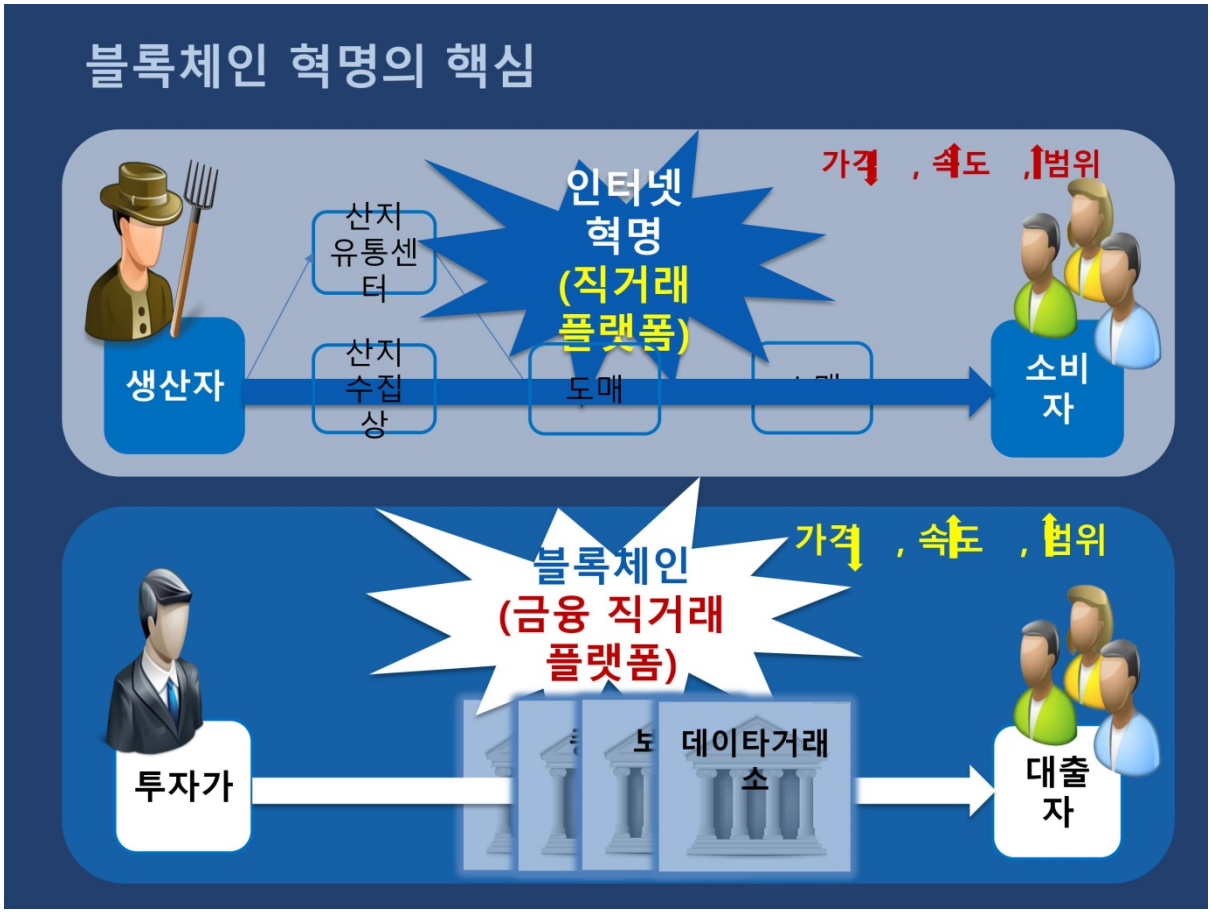


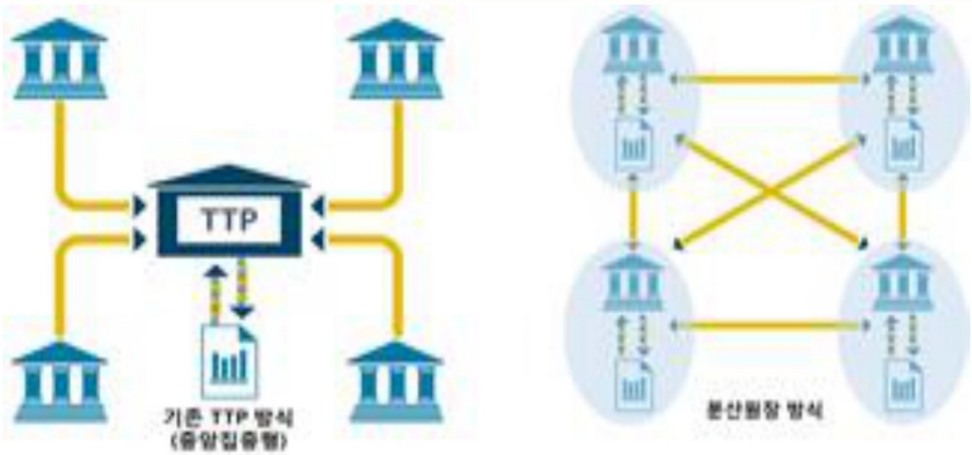
그림 MBN 6.17

블록체인과 기존 중앙집중형 결제네트워크 비교





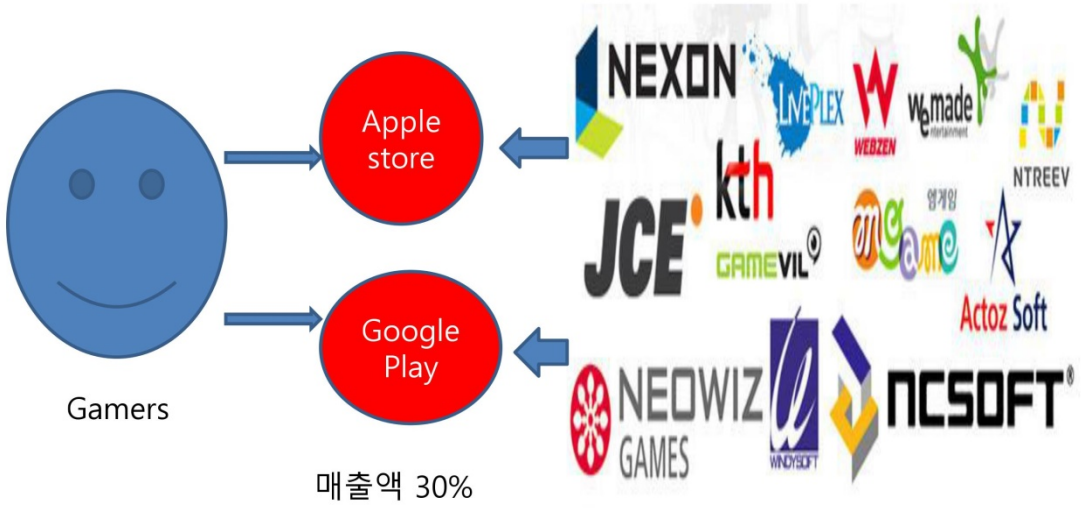
거래의 효율성과 신뢰성



예금자--- 은행--- 대출자
은행--- 금융결제원---은행
은행--- 중앙은행--- 은행
주식 채권 투자자—예탁결제원---주식 채권 매도자

→ P2P 거래

막대한 거래비용



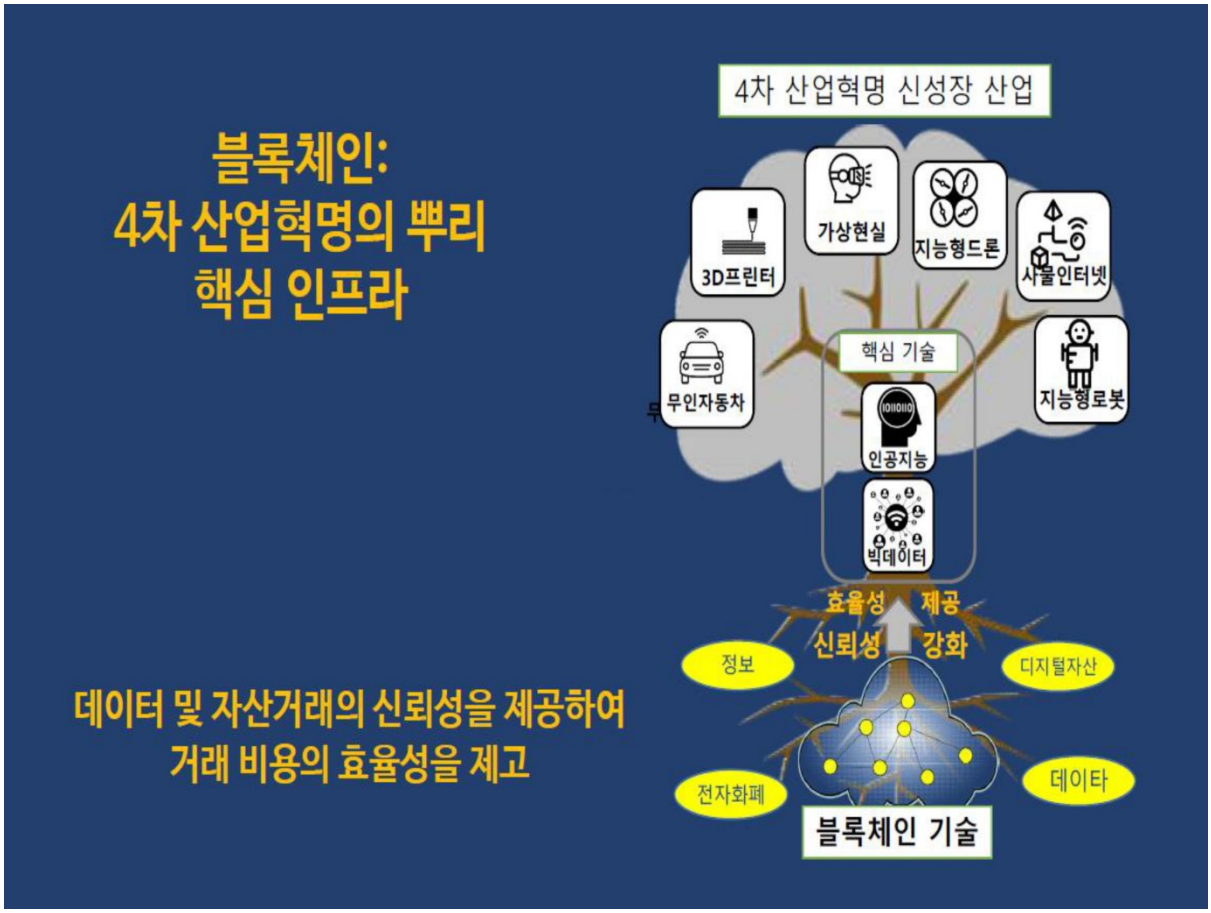
블록체인 이점과 폭발적 확산

- 블록체인(Block chain)이 은행권의 핵심 보안기술로 부상. 글로벌 은행에 이어 국내 은행도 속속 블록체인을 도입 중
- 중앙서버를 관리할 필요가 없어 비용부담이 줄고 시스템상 위변조가 불가능해 금융권의 뜨거운 관심
- 소비자들도 자산을 안전하게 관리할 수 있어 이득
- WEF: 세계 금융기관 80% 블록체인 사용 전망
- 영란은행: GDP 3% 증가효과 분석

블록체인과 암호화폐의 미래

만물인터넷 (IOE) 시대와 블록체인

- 모든 사물 디바이스 인간이 연결되어 모든 데이터 정보 상품 서비스가 거래되는 만물인터넷 시대
  - 연결될 수록 보안문제 대두
- 거래 효율성 투명성 보안성을 위한 블록체인 기반 확산
  - 블록체인: 4차 산업혁명의 기반
- 블록체인 기반거래 가능하게 하는 암호화폐 사용도 급증



Industry 4.0

- IoT, IoE → Big Data → AI →인류생활 획기적 향상 → IoT, IoE 의 순환
- Cyber-Physical System 의 순환

Blockchain: 거래의 효율성 보안성 투명성

Crypto currency: 예약 결제로 거래 금융적 종결

코인의 진화와 토큰의 급증

- 코인의 진화
  - 코인 1.0 (비트코인) 코인2.0 (이더륨)
- 토큰의 급증 (코인 3.0)
  - 모든 거래 사용될 토큰 폭발적 급증

코인 토큰의 부침생멸도 급증 전망

- 기술성 (우수성 구현가능성 기술팀수준),
- 시장성 (비즈니스 모델에 대한 시장의 수요)
- 도덕성 (CEO 경영진)

급증하는 토큰시대 개화

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Global Agenda Council on the Future of Software & Society

Deep Shift
Technology Tipping Points and Societal Impact

폭발적으로 늘어나는 산업별 부문별 블록체인 활용, 즉 토큰들 -코인 3.0 시대

- 금융거래(국제송금, 유가증권거래, 조건부채권발행(**코코본드**: CoCo bond: contingent convertible bond)
- 물류 유통 해양(머스크), Food (중국 돈육거래)
- 자금 회수 위험으로 에스크로(escrow)가 필요한 거래들
  - 무역거래
  - 부동산거래 상업등기 등 각종 스마트계약
  - 자동차 등 내구소비재 거래

***에스크로(escrow) : 구매자와 판매자 간 신용관계가 불확실할 때 제3자가 상거래가 원활히 이루어질 수 있도록 중계를 하는 매매 보호 서비스**

폭발적으로 늘어나는 산업별 부문별 블록체인 활용, 즉 토큰들 -코인 3.0 시대 (계속)

- 예약을 동반하는 거래들 숙박시설
  - 교통기관
  - 의료시설
  - 학습시설
- 사용시간 사용량에 따라 요금이 부과되는 산업들
  - 주차장 렌터카 임대회의실 대여금고 임대창고
  - 디지털콘텐츠
  - 노래방 헬스클럽 대중목욕탕 등

폭발적으로 늘어나는 산업별 부문별 블록체인 활용, 즉 토큰들 -코인 3.0 시대 (계속)

- 센서 네트워크 IOT 등을 활용한 자동거래 산업
  - 가스 수도 전기
  - 통신 교통
  - 농업 축산업

- 게임 오락 (게임코인)
- 의료(메디블록)
- 연예 스포츠 스타(스타그램 토큰스타)
- 화장품 패션
- 지역화폐(노원구 노원화폐)

폭발적으로 늘어나는 산업별 부문별 블록체인 활용, 즉 토큰들 -코인 3.0 시대 (계속)

- 자동운영기업(DAC: Distributed Autonomous Company) 또는 자동운영조직(DAO: Distributed Autonomous Organization): : 프로그램된 블록체인 기반 자동기업경영, 자동조직운영
  - 홈쇼핑은 수년 내 자동운영기업으로 전환 전망
- .....

- 획기적인 거래의 효율성, 비용절감, 투명성, 보안성으로 인해 매년 수 백 개의 코인 탄생

- 산업별 부문별 블록체인기반 거래가 확산될 수록 블록체인 거래에 필요한 더 많은 코인이 발행될 전망

금융권: 블록체인 기반거래 폭발적 확산

- 블록체인(Block chain)이 은행권의 핵심 보안기술로 부상. 글로벌 은행에 이어 국내 은행도 속속 블록체인을 도입 중
  - 한국증권업계: 공인인증서 대신 블록체인 이용 공동인증제 도입 (2017년 말)
  - 한국은행업계: 공동인증제 2018년 중 도입 예정
- 중앙서버를 관리할 필요가 없어 비용부담이 줄고 시스템상 위변조가 불가능해 금융권의 뜨거운 관심
- 소비자들도 자산을 안전하게 관리할 수 있어 이득
- WEF: 2018년 까지 세계 금융기관 80% 블록체인 사용 전망
- 영란은행: 거래효율의 획기적 증가로 GDP 3% 증가효과 분석

블록체인 기반 글로벌 송금결제 컨소시엄

글로벌 금융서비스 개발 스타트업 R3는 'R3CEV(Crypto, Exchanges and Venture practice)'라는 블록체인 컨소시엄을 운영

R3CEV는 지난2016년 9월 결성돼 씨티그룹, 뱅크오브아메리카(BoA), JP모건체이스, 모건스탠리, 골드만삭스, UBS 등 100여개 금융회사 회원사 (연간 25만 달러(약 3억원).

R3는 기본적인 시스템 설계 및 기술개발을 담당하고, 회원사는 자사 응용 프로그램 프로그래밍 인터페이스(API)에 연결해 시스템을 테스트. 우선 블록체인 기반의 해외송금시스템을 개발해 해외송금 수수료를 기존의 1/10 수준으로 낮출 계획.

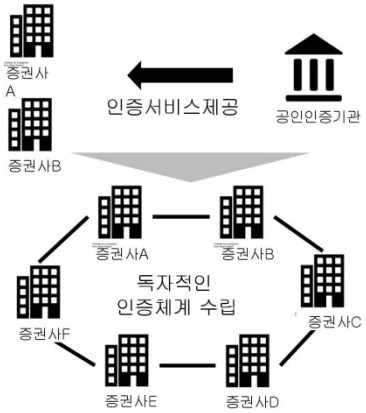
R3CEV는 송금을 넘어 결제, 회사채, 보험, 주식, 부동산 등 8개 영역에 블록체인 기술을 적용해 거래 안정성을 강화

금융권 블록체인 컨소시엄 사업 본격화

증권, 은행, 보험 각 분야별 블록체인 컨소시엄이 출범되어 사업 착수, 우선 고객 편의성을 높일 수 있는 인증서비스 분야 개발

금투업권 컨소시엄

- 금융투자협회 주관, 25개 증권사와 5개 블록체인업체 참여 (16년 12월)
- 블록체인 기반 공동사설인증 시범서비스 예정 (17년 7월)
- 공인인증에 투입되는 자원과 비용을 절감하고, 향후 금융투자상품 거래 적용 계획



은행권 컨소시엄

- 전국은행연합회 주관, 18개 은행이 참여 (16년 11월)
- 은행권 공동 인증 서비스, 외국환 지정 거래 변경 사업 추진

보험업계 컨소시엄

- 생명보험협회와 손해보험협회가 각각 블록체인 컨소시엄 TF 구성 (17년 6월)
- 스마트계약을 통한 보험금 자동지급 기술 검토

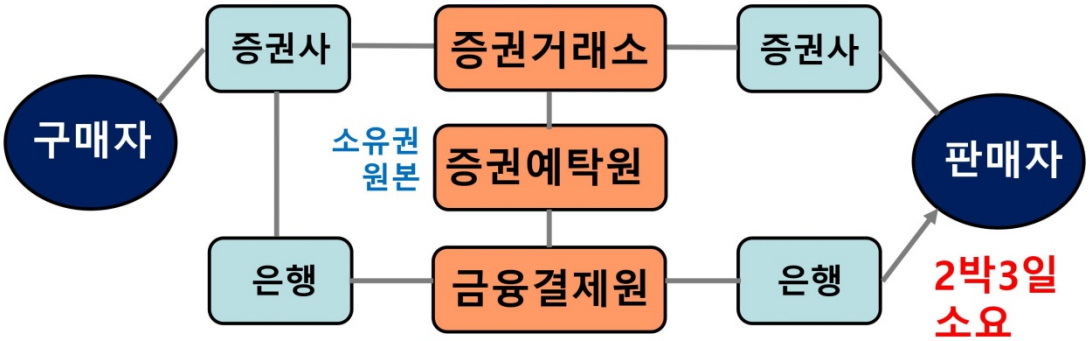
카드업계

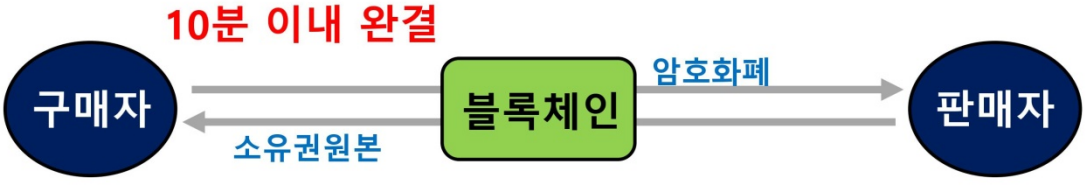
- 각 카드사별로 블록체인을 인증 기술에 적용
- 간편인증, 포인트관리, 간편송금으로 적용 확대

29

증권거래

민간 TTP Trusted Third Party
공공 TTP 제3의 신뢰기관





보험업계

- AIG와 IBM 블록체인 기반 스마트 보험계약 시스템 구축

- Aegon, Allianz, Munich Re, Swiss Re 및 Zurich는 2016년 10월 블록체인 컨소시엄인 B3i (Blockchain Insurance Industry Initiative)를 출범함
  - 이후 10개의 (재)보험사들이 합류하여, 현재는 15개의 (재)보험회사들로 구성된 최대의 보험산 업 블록체인 컨소시엄임. 2017년 12월까지 상용화하는 것을 목표로 하고 있음
  - 재보험 계약의 체결, 보험료 납입, 보험사고 보고 및 보험금 정산이라는 일련의 과정을 블록체인으로 처리 가능하도록 시스템 구축

유통분야 활용사례

- 공급체인(supply chain)상 상품의 원재료에 이르기 까지 추적 관리가 가능하여 업무의 효율화와 비용절감

- 표시나지 않는 바꿔치기 (silent change) 방지
  - 정규계약의 제조회사만이 할 수 있는 전자서명이 들어있는 블록체인거래로 위조방지, 제조책임 명확화

유통분야 활용사례(계속)

- 물건과 정보의 일치, 유통도중의 상태를 가시화해 제조회사에서 소비자에게 전달되는 과정을 추적 확보
  - 물리적인 로케이션(물건이 어디에 있는지)을 관리
    - ㅇㅇ항 xx 컨테이너, aa 창고 bb 선반 등
  - 논리적인 로케이션을 관리
    - 검품 중, 보관 중, 포장 중, 파킹 중, 이송 중 등
  - 상품의 소유권을 관리
    - 제조회사, 유통회사, 점포, 소비자 등

다이아몬드를 합법화하고 사기를 줄인다

everledger

What?

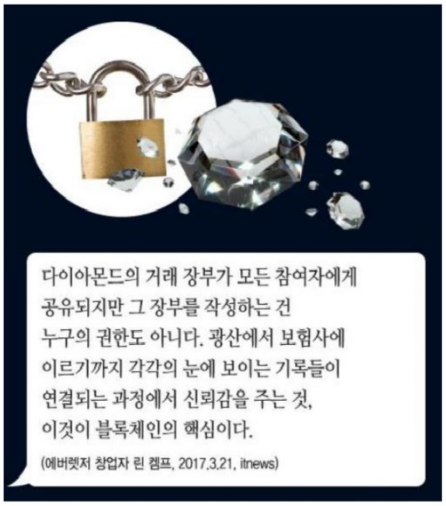
- 광산에서부터 리테일러까지 다이아몬드 공급망을 추적
- 에버렛저(everledger) : 2015년 4월 출시

How?

- 원산지를 증명하는 종이문서 대신 블록체인 기반 전자인증서(Digital Certification)를 활용해 디지털 장부를 발급하여 이전 거래 내역, 현재 소유주에 대한 기록을 공유
- 훔친 다이아몬드를 보석상에 판매하려고 시도하면 보석상 주인은 에버렛저에 이력을 요청하고 도난 다이아몬드라는 사실이 확인될 경우 중개인은 인수거절하고 에버렛저는 경찰과 보험회사에 이에 대한 정보를 자동으로 제공

Benefits

- 사기, 절도, 암시장, 밀매 등의 발생으로부터 보호
- 진위 감별을 돕고, 인조를 진짜 보석으로 둔갑시켜 유통하는 경우의 수를 줄임
- 보험사, 은행, 그리고 수당 청구자의 국경간 거래의 투명성
  검증의 속도 (speed of transparency) 를 증가시킴



중국의 "농장에서 식탁까지" 음식추적

Walmart

What?

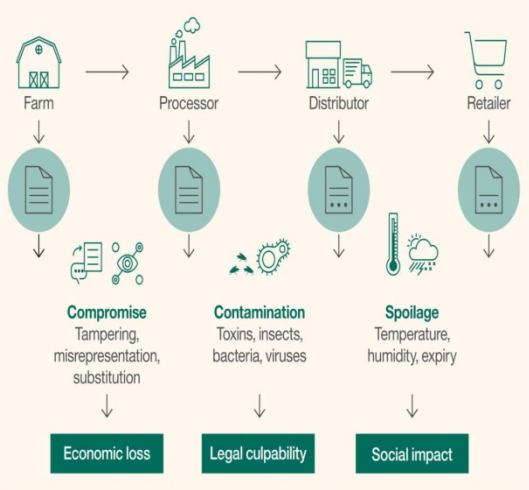
- "농장에서 식탁까지"의 음식 추적

How?

- 블록체인은 각 식재료의 전 공급망 프로세스 과정에 대한 내용을 보유

Benefits

- 신뢰의 향상 : 참여자가 많아질 수록 강화
- 손상된 음식의 근원을 정확히 찾아내어 불필요한 대량 리콜 사태를 줄임
- 음식 공급망의 조화/조정 (co-ordination) 향상



무역관련 업무 스마트계약화

- 무역관련 매매계약 사인,
- 신용장 발행의뢰와 통지,
- 선화증권 인도,
- 대금지불 등 일련의 과정을 블록체인으로 스마트계약을 통해 자동화

콘텐츠를 직거래 하다

What?

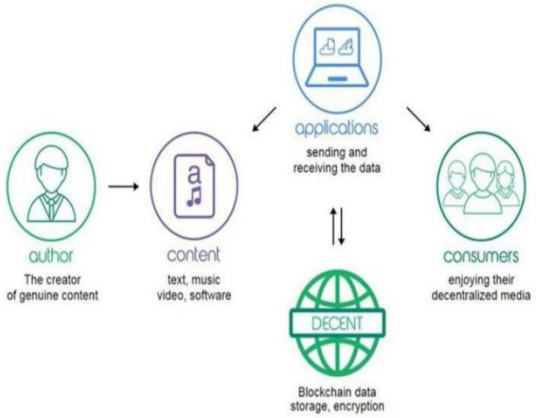
- 예술가 콘텐츠 직거래 플랫폼
- 디센트(DECENT) : 2017년 XX월 출시

How?

- 블록체인 기반 제3의 플랫폼 도움 없이 개인간 거래 가능 → 책, 음원, 영상, 그림, 사진 등
- 예술가들이 IP권한을 갖고 가격과 거래를 직접 결정하고 구매자들은 예술가들의 계좌로 직접 송금(추가 수수료 없음)

Benefits

- 소수 업체에 부여된 독점적 지위와 통제에서 벗어나 예술가들이 자유롭게 콘텐츠 거래 가능
- 콘텐츠 산업을 투명하고 공정하게 부응시키며, 예술가들의 수익 향상 도움



게임 오락 (게임코인)

- 현재의 게임개발회사와 게이머 매매구조
  - Apple Store, Google Play에서 다운받아 사용
  - 이 때 매출액의 30% Apple이나 Google Play
- 블록체인을 이용해 게임개발화사와 게이머 간 직접 P2P거래로 획기적인 거래비용 감축

암호화폐와 블록체인 기반 온라인 게임

CryptoKitties

What?

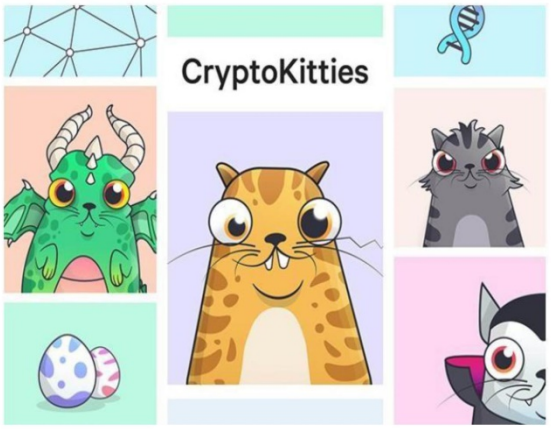
- 가상의 펫(애완동물) 육성 게임
- 액시엄젠(AxiomZen) : 2017년 12월 출시

How?

- 블록체인 기술과 가상화폐 이더리움 기반의 온라인 게임
- 깜찍하고 귀여운 고양이 캐릭터를 수집, 교배,
  가상화폐를 통하여 판매 → 유일한 고양이 탄생
- 게임에서 사용되는 모든 거래 장부와 데이터가 블록체인 방식으로 기록되어 원천적 해킹 불가

Benefits

- 가상화폐 거래와 재미의 두 마리 토끼를 다 잡다
- 가상화폐(이더리움) 거래 활성화에 도움 및 긍정적 이미지 부각



Loyalty Points Exchange (China Union Pay)

What?

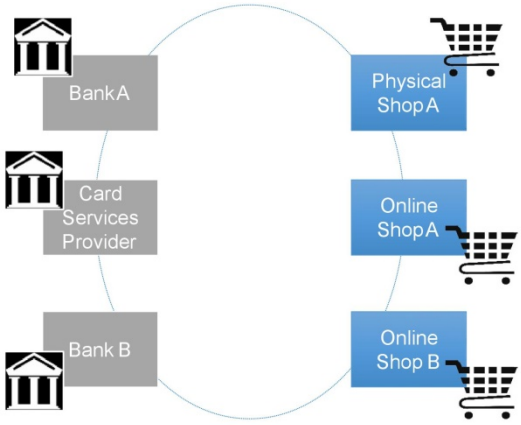
- 고객들이 구매 등의 행위를 통해 얻은 포인트들을 서로 교환하는 플랫폼
- 각 은행별 '보너스 포인트'는 자유롭게 상호교환이 안되므로, 시장 전체에 많은 미사용 포인트들 존재

How?

- 블록체인 네트워크를 통해 은행들이 허용된 파트너간에서만 로열티 포인트를 교환 가능토록 보장

Benefits:

- 서로 다른 은행들이 제공하는 혜택을 개방함으로써, 새로운 고객을 유치하고, 사용 가능한 혜택이 늘어난 고객들의 충성도를 향상



미래 새로운 공유경제를 꿈꾸다

slock.it

What?

- 중개 플랫폼 없이 개인간(P2P) 거래가 가능한 시스템 → 스마트 도어락

How?

- 블록체인 기반의 '스마트계약(Smart Contract)' 시스템으로 일정 조건을 만족하면 자동으로 거래가 수행
- 빈집을 여행자에게 대여할 경우 집주인이 입금내역을 확인하면 여행자에게 자동으로 스마트폰으로 도어락을 열 수 있는 권한 부여

Benefits

- 우버와 에어비앤비와 같은 중개 플랫폼 없이 공급자와 소비자에게 신뢰성 확보
- 집, 자동차, 자전거 등 개인이 소유하고 있는 자산을 공유해 안전하게 거래할 수 있는 공유경제 기반 마련

지역발전을 위한 화폐 발행

- 지역기업이 이점을 가지는 인센티브 부여를 통해 지역발전에 기여할 수 있도록 프로그램화된 지역화폐 발행
  - 특정지역의 숙박시설, 가게 등에만 사용할 수 있는 지역화폐를 발행해 해장지역에서만 사용할 수 있도록 하여 지역경제 발전에 기여

- 법정화폐를 보완하는 수단으로 도입된 **지역화폐**는 **지역경제 발전의 원동력**을 지역 내부에서 찾아 활용되는 특징을 가지고 **지역경제 자립과 활성화**의 **선순환** 을 만들어내는데 의의

지역화폐 현황 01

서울	인천	광주	경기	강원	충북	총 60개
1	2	1	2	10	9	
충남	전북	전남	경북	경남	제주	올 해 약 10개 지역 추가 발행 예정
7	5	8	7	7	1	

지역화폐 분류

- 지역공동체 유대 강화
- 소외계층 지원 및 자립
- 관광, 문화, 레저 예술 활성화
- 골목상권 등 지역 경제 활성화
- 특정행사 참여 유도

지역화폐 현황 02

지역경제 활성화

마포구 지역화폐 '모아'

- 2016년 발행
- 가맹점 180여곳
- 누적된 유통규모 2억여원

지역공동체 유대 강화

대전의 '두루'

- 2000년 발행
- 회원수 651가구
- 매년 1만~15000건 거래
- 약 3억원 가량중 50%이상을 지역화폐 두루로 거래
- 주민 주체 발행

소외계층 지원

성남의 '성남사랑상품권'

- 2006년 발행
- 청년배당 명목
- 7000여개 가맹점
- 소외계층 지원

관광 활성화

'화천사랑상품권'

- 축제장 입장료 일부를 지역화폐로 반환
- 입장료 부담을 줄여 더 많은 관광객 유치
- 지역 내 소비 유도

노원 지역화폐

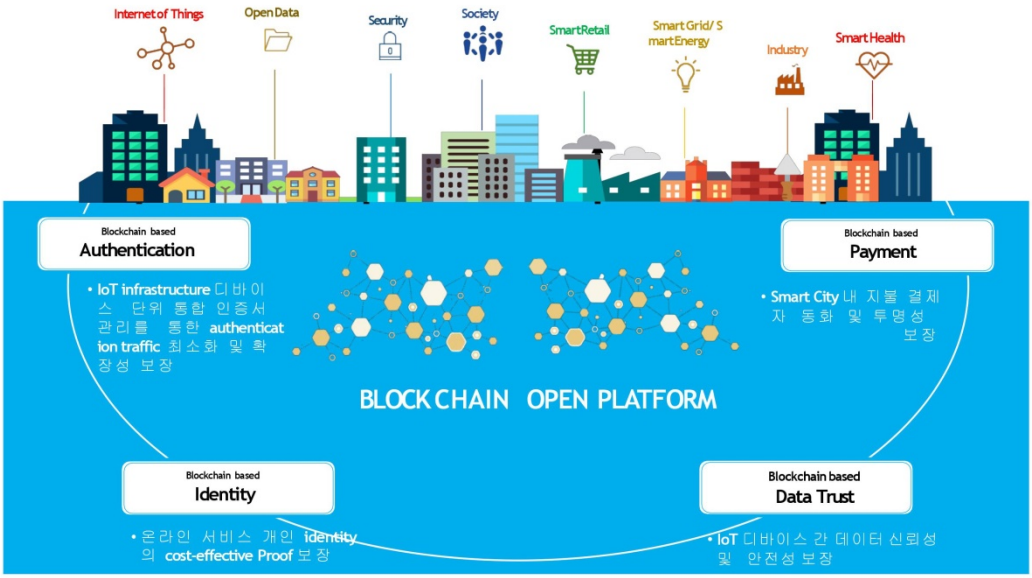
사회적 가치를 경제적 가치로의 전환

봉사활동 · 기부

지역화폐 지급
(봉사활동 1시간에 700NW 지급)

가맹점에서 사용
(애플리케이션 · 회원카드)

Smart City Future



22

"항저우를 현금·종이없는 블록체인 도시로"...中의 飛上

완샹그룹, 33조원 투입 7년내 완공
中정부 인프라·규제철폐 등 전폭 지원

중국 상하이 푸둥신구에 위치한 완샹블록체인연구소.

20여 명의 직원이 컴퓨터 앞에 앉아 신도시 개발 프로젝트를 진행하고 있다. 자동차 부품업체 완샹그룹이 설립한 이 연구소는 블록체인 기술에 특화한 비영리 연구기관이다. 제조업체가 블록체인 연구에 뛰어든 것은 블록체인 기반 스마트시티를 설립한다는 원대한 목표를 가지고 있기 때문이다. 완샹그룹은 지난해 9월 상하이에서 열린 글로벌 블록체인콘퍼런스 현장에서 "블록체인 기술에 기반해 운영되는 도시를 건설하겠다"고 선언해 주목을 받았다.

중국 상하이·항저우 블록체인 프로젝트

:

(출처 : 매일경제)

블록체인 플랫폼 경쟁

블록체인 플랫폼을 둘러싼 치열한 경쟁은 다양한 방식으로 진행 중

Top 10 Capital Markets Chaintech Platforms: Securities Settlement in Focus

HYPERLEDGER — Hyperledger's Fabric
Chain — Chain Core
corda — R3's Corda
Nasdaq — Nasdaq Linq
ENTERPRISE ETHEREUM ALLIANCE — Enterprise Ethereum
AXONI — Axoni AxCore
Digital Asset — Digital Asset platform
symbiont — Symbiont's Assembly
SETL OpenCSD — SETL's OpenCSD
t0 T ZERO — Overstock.com's t0

(출처 : Aite Group)

주요 민간 분산원장기술 컨소시엄

컨소시엄	참가기관	주요 특징
R3 컨소시엄	미국 IT기업 R3사 설립 100여개 대형 금융회사 국내 5개 은행(국민, 신한, KEB하나, 기업, 우리)	-금융회사 계약 기록관리 시스템 (Corda) 개발
Hyperledger	리눅스재단이 관리 금융회사 및 비금융 IT기업 등 100여개 기업 국내 기업 (한국예탁결제원, 코인플러그, 삼성SDS)	- 오픈소스 - 범산업용 블록체인 플랫폼을 연구 개발
SBI 핀테크 컨소시엄	일본 SBI 금융그룹 주도 리플, 코인플러그 등 참여	- 아시아에서 활용 가능한 블록체인 플랫폼 개발 - R3와 이더리움 재단 자문
Chinaledger	중국 완샹 블록체인 랩 주도 중국 11개 대형 금융회사 참여	중국 내 금융회사 간 통용할 수 있는 오픈소스 블록체인 플랫폼 개발

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

디지털국가 디지털정당

블록체인기반 전자투표

- 주주총회
- 국민투표

- 보안성, 신뢰성,
- 시간・비용 절감
- 유권자의 익명성 보장

블록체인 디지털국가 에스토니아

- 수도: 탈린, 면적452만 3천ha 세계130위 (2015 국토교통부 기준)
- 인구130만 3,798명 세계156위 (2019 통계청, UN, 대만통계청 기준)
- GDP259억 2,107만 9,612.3달러 세계97위 (2017 한국은행, The World Bank기준)
- 1인당 GDP1만 9,704.66달러 세계38위 (2017 한국은행, The World Bank, 대만통계청 기준)
- 종교루터교, 러시아정교

- 2014년부터 블록체인 기술을 활용한 '이레지던시'라는 전자 시민권, 가상영주권 발급
  - 전자 시민권은 온라인으로 신청하고 100유로를 내면 누구나 발급받을 수 있음
- 발급 후에는 에스토니아 시민이 되어 가상영토에서 창업 및 정부가 제공하는 행정 서비스를 누릴 수 있음
- 에스토니아의 블록체인 인터넷 투표
  - 블록체인 기술의 보안성, 신뢰성, 시간·비용 절감 효과와 함께 유권자의 익명성도 보장

- 2014년 가상영주권 도입 후 3년 만에 150여 개 국가에서 4만 7천여 명 가상영주권 발급, 한국인도 1300여 명

- 창업 6000여 개,
- 2021년까지 2만 여개 기업 창업 전망

- 2025년까지 인구의 10배인 1000만 명 가상영주권 발급,

- 약 100만개 기업창업 전망, 엄청난 세수 예상: 에스토니아 만의 저출산 고령화 대책

가상영토 시대

- 가상영토

- 가상인구

- 가상기업

* 어느 국가가 블록체인 기반 더 넓은 가상영토 가상인구 가상기업을 가질 것인가
  => 부국의 조건

디지털 정당 시대

- **호주의 정당 플럭스**를 시작으로 이태리 오성운동, 스페인 포데모스, 덴마크 자유연합 등이 당내 의사결정시스템에 블록체인 기술을 적용해 모든 투표를 블록체인으로 진행하는 디지털 정당으로 변신

디지털 정당 운영

- 블록체인 기반 당운영 플랫폼 구축
- 당원 디지털ID발급
- 당원과 당의 직접 의사소통을 통한 당운영 민주화 투명화
  - 플랫폼을 이용한 당원과 국민들 제안
  - 제안된 안건에 대한 토론
  - 일정 수준 도달한 제안은 입법화
- 당대표 대선후보 선출시 디지털ID이용한 당원 직접투표
- 플랫폼을 이용한 비당원과 의사소통 확대, 당 기반 확충
- 보다 많은 참여 동기부여 위한 보상코인 발행 지급
- e-Learning

이태리 "오성운동"의 디지털 플랫폼

2009년 창당

2013년 제3당

2016. 6 로마, 토리노시장 당선, 전국정당으로 부상

2018. 3 제1당 연정 집권

한국의 디지털 정당화

- 자유한국당 더불어민주당 등 디지털 정당화 박차

암호화폐 동향과 규제 동향

가상화폐 채굴장면

상장된 코인 채굴되면 바로 거래소에 연결

•CryptoCurrency Market Capitalizations (2018. 4. 12)

Cryptocurrencies: **1565,** / Markets: **10245,** Market Cap: **$325,588,033,575** / 24h Vol: **$23,270,616,453** / BTC Dominance: **42.0%**

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)
1	BTC Bitcoin	$136,892,311,030	$8,064.20	$7,990,060,000	16,975,312 BTC	5.37%
2	ETH Ethereum	$51,015,719,753	$516.38	$2,590,990,000	98,794,344 ETH	11.44%
3	XRP Ripple	$26,186,725,443	$0.669347	$1,420,320,000	39,122,794,968 XRP *	20.17%
4	BCH Bitcoin Cash	$12,912,026,148	$756.37	$412,568,000	17,071,113 BCH	6.65%
5	LTC Litecoin	$7,335,752,717	$130.85	$524,152,000	56,063,163 LTC	7.26%
6	EOS EOS	$7,153,586,066	$9.05	$1,041,800,000	790,809,766 EOS *	2.36%
7	ADA Cardano	$5,519,406,630	$0.212882	$277,904,000	25,927,070,538 ADA *	10.99%
8	XLM Stellar	$4,806,105,637	$0.258956	$111,912,000	18,559,545,393 XLM *	15.44%
9	NEO NEO	$4,305,333,500	$66.24	$196,190,000	65,000,000 NEO *	7.80%
10	MIOTA IOTA	$4,122,071,205	$1.48	$101,180,000	2,779,530,283 MIOTA *	24.08%
11	XMR Monero	$3,128,318,294	$196.44	$58,212,200	15,925,057 XMR	6.79%
12	DASH Dash	$3,008,886,339	$375.75	$92,938,900	8,007,660 DASH	10.30%

암호화폐 거래 시장 만개 돌파

<2019년 5월 3일>

Cryptocurrencies: 2143

Markets: 18126

MarketCap: $177,495,613,047

24h Vol: $43,514,905,466

BTC Dominance: 54.8%

•CryptoCurrency Market Capitalizations (2019. 5. 3)

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$97,220,392,993	$5,499.21	$14,237,205,192	17,678,975 BTC	2.09%	
2	Ethereum	$17,020,249,784	$160.71	$5,667,755,573	105,904,450 ETH	0.00%	
3	XRP	$12,738,612,757	$0.303264	$881,787,015	42,004,966,728 XRP *	-0.29%	
4	Bitcoin Cash	$4,766,126,690	$268.36	$1,472,097,265	17,760,400 BCH	-0.53%	
5	Litecoin	$4,513,952,589	$73.28	$2,782,173,192	61,599,558 LTC	-0.28%	
6	EOS	$4,461,730,871	$4.73	$1,617,477,092	944,123,306 EOS *	-0.83%	
7	Binance Coin	$3,348,507,657	$23.72	$251,673,903	141,175,490 BNB *	8.74%	

비트코인 가격 동향

암호화폐 성격

- 미국: 가상화폐를 '교환의 매개, 회계단위 또는 가치저장 기능 수단으로 사용가능하지만 법정통화 지위는 없는 전자적 단위'로 정의.

(2015년 9월에 발표된 미국의 주은행감독협의체 (CSBS: Conferences of State Bank supervision)의 가상화폐 표준 규제체계(State Regulatory requirements for Virtual Currency Activities: CSBS Model Regulatory Framework)

- 일본: 가상통화는 결제수단의 하나로 재산적 가치를 지니며 불특정 다수간의 지불수단기능 및 법정통화와의 교환기능과 전자거래기능을 갖지만 법정통화는 아닌 것으로 정의

(2016년 5월 가상통화 서비스업체의 등록 및 규제를 위한「자금결제에 관한 법률」개정안이 국회를 통과하고 2017년 4월에 시행. 이 개정 자금결제법 2조 5항에서 '가상통화 ' 규정)

사례연구: 일본 자금 결제법 개정의 주요내용

법령		주요내용
가상화폐교환업 (가상통화거래소)		• '가상통화교환업'에 대한 규제가 자금결제법 개정의 주요내용임. • 상법상의 회사로 간주되어 파산할 경우 민사재생 또는 파산절차를 거쳐야하며, 이때 이용자는 자산 상실의 우려가 있음.
	가상통화의 정의 (제2조5)	• 가상통화는 결제수단의 하나로 '재산적 가치 ' 를 지님. • '재산적 가치 ' 란 가상통화가 불특정다수 간의 지불수단 기능 및 법정통화와의 교환기능, 전자거래 기능을 갖지만, 법정통화는 아님.
	가상통화교환업에 대한 등록제 도입 (제63조2)	• 가상통화교환업을 수행하려면 자본,순자산(자본,순자산에 대한 구체적인 금액에 관해서는 현재 검토중임) 등에 관한 요건이 충족되어야 하며 총리대신에게 등록을 받은 자만이 가상통화교환업을 운영할 수 있도록 규정함
	가상통화교환업자에 대한 업무규제 (제63조 11)	• 가상통화교환업자는 이용자와의 거래내용 및 수수료 등의 정보, 시스템의 안전관리 등에 관한 사항을 정기적으로 공인회계사 또는 감사법인에게 감사받아야 함.
	가상통화교환업자에 대한 감독(제63조13)	• 가상통화 교환업자는 공인회계사 또는 감사법인의 감사 보고서를 첨부한 해당 보고서를 내각총리대신에게 제출해야 하며, 금융청으로부터 업무개선 명령 등의 감독을 받아야 함.

자료:「 자금결제법 개정안과 가상통화(디지털 통화) 이용현황」 금융브리프 25권 29호 (2016.07.23~29), 금융연구원

미국 유럽 암호화폐 규제동향

	정의	규제	과세	ICO
미국	자산/ 화폐	거래소 등록	자본이득세 / 소득세 부과	적격투자자제도
일본	화폐	거래소 등록	소비세 면제. 거래차익 잡소득으로 과세	허용.
영국	민간화폐	거래소 등록	부가가치세 폐지 거래수익 비과세 법인세 부과	허용
독일	금융상품	거래소 등록	투지거래 소득세 25% 부과 채굴, 개인거래 비과세	허용
스위스	지방정부화폐 지방결제수단. 물건 등 자산	스위스 금융시장감독위원회(FINMA) 라이선스	부가가치세 없음 법인세 14.6%(Zug) 개인자본소득 비과세	허용. 크립토밸리 육성

규제 동향 요약

- 암호화폐를 자산, 금융자산 또는 민간화폐로 인정하는 추세 확산
- 투자자보호를 위해 거래소는 등록제를 도입하는 추세
- 과세는 부가가치세 면세, 거래소득 비과세 추세 (화폐로 간주) 속 미국 일본은 소득세 과세
- ICO는 증권형토큰은 증권으로 간주 증권거래법 규제, 지불형코인/토큰은 자금세탁방지시스템(AML) 고객신원확인(KYC) 구축 요구. 반면 유틸리티토큰은 비규제 추세
- 점차 제도 구축되면서 암호화폐 사용 확산 전망

디지털화폐와 디지털금융 시대

화폐의 역사

상품화폐

↓

금속화폐

↓

법정화폐

↓

디지털화폐

거래의 효율성을 높이는 방향으로 발전해 옴

CBDC (Central Bank Digital Currency)

자국 발행 디지털 e-머니를 실험 중인 중앙은행

디지털화폐와 현금 및 전자화폐 비교

	현금	전자화폐	디지털화폐
발행기관	중앙은행	금융기관, 전자금융업자	없음
발행규모	중앙은행 재량	법정통화와 1:1 교환	알고리즘에 의해 사전 결정
거래기록 및 승인	불필요	발행기관 및 청산소	분산원장 이용 P2P 네트워크
화폐단위	법정통화	법정통화와 동일	독자적인 화폐단위
법정통화와 교환 여부	-	발행기관이 교환을 보장	가능하나 보장되지 않음
법정통화와의 교환가격	-	고정	수요-공급에 따라 변동
사용처	모든 거래	가맹점	참가자

자료: 한국은행 2016

암호화폐 전문 상업은행 등장

- 암호화폐계의 거물 노보그라츠는 2월 2억 5000만달러를 모금해 "갤럭시 캐피털"이라는 암호화폐 전문 상업은행을 설립할 계획이라고 발표.

- 암호화폐만 취급. 암호화폐 자산관리, 거래, ICO, 시장 조사 등 암호화폐와 관련한 업무를 전문적으로 처리할 계획이라고 발표.

암호화폐 전문 투자펀드도 속속 등장

- 2017년 월가를 떠난 매트 괴츠는 암호화폐 투자회사 블록타워 캐피탈을 설립

- 코인베이스도 본업인 암호화폐 거래소를 넘어 암호화폐 스타트업 육성을 위한 투자기업 '코인베이스 벤처' 설립을 공식 발표.

블록체인 기반거래 국제규범도 추진

- 최근 EU집행위원회는 영국을 포함한 22개 EU 회원국이 '유럽 블록체인 파트너십' 출범에 공동서명했다고 발표.

- EU를 블록체인 기반 단일 금융시장으로 발전시키자는 원대한 계획 추진

블록체인과 통화제도 통화정책

- 법정화폐와 민간화폐의 공존

- 중앙은행제도 vs 자유은행제도

- 기술혁신 vs 통화제도의 안정성

  – 거시경제 단기 안정화 위한 통화정책의 운용방식

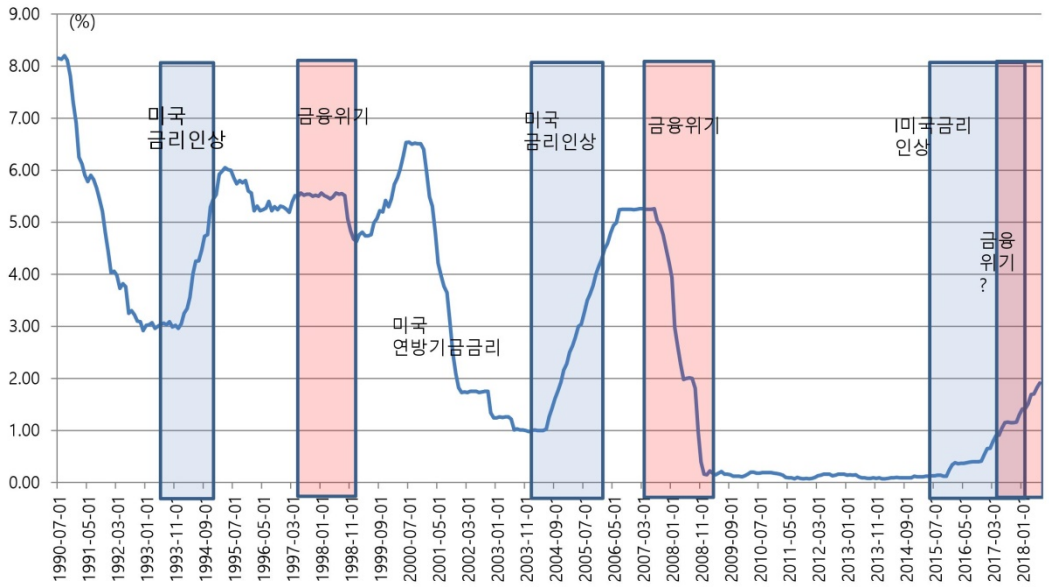
국제기축통화제도에 미칠 영향

- 현재: 달러 유로 엔 파운드
- 미래: 달러 유로 엔 파운드 + 암호화폐
- 암호화폐 많이 보유=외환보유액 많이 보유 기능하게 되는 시대 도래 전망
- 스테이블 코인 등장

트리핀의 딜레마(Triffin''s dilemma)

- 기축통화 발행국은 기축통화의 국제 유동성을 유지하기 위해 경상수지 적자를 지속해야 한다. 이럴 경우 기축통화에 대한 신뢰도가 하락할 수 밖에 없는 문제가 발생한다. 그러나 신뢰도를 유지하기 위해 긴축정책을 펴면 경기 침체를 불러 올 수밖에 없는 딜레마에 빠지게 된다는 이론
- 미국 예일대 교수였던 로버트 트리핀(Robert Triffin)이 미국 의회 연설에서 "미국이 경상적자를 허용하지 않고 국제 유동성 공급을 중단하면 세계 경제는 크게 위축될 것"이라면서도 "그러나 적자 상태가 지속돼 미 달러화가 과잉 공급되면 달러화 가치가 하락해 준비자산으로서 신뢰도가 저하될 것"이라고 한 데서 비롯

국제금융위기 예방에 기여할 수 있을 것인가



암호화폐와 부패방지, 포용금융

가상화폐와 부패방지

- 중세 르네상스시대 글로벌 무역에서 막대한 금은보화를 축적한 이태리I 베네치아 피렌체 상인들이 금은보관증서를 유통시키며 시작된 은행업은 엄청난 부를 축적하는 과정에서 정경유착의 부패고리가 형성. 이러한 부의 축적과정은 현대의 금융그룹도 예외가 아닌 실정

- 특히 관치금융이 심한 나라일수록 언제나 정경유착의 부패문제가 심각. 특히 거대금융그룹의 과도한 탐욕은 2008년 글로벌금융위기와 같은 금융위기를 초래해 세계경제를 강타

- 가상화폐는 이러한 관치금융과 정경유착 부패의 고리인 금융업의 중개를 필요 없이 블록체인이라는 신뢰 시스템을 기반으로 한 쌍방거래이어서 관치금융과 정경유착 부패 문제를 획기적으로 감소시킬 전망 (하바드대 로고프 교수의 근간『현금의 저주』).

가상화폐와 부패방지(계속)

- 암호화폐의 출현이 경제의 효율을 획기적으로 증진시켜 새로운 부를 창출함은 물론 많은 사람들을 중앙화된 엘리트중심의 금융권력으로부터 자유롭게 할 전망

- 암호화폐가 범죄에 악용될 것이라는 우려도 있으나 이는 현재 세계적으로 논의되고 있는 고객신원확인(KYC) 자금세탁방지(AML) 강화로 상당부분 해결될 수 있을 것으로 전망

가상화폐와 포용적 금융

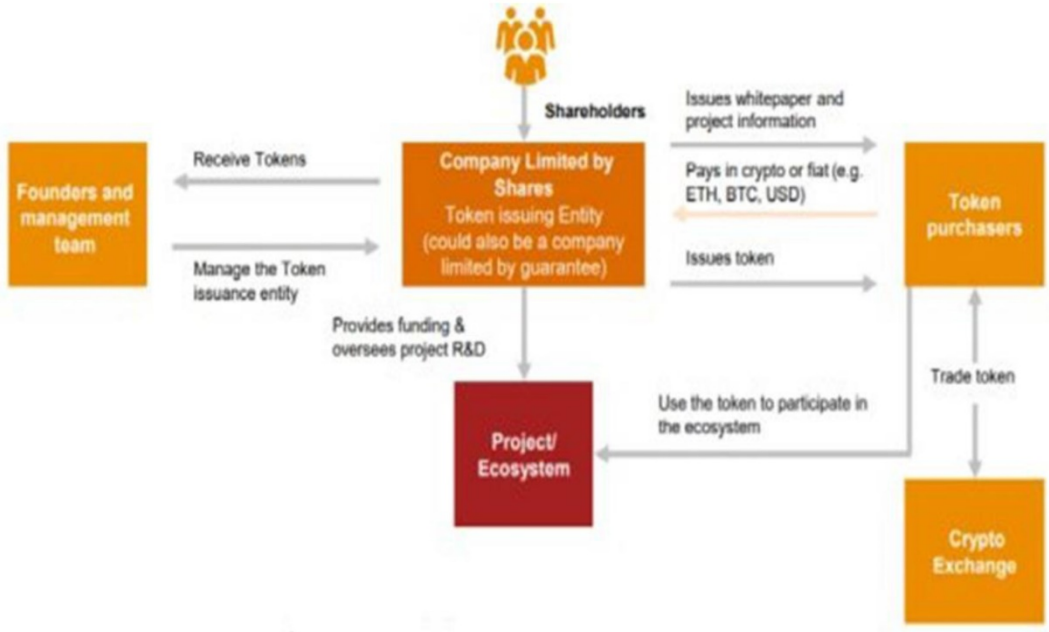
- 중국 서남아시아 중동 아프리카 등 25억 명 정도의 인류는 아직도 은행계정을 갖지 못하고 있지만 상당수는 모바일폰은 가지고 있음

- 스마트폰의 등장과 이로 인해 가능해진 쌍방(P2P)거래를 근간으로 하는 P2P대출 크라우드펀딩 인터넷전문은행 등 모바일금융은 이들에게 생애 처음으로 금융이라는 것을 이용할 수 있는 기회를 제공. 금융포용이 확산. 빈곤 탈출의 기회 제공

- 가상화폐의 출현은 금융소외 계층에 금융포용의 새로운 기회를 제공. 모바일폰을 통해 비트코인을 전송해 새로운 삶의 기회를 제공 (폴 비냐, 마이클 케이시 공저인 『암호화폐 시대』(The Age of Cryptocurrency)(2016))

폭발적으로 늘어날 ICO

ICO의 개념과 구조



블록체인 암호화폐 시대의 자본시장 구조

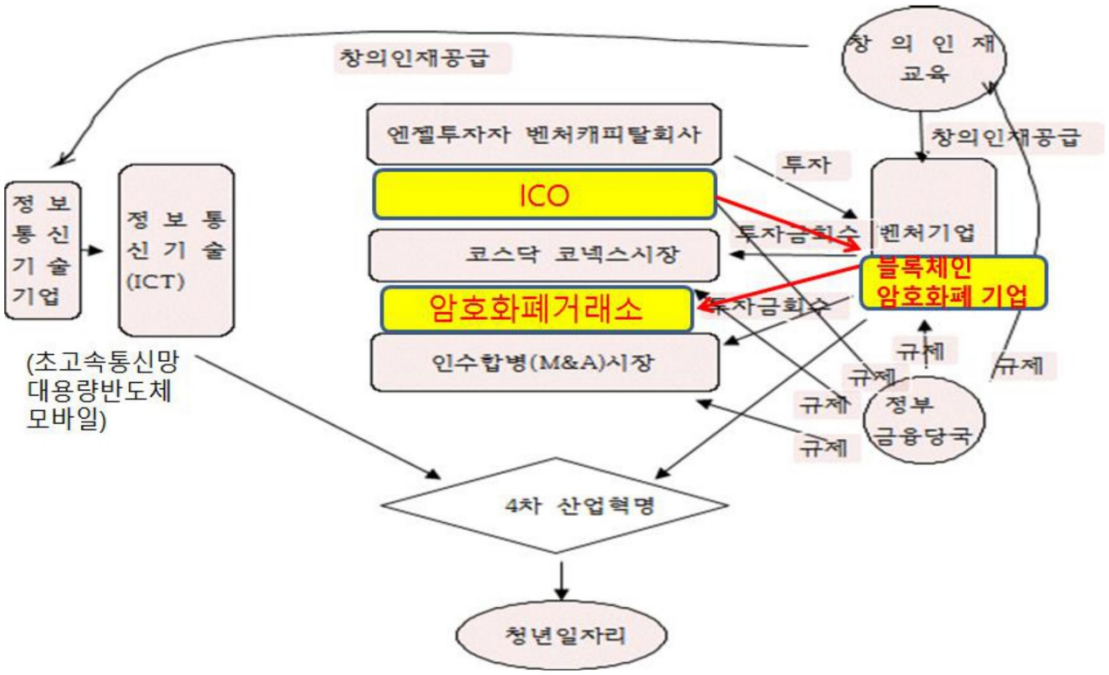
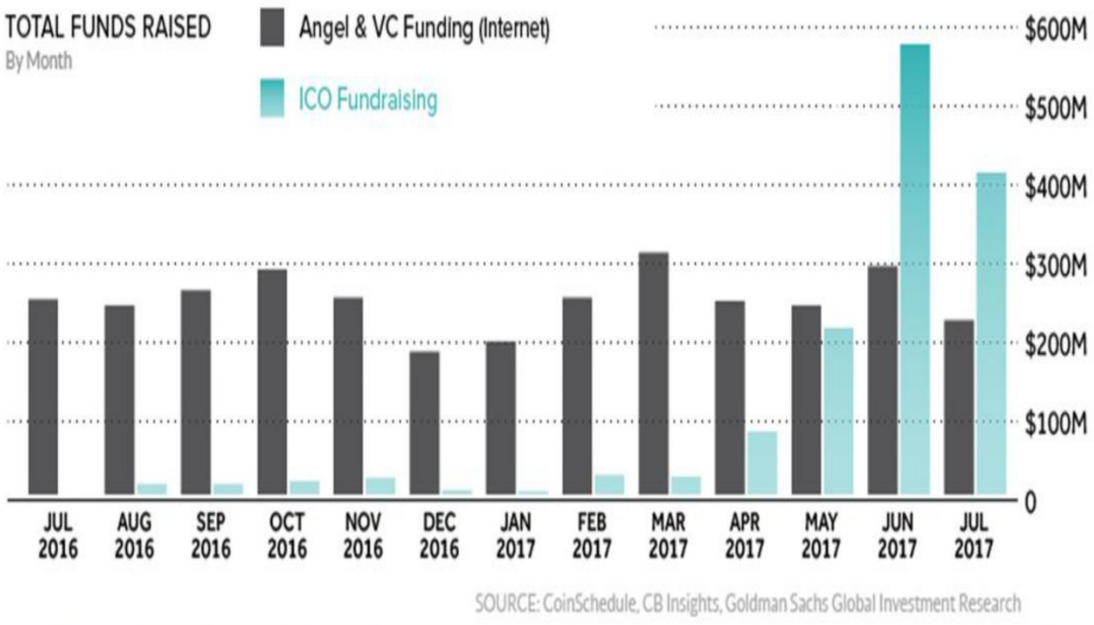


그림: 오정근「4차 산업혁명시대 ICO의 중요성과 글로벌 동향」2018

지역별 ICO 현황

최근 ICO 추이



점차 벤처스타업들의 자금조달원으로 ICO가 더 많이 활용되기 시작

2017년 ICO

Total: **$3,880,018,203**

Total Number of ICOs: 210

Position	Project	Total Raised
1	Hdac	$258,000,000
2	Filecoin	$257,000,000
3	EOS Stage 1	$185,000,000
4	Paragon	$183,157,275
5	Bancor	$153,000,000
6	Status	$90,000,000
7	BANKEX	$70,600,000
8	TenX	$64,000,000
9	Nebulas	$60,000,000
10	MobileGO	$53,069,235

자료: coinschedule

2018. 1~3월 중 ICO

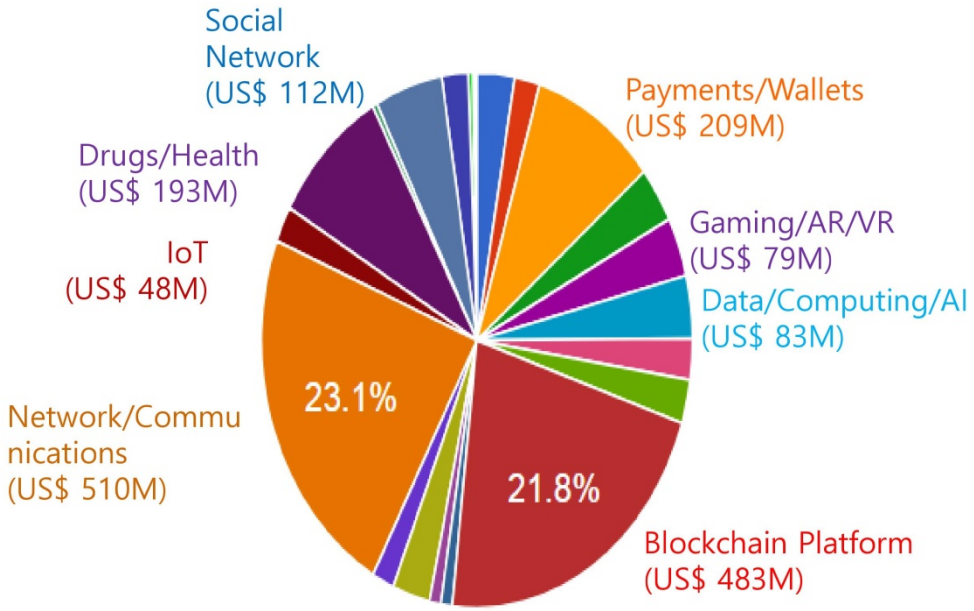
Total: **$2,653,302,364**

Total Number of ICOs: 67

Position	Project	Total Raised
1	Telegram ICO (Pre-sale 1)	$850,000,000
2	Huobi token	$300,000,000
3	Envion	$100,000,000
4	Neuromation	$71,669,400
5	Crypterium	$51,656,963
6	SwissBorg	$50,000,000
7	Lendroid	$47,500,000
8	iungo	$45,978,800
9	Fusion	$42,185,216
10	Bloom	$41,420,705

자료: coinschedule

산업별 ICO 현황



투자자보호

투자자 보호 1: 건전한 거래소 정비

- 건전한 가상화폐 거래소 등록/인가 등 거래 생태계 구축
  - 일본 최대 거래소 해킹 사건의 교훈

코인체크는 2017년 일본 금융청(FSA)에 등록한 15개의 거래소가 아니었음

대부분의 코인을 외부인터넷과 연결된 전자지갑인 핫월렛에 저장하고 있었음. . 미국 거래소 코인베이스가 전체 암호화폐의 97%를 외부인터넷과 연결되지 않는 콜드월렛에 저장

주요 거래소에서는 비밀키를 여러 개 사용하는 다중증명기능을 사용하고 있는데 이 거래소는 비밀키를 하나만 사용하는 단독서명기능에 의존. 이 경우 하나뿐인 비밀키가 해커 손에 넘어가면 탈취당한 암호화폐를 바로 꺼내갈 수 있음

이런 점들을 볼 때 코인체크 사고는 예고된 사고이라고 해도 과언이 아님.

투자자 보호: 건전한 거래소 정비

- 한국도 조속히 투자자보호를 위한 가이드라인을 정하고 법제화해 등록제나 인가제/등록제를 시행
- 요건에 미달하는 거래소는 즉각 거래를 중지하도록 해야 투자자 손실을 막을 수 있음
- 해킹 파산 등으로 투자자가 입을 손실에 대비한 보험제도, 거래소 전용 이상징후탐지시스템(FDS), 국제공조체제도 구축하는 등 다각적인 투자자보호대책을 강구해야 함
- 문제가 발생하면 무조건 거래소 폐쇄는 올바른 대책이 아님.

투자자 보호 2:
가상화폐 신용평가제도 구축

- 건전한 가상화폐 거래 생태계를 구축하기 위해서는 가상화폐 신용평가제도 구축 필요
  - 미국의 한 신용평가회사가 세계 최초로 74종의 암호화폐에 대한 신용등급을 발표

한국형 암호화폐공개(ICO) 가이드라인

ICO 허용국가와 금지국가

ICO금지 국가	ICO허용 국가			
Ban	Allowed	Allowed/ Regulated	Allowed, but unregulated/Subject to future regulations	Allowed/Subject to future regulations
China **Korea**	Estonia Germany	Australia **United States**	Russia	EU Gibraltar (UK) Hong Kong (China) Isle of Man (UK) Israel Japan Philippines **Singapore** Switzerland Thailand United Kingdom

미국 암호화폐공개

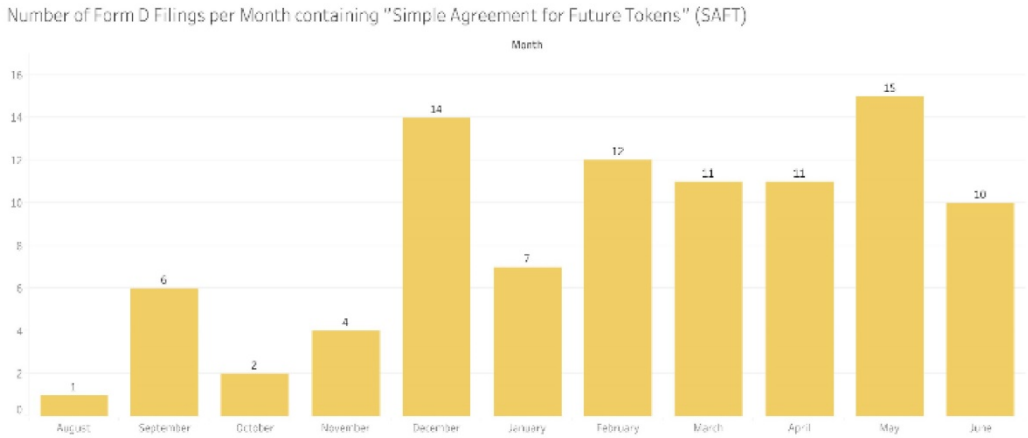
- 2017년 9월, Filecoin, 최초의 SEC 규정을 준수한 ICO ($25M 공모)
- 적격투자자 제도 활용 (SEC Regulation D)
  1. 은행, 투자회사 등
  - .....
  5. 주거주지를 제외한 개별 또는 부부합산 순 자산 100만불 이상
  6. 개인 (최근 2년간 매년 연소득 개별 20만불 이상 또는 부부합산 30만불 이상)
- KYC/AML 등 규정 준수

- 최근 SAFT(Simple Agreement for Future Tokens) 투자 협약서, 방식 확산. 현 미국의 증권법과 규제 준수

ICO의 새 조류 SAFT

SAFT(Simple Agreement for Future Tokens) 투자 협약서, 현 미국의 증권법과 규제 준수

미국 2018 월별 SAFT Filing 건수



자료: 하태형(2018)

103

스위스 FINMA 가이드라인

The table below illustrates the key factors:

	Pre-financing and pre-sale / The token does not yet exist but the claims are tradeable	The token exists
ICO of payment tokens	= Securities ≠ subject to AMLA 지불수단에 중점.	≠ Securities = means of payment under AMLA[3]
ICO of utility tokens[4]	App, 서비스에 대한 디지털적 접근 목적	≠ Securities, if exclusively a functioning utility token = Securities, if also or only investment function ≠ means of payment under AMLA
ICO of asset tokens[4]	기초자산, 수익/배당 등에 대한 참여권. 증권, 파생상품 유사	= Securities ≠ means of payment under AMLA

최근 거래소공개(IEO)도 등장

- ICO 문제점은 첫째, ICO 프로젝트에 대한 검증이 어려움.
  - 증권사가 중간자로 개입하여 회사의 상장 적절성을 검토하고 공모주 청약을 진행하는 기업공개(IPO)와 달리 ICO는 프로젝트의 실체와 경제성을 검증할 수 있는 공식적인 절차가 없음
- 둘째, 투자자 수가 점점 더 줄어들고 있는 추세
  - ICO 과정 중 크라우드 세일을 하지 않고 크립토펀드 사모펀드 등 프라이빗 세일 단계에서 모금을 끝내는 사례가 증가.
  - 많은 투자자가 참여하지 않아서 토큰의 가치는 상승하기 어렵고 프로젝트 또한 지속적인 성장도 보장되지 않을 우려.

- ICO의 대안으로 IEO(Initial Exchange Offering)가 주목 받고 있음.
  - IEO는 거래소에서 ICO 프로젝트의 발행토큰을 받아 거래소 회원으로 제한된 투자자들에게 판매하는 행위. 거래소가 적극적인 중개인으로 투자 모금
- 최소한의 프로젝트 신뢰성이 담보.
  - 프로젝트에 문제가 생겼을 때 모금 주체인 거래소가 그 책임을 분담하므로 거래소는 IEO를 진행하는 프로젝트에 대해 꼼꼼하게 검토를 하고 건전성을 평가하게 됨
- IEO는 크라우드 세일을 보다 간단하고 적은 비용을 진행할 수 있어 보다 많은 사람들에게 토큰을 유통하기 쉬움
  - 거래소 고객을 대상으로 하기 때문에 이미 KYC 등 신원 확인절차가 끝낸 사람들만이 투자에 참여할 수 있으며 마케팅 비용 또한 제한된 타겟을 대상으로 하기에 훨씬 효율이 높고 상장 후 거래를 활성화하는 것도 보다 용이.
- IEO는 투자자들에게는 신뢰를, 프로젝트 주체에게는 마켓팅비용 절감효과를, 거래소에는 신규 고객 유입의 기회를 제공.
- 거래소에 너무 많은 힘이 실릴 수 있다는 문제점도 존재.
  - 탈중앙화를 기치로 건 블록체인 산업에서 거래소라는 중앙화된 기관이 존재하고 강한 영향력을 행사하는 문제점

ICO 인가제 속속 도입…
자율규제기구 표준안도 마련

- 암호화폐 거래 플랫폼인 웨이브즈(Waves)를 창업한 알렉산더 이바노프가 주축이 돼 만들어진 ICO 거버넌스 재단: 고객 파악과 신원 확인(KYC) 및 자금세탁 방지 시스템, 프로젝트 존속 가능성 평가를 위한 비즈니스 사전조사 및 법적 평가제도 등 ICO 표준안을 내놓겠다는 계획

- **DAO와 ICO 결합한 DAICO 대안으로 제시…탈중앙화된 ICO (**이더리움 창시자인 비탈릭 부테린 제시)
- **스마트계약 활용해 기업 출금한도 설정-프로젝트 실패시 환불 요청 가능**
  투표시스템으로 자금 추가모집 등 주요 의사결정에도 참여…지속적 개선 기대

DAO와 ICO를 결합한
DAICO 메커니즘 등장 전망

한국형 암호화폐공개 가이드라인(제안)

- 스위스의 분류 적용
  - 증권형일 경우 증권거래법 준수
  - 지불형일 경우 자금세탁방지 준수
  - 순수한 유틸리티형, 서비스에 대한 디지털접근이 목적일 경우 증권거래법 자금세탁방지 준수 불요
- 미국의 적격투자자 제도 응용
  - 12개월내 50명이 넘지 않는 사모(Private Placement)
  - 기관투자자들에게 판매: 은행, 증권, 보험 및 자산운용사, 펀드등
  - 적격투자자들에게 판매
    - 개인: 순자산 10억원 이상 또는 연소득 2억원, 부부합산 3억원 이상
    - 회사: 순자산 100억원 이상
- 토큰 Pre-sale: IEO방식, 점차 자율규제방식 확대
- 투자자보호를 위해 코인평가회사 육성 (주식 채권의 신용평가회사)

ICO 금지에 따른 블록체인 암호화폐 기업들의 탈한국러시와 국부유출

한국, 블록체인은 육성

- 정부: 블록체인을 신성장 동력 산업으로 선정 육성
  - 한국인터넷진흥원(KISA): 블록체인 시범사업 프로젝트: 기존 6개-> 12개로 확대.
  - 과학기술정보통신부: 4개 시범사업 추진
  - 중앙선거관리위원회(온라인투표), 국토교통부(부동산거래)) 농림축산식품부(축산물이력관리) 외교부(국가간 전자문서 유통) 해양수산부(해양물류)

- 지자체: 제주: 블록체인특구 추진. 서울: 블록체인 5년계획 발표: 마포와 개포에 블록체인단지 조성, 1223억 투입, 충북: 블록체인센터 설립 등

- 국회: 관련 법안 논의 중 (현재 20여 개 법안 제출 중)
  - 최근 "국회블록체인포럼" 출범

한국, 암호화폐는 과도한 '무법'규제

- 암호화폐 실체를 불인정

- 암호화폐거래를 유사수신행위로 간주

- 암호화폐거래소를 단순 통신판매업자로 간주

  - 필요한 건전한 규제도 하지 않아서 영세한 거래소 난립으로 투자자 피해 속출

규제철폐 필요: 적기조례 (Red Flag Act)

https://goo.gl/images/OKf5v8

블록체인 경제을 위한 스마트 규제 필요

1. 블록체인의 법적 지위 부여: 공공 서비스 가능
2. 스마트계약의 법적 지위 부여: 계약 자동화 가능
3. ICO 법적 규제: 건전한 생태계 조성 및 소비자보호 방안 필요

블록체인 규제 원칙 권고(안)

- 불간섭주의(Hands-off Approach): 5월 유럽의회 권고사항
  - 현 단계에서 정부가 선제적 규제(preemptive regulations)를 택하기 보다는 '세심한 모니터링(precautionary monitoring)'을 정책의 기본 기조로 권장됨
  - 상황에서 정책닥국이 블록체인의 기술적 한계나 부작용에 집중하기 보다는 혁신의 과실을 충분히 향유하는데 정책의 우선순위를 두어야 한다는 뜻으로 해석됨
- 블록체인 규제 설계의 접근방법
  - 기술의 발달에 따라 새롭게 등장하는 분야에 대해서는 기존 규제와 충돌하는 부분이 무엇이고 새로 도입해야 할 규제는 무엇인지?
  - 블록체인과 같은 시스템을 법적으로 어떻게 정의할 것인지?
  - 블록체인 자체를 규제한다면 어떠한 유형의 규제가 핵심규제가 되어야 하는지?
  - 어떤 규제강도가 바람직할지?

참고: 지식산업정보원, 차세대 퀀텀닷 신소재 기술개발 동향과 양자정보통신/블록체인 최근 실태

블록체인 규제 설계의 접근방법

1. 블록체인과 같은 신기술이 등장할 경우 '왜 규제를 하려고 하는지'에 대한 목적 및 우선순위를 분명히 함
2. '특정 기술 중심의 규제체계를 유지할 것인지' 여부를 판단함
3. 신기술을 어떻게 분류할 것인지 판단해야 함: Public vs. Private Blockchain
4. 전자금융과 관련된 규제의 경우 기능별 규제(functional regulations)이기 때문에 기존의 금융 업권별 규제 등과 중복될 가능 성이 존재함
   - 거시건전성규제: 금융시스템의 안정성과 신뢰성을 확보하 기 위한 규제
   - 미시건전성규제: 금융기관의 건전성을 확보하기 위한 규제
   - 영업행위규제: 소비자를 보호하고 시장경쟁을 촉진하기 위 한 규제

참고: 지식산업정보원, 차세대 퀀텀닷 신소재 기술개발 동향과 양자정보통신/블록체

사례연구: 일본 vs. 미국

소비자 보호을 위한 규정

- 미국: 뉴욕주의 BitLicense는 고객재산 보호를 위해 고객 재산의 판매 · 이전 · 대출을 금지하고 일정 금액을 채권 또는 신탁 계좌로 보유하도록 의무화하고 있음
  - ✓ CSBS 가이드라인은 이용자의 재산과 분리하여 일정량의 디지털통화를 보유하고 잠재적 리스크 등 계약 내용의 설명을 의무화하고 있음.
- 일본: 정기적인 외부감사 시행과 고객 재산의 분리 관리, 계약 내용의 설명 의무화를 요구하고 있음.

참고: 지식산업정보원, 차세대 퀀텀닷 신소재 기술개발 동향과 양자정보통신/블록체

사례연구: 일본 vs. 미국

자금세탁 방지을 위한 규정

- 미국: 미국 뉴욕주의 BitLicense는 지급 ·수취 등 모든 거래관련 정보를 기록하고 보존하며, 의심거래의 모니터링 및 감독당국 보고를 의무화
  하고 있음.
  - ✓ CSBS 가이드라인은 디지털통화에 관해서도 은행비밀법/자금 세탁방직법(BSA/AML)을 준수하고, 계좌보유자 및 서비스 이용자를 증명하도록 요구하고 있음.
- 일본: 가상통화 계좌개설시 본인 확인과 거래 기록의 작성과 보존을 의무화하고 의심거래는 신고하도록 요구하고 있음.

.

참고: 지식산업정보원, 차세대 퀀텀닷 신소재 기술개발 동향과 양자정보통신/블록체

제언

1. 규제에 앞서 정보의 비대치성 해소 및 접근성 문제 해결
   ① 국민들이 어느 가상화폐가 진짜이고 가짜인지 구별할 수 있도록 분석/평가 보고서 및 교육을 제공하는 것이 필요
   ② 차라리 믿을 수 있는 제도권 금융권이 가상화폐 거래를 할 수 있게 하여 시스템의 안전성 및 접근성을 제고하여 사기를 방지함

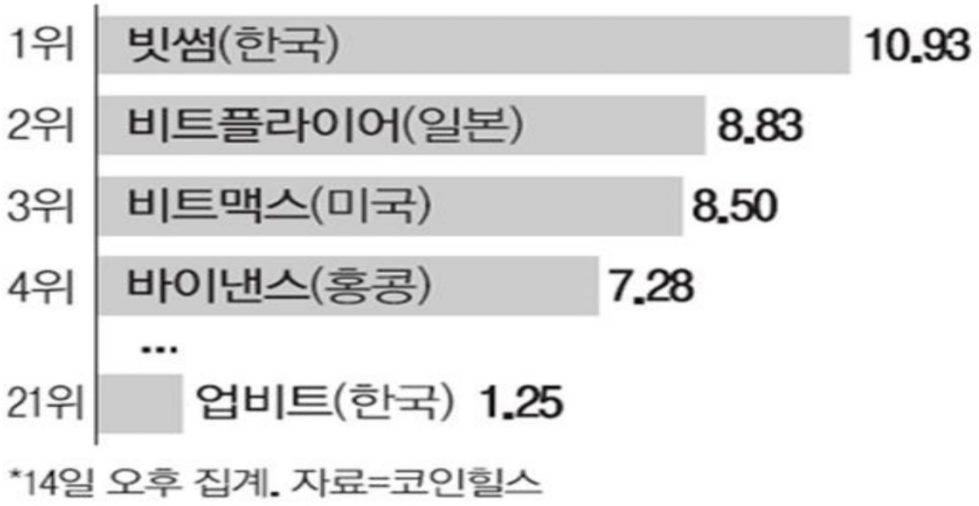
2. 유럽연합의 불간섭주의 원칙하에
   문제되는 부분은 업계 자율 규제 속에서 우선 해결하고

3. 학계 등 민관 합동으로 정교한 리서치 후에
   정부의 네거티브 규제 원칙 (이것 이것만은 안되고 나머지는 모두 합법임) 하의 규제 안을 도출함

한국의 블록체인 암호화폐 회사

- 한국은 세계적으로 블록체인 암호화폐 산업 열기가 뜨거운 국가임
  - 세계 최고 수준의 반도체 모바일폰 초고속통신망 등 관련 정보기술(IT) 하드웨어 산업발달 (IT 강국)이 중요한 배경
  - 대학교 진학률 80%의 고학력도 청년들의 창업열기
- **가상화폐공개(ICO)를 한 회사: 124개**
- **코인을 거래소에 상장한 회사: 81개**
- **ICO를 준비 중인 회사: 38개**
- **암호화폐 거래소: 56개**
- 이외에도 대략 200여 개의 많은 스타트업들이 창업을 준비 중임

세계적인 수준의 거래소



올비트: 해킹방지를 위한 블록체인 기반 거래소 세계 1위

국내 규제로 거래소 해외탈출 러시

- 네이버: 싱가포르에 거래소 "비트박스" 설립하고 암호화폐 "링크" 발행 (2018. 7)
- 카카오: 일본에 블록체인자회사 "그라운드x" 설립, 암호화폐 "클레이" 공개(2018.10)
- 빗썸: 홍콩에 거래소 빗썸덱스 설립(2018.10) 등 아시아 10개국에 진출 계획
- 업비트: 싱가포르에 거래소 설립(2018.10)
- 넥슨: 유럽 거래소 "비트스탬프" 인수(2018.10)
- 코인원: 인도네시아에 거래소

중국 암호화폐 거래소는 '법이 없는' 한국진출

구분	거래소 명	진출 국가	해외 법인명	진출 시기	비고
중화권 최대	Binance	한국		준비중	원래 홍콩에 있었으나 몰타로 이전 예정, 한국어 지원
		일본		2018.7 철수	일본 금융청 규제로 현지 철수
중국 Big 3	Huobi	한국	후오비코리아	2018.3	
		미국	HBUS	2018.6	
		일본		2018.7 철수	일본 금융청 규제로 현지 철수
	Okcoin	한국	오케이코인코리아	2018.4	NHN엔터테인먼트과 제휴
		홍콩	OKEx	2017.1	홍콩으로 이전하여 자회사 형태로 운영
	BTCC	한국	BTCC 코리아	2018.3분기 예정	
		홍콩, 런던		2018.1	2018.1 홍콩 블록체인 투자사에 피인수
그 외	Zeniex	한국	지닉스	2018.5	한·중 합작
	비트제트	한국		2018.5	한국블록체인협회 가입 타진 중
	Gate.io	한국	게이트코리아	2018.5	

한국 블록체인 암호화폐 기업들의 탈한국러시

— BOSCOIN(2017.6), ICON (1000억원, 2017. 8) Hdacs(3000억원, 2017. 12): 스위스에 재단 설립하고 ICO

— 메디블록(2017.12): 지브롤터에 재단 설립하고 ICO

— 글로스퍼: 홍콩에 재단, 조만간 글로스퍼 재팬 오픈 예정

— 블록체인 기반의 보험플랫폼 구축을 추진하고 있는 직토(Zikto): 싱가포르에 재단 설립하고 ICO 설립하고 ICO

— 카카오: 블록체인개발 자회사 '그라운드X' 일본에 설립, 연내 블록체인개발 위한 '카카오 3.0시대' 전략 발표(2018. 3. 27)

— 네이버: 자회사 '라인파이낸셜' 일본에 설립(2018. 1월). 일본정부에 암호화폐 거래 허가 신청

한국 블록체인 암호화폐 생태계 붕괴 우려

- 벤처기업자금조달 어려움 증대로 창업생태계 붕괴 우려
- 법률자문 회계자문 컨설팅 등 관련 사업서비업 발전 저해
- 관련 인력양성 지체

국부유출

- 높은 해외 재단 유지비용으로 인해 1~200억원 규모의 ICO로는 한국에 가져와서 사업할 자금 마련이 쉽지 않은 실정 (현재 약 100여 개 기업 해외ICO 추정)

— 법인세: 쥬크 14.6%. 싱가포르 15%

— 인건비: 스위스; 스위스인 고액연봉의 대표와 임원 3명 등 한국인과 현지인 5:5 채용의무

— 급등하고 있는 사무실임대료 등

— 송금도 현지 법인의 판단에 따라 가부 결정하는 등 ICO 조성된 자금을 가져오는데도 어려움

기술유출

- 명목상으로는 현지 법인(비영리)이 ICO의 주체
  - 코인발행 비지니스모델과 기술내역 관장해 과도하게 세밀한 기술내역까지 제출할 것으로 요구하는 사례

4차 산업혁명 지연

- 블록체인과 암호화폐 산업의 미발달은 블록체인을 기반으로 하는 각종 4차 산업혁명을 지연시켜 한국이 4차 산업혁명에서 낙오되게 할 수도 있을 우려
- 산업혁명에서 뒤진 국가가 그 후 후진국의 신세를 면치 못했듯이 4차 산업혁명의 낙오는 한국을 다시 도래하는 새로운 문명의 시대에 후진국으로 주저앉게 할 우려

대응방안: 특구육성

특구지정 필요성

- 한국은 규제가 많은 국가로 한꺼번에 모든 규제를 개혁하는데 한계

○ 규제친화적 top-down 국가시스템을 비즈니스친화적(business friendly)인 bottom-up 국가시스템으로 개조하는 데는 엄청난 노력과 시간이 소요

.

— 한 국가사회의 문화를 바꾸는 문제이므로 쉽지 않을 수도 있음

○ 각종 기득권 그룹 세력들의 막강한 반규제 파워

- 복지국가 지향에 따른 높은 재정수요를 감안할 때 동아시아 외국의 블록체인기업들이 한국으로 들어올 정도로 법인세를 낮추는데도 한계

규제프리 특구 혜택

□ 결국 한국의 제반 여건을 고려할 때 현 단계에서는 크립토산업에 대해서는 사전허가 사후규제(문제가 발생시 사후에 규제하는 샌드박스식 규제) 하는 규제프리 특구 조성 필요

○ 특구 내에서는 획기적인 규제개혁으로 Bottom-up 기업투자 환경 조성

○ 특구 내에서는 동아시아지역 기업들도 들어올 정도로 매력적인 수준의 법인세 인하

— 법인세 쥬크 14.6%(외국법인 9~10%, 2020년 12%로 인하), 싱가포르 15%인 점을 고려해 15% 수준까지 인하

○ Crypto labs, 인큐베이터 등 창업공간을 제공하는 민간기업에 대한 세제, 금융 혜택 등 유인제도 도입

크립토특구 조성 효과

□ 한국 블록체인 암호화폐 산업 발달로 디지털금융생태계 조성

○ 한국은 디지털금융에 필요한 하드웨어, 즉 △5G 초고속통신망, △ 모바일, △ 반도체가 세계 1위
○ 청년들의 창업열기도 높은 편임
○ 소프트웨어 발달에 필요한 규제만 혁파되면 디지털금융시대 세계의 금융중심이 될 수 있음
— 쥬크와 싱가포르는 글로벌 디지털금융허브를 두고 쟁패하는 모습

□ 블록체인 암호화폐 산업 발달은 4차 산업혁명의 기반이 되어 4차 산업혁명 시대 한국이 선진국으로 도약할 수 있는 토대가 될 것임

□ ICO통한 자금조달 활성화로 창업생태계 활성화

규제프리 특구 효과

□ 국부유출도 방지

○ 법인세 한국납부
○ 인건비 사무실 운영비 등 한국지출

□ 기술유출도 방지

○한국에 ICO 법인 설립 운영

□ 관련 연관산업 발달로 디지털금융 허브 조성, 아시아디지털금융중심지로 발전

○ 각종 미트업 컨퍼런스 등 MICE산업 발달

○ 법률 회계 컨설팅 등 사업서비업 발달

○ 관련 우수인력 양성 위한 대학 활성화 등 교육산업 발달

— 대학에 관련 학과 증설, 경영대학원, 기술경영대학원 등 확충 활성화

□ 자연스럽게 금융 MICE 사업서비스 교육의 허브로 발전하며 고부가가치 고임금의 양질 일자리 창출

□ 기존의 관광문화휴양도시+ 블록체인 암호화폐산업 (동아시아지역 블록체인 암호화폐기업, 암호화폐 재단 200개 이상)+금융+법률+회계+세무+교육+MICE산업+숙박 음식업 등 관련산업이 집적된 종합 크립토밸리나 비치, 마운틴, 아일랜드로 발전

특구 고용창출효과

□ 고용창출: 약 3.5만 명 정도 양질의 일자리 창출 전망

○ 블록체인 암호화폐기업, 암호화폐 재단: 200개*100명=20,000명

○ 금융: 암호화폐거래, 암호화폐펀드, 암호화폐은행, 크라우드펀딩, 투자, 디지털보험 등: 50개*100명=5000명

○ 법률 회계 세무 컨설팅: 50개*30명=1500명

○ 교육: 대학 인큐베이터 데이터분석 등 500명

○ MICE산업: 20개*50명=1000명

○ 숙박 음식업: 100개*20명 =2000명

○교통 관광 등 관련 파생산업: 5000명

외국의 혁신 사례

외국의 혁신 사례

- 스위스 쥬크: **"암호화폐 수도(capital of crypto nation) "** 를 목표로 조세 혜택 (법인세 14.6%, -> 2020: 12%), 친기업 환경, 법제도 등 각종 **인프라 개선에 필요한 환경 조성 등에 정책 역량 집중**
  - **300여 개 블록체인 암호화폐 회사 운집해 세계적인 "크립토밸리"로 발전**

Zug 개관

- Heart of Europe - in the middle of Switzerland
- 124,000 명 인구 - 131 개 국적
- 109,000 일자리 (인근 통근자 38,400)
- 32,000 기업
- 최근 급속한 경제발전

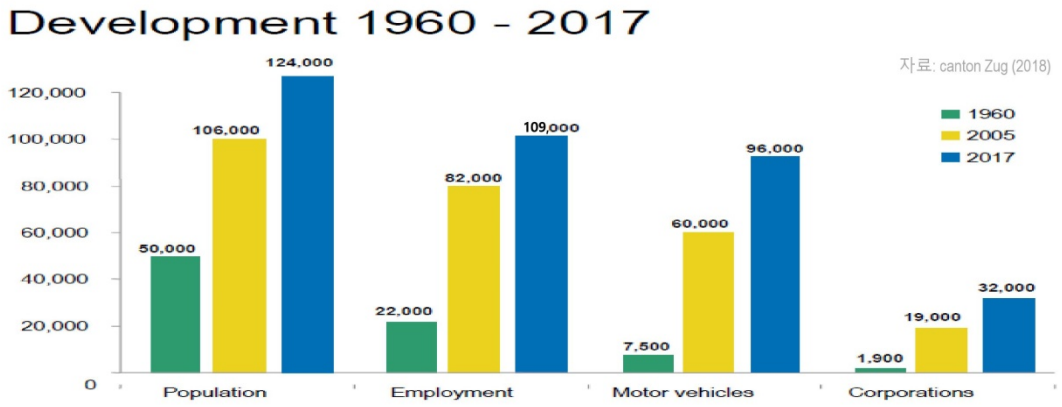
자료: canton Zug (2018)

Zug 개관

◆ Zug : 스위스 26개 캔톤(주) 중 면적 최소

- 2017년 인구 12만4천명, 일자리 10만9천개 , 기업 3만2천개
  * 최근 7년 인구증가율 9.6%
- 2005년 이후
  인구 1만 8천명 증가 < 일자리 2만 7천개 증가 & 기업 1만 3천개 증가

- 경제활동참가율 81.6% (스위스 81.3%) 실업률 2.4% (스위스 3.2%)
- 경제성장률 2.8% (스위스 1.2%, 2015)



Zug 개관

Crypto Valley today

Fintech 허브 랭킹 2018

Rank	YOY	City / Country	Scores
1	-	Singapore	
2	-	Zurich / Switzerland	
3	-	Geneva / Switzerland	
4	+4	London / UK	
5	+2	Amsterdam / Netherlands	
6	-2	Toronto / Canada	
7	+3	Stockholm / Sweden	
8	-3	New York City / US	
9	-3	San Francisco / US	
10	-1	Hong Kong (China)	
11	+2	Frankfurt / Germany	
12	+2	Berlin / Germany	

정치/법 경제 사회 기술

자료: canton Zug (2018)

- **250-300 companies with main focus on Blockchain**
- Crypto Valley Association (**891 members** by Biz Activity)

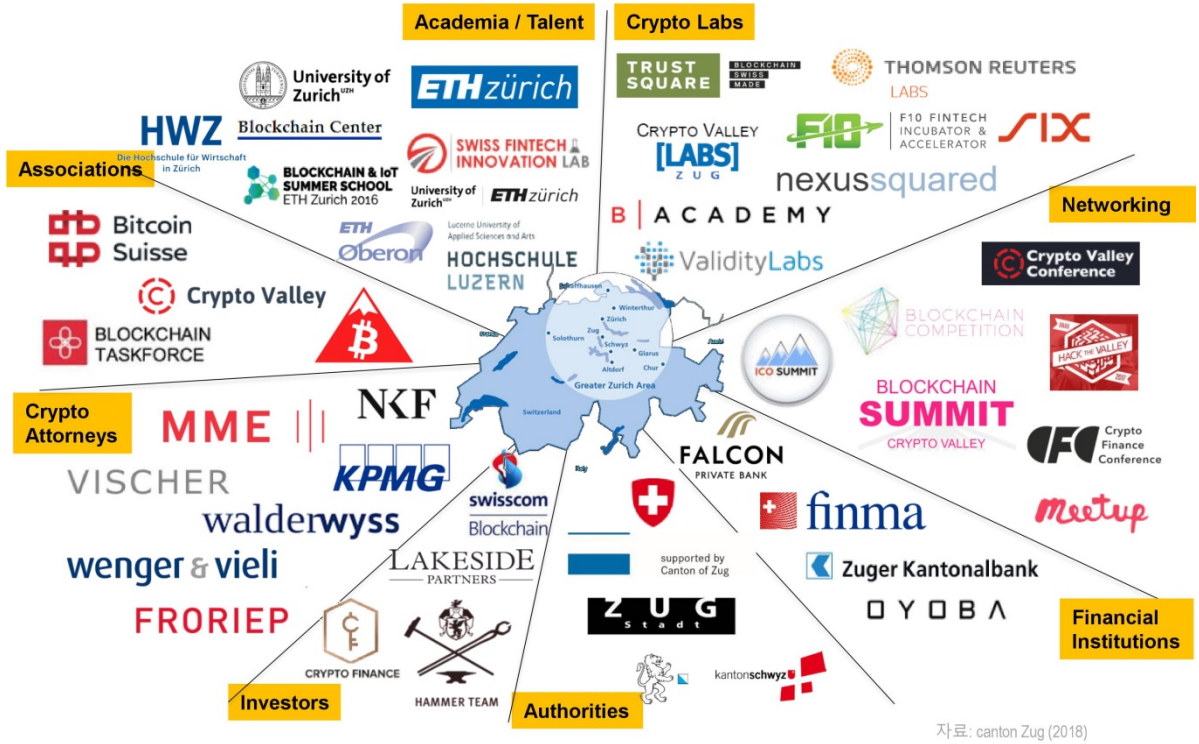
Start-up: 225	Incubator: 32
Investor / Venture Capital: 129	Multi-National Corporation: 31
Technology Consultancy: 73	Crypto Trading / Brokerage: 27
Education / Training: 44	Tax Services: 23
Legal Services: 43	Location Services: 21
Marketing / Communications: 34	Media / Journalism: 17
Association: 33	NGO: 17
Corporate: 14	
Human Resources: 11	
Cyber Security: 9	
Technology Consultant: 8	
ICO Advisory: 2	
Undefined: 98	

Crypto Valley
LAKESIDE PARTNERS
CRYPTO VALLEY [LABS] ZUG

www.cryptovalley.swiss

Zug 개관

Crypto Valley 생태계: 주요 players & 플랫폼



자료: canton Zug (2018)

Zug 개관

Crypto Valley의 Blockchain/Crypto 기업

(www.cryptovalley.directory)

자료: canton Zug (2018)

주요 글로벌기업 – mainly HQs

자료: canton Zug (2018)

세계 디지털금융중심지 한국의 꿈

세계 1위 하드웨어: 초고속통신망, 모바일, 반도체

갖추어야 할 소프트웨어:

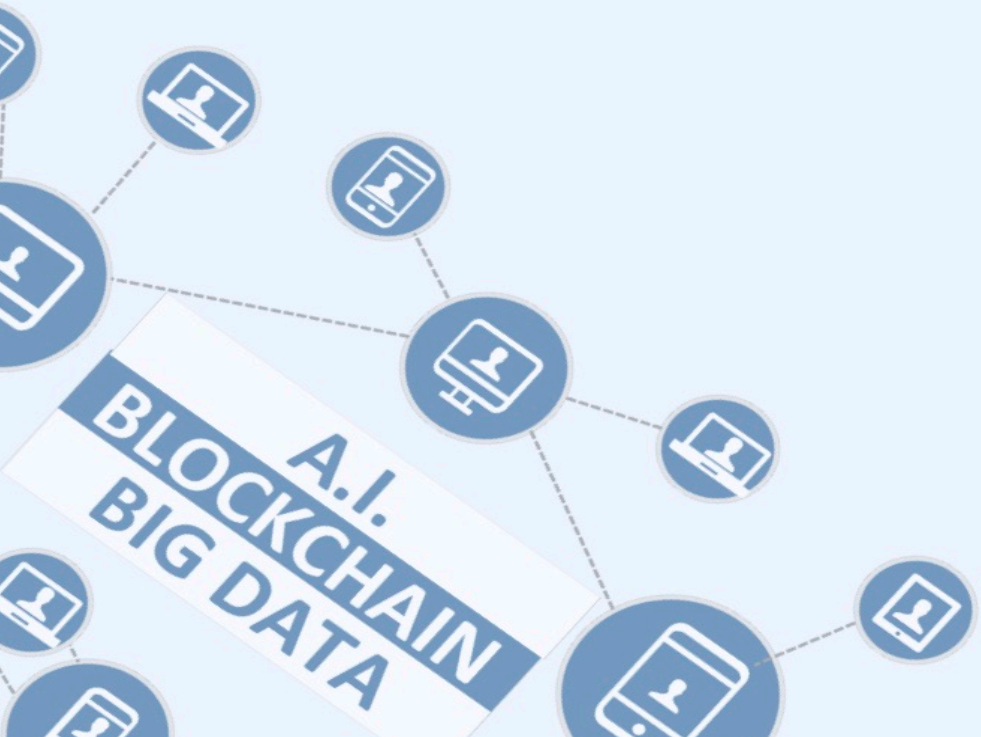
규제혁파 (사전허가 사후규제)
창의인재 양성
모험금융산업 육성

10강

Blockchain and Financial Policy

김 기 흥 교수

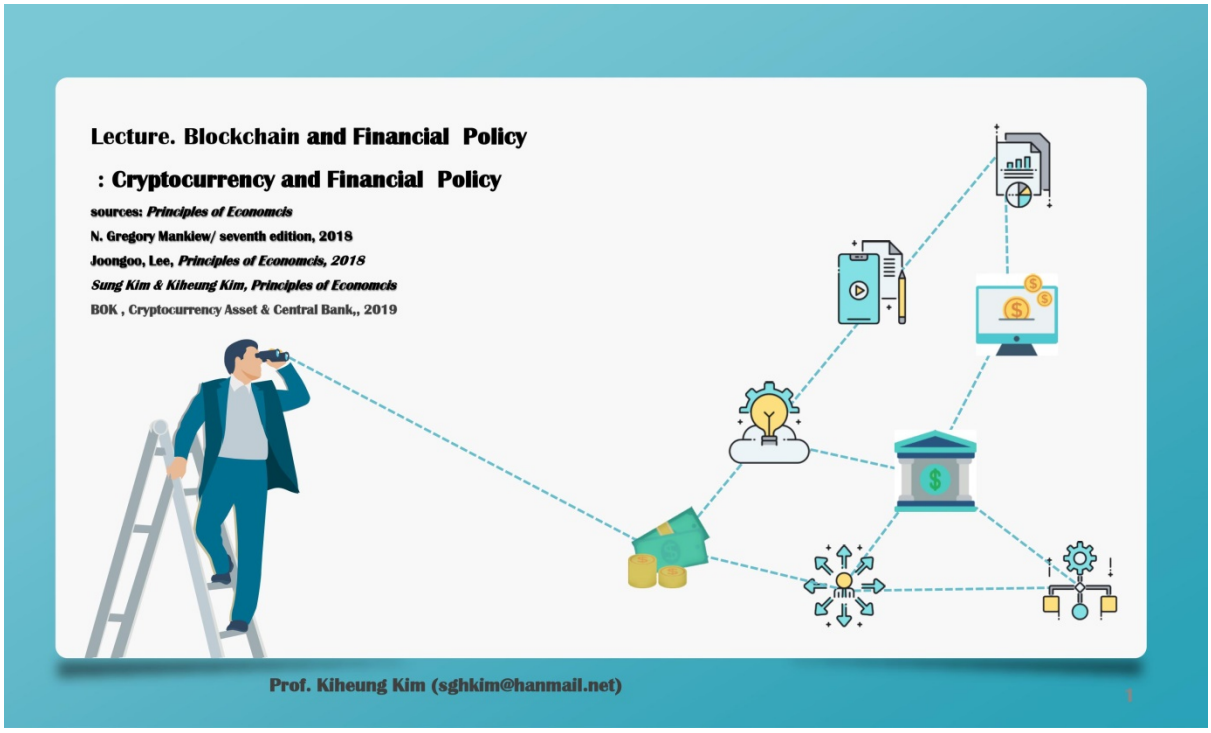
(경기대학교)



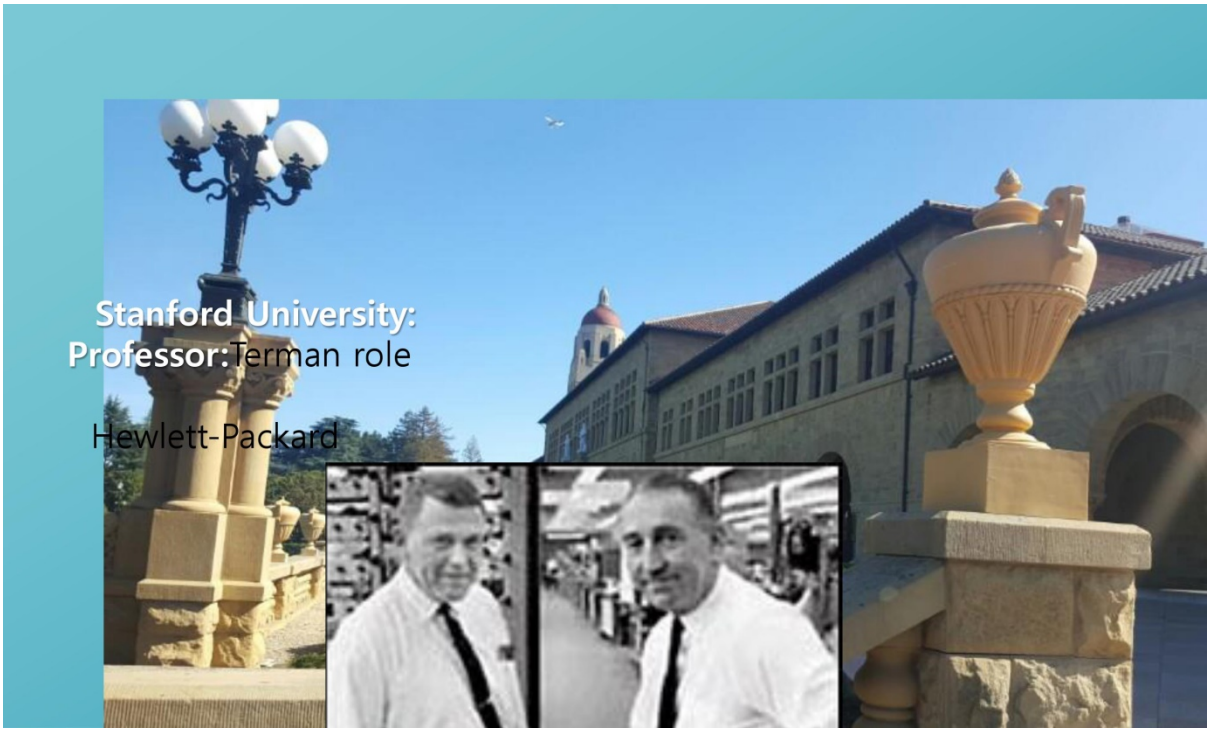
강의 동영상 URL

1 부: https://youtu.be/uDR7NjU-6Kk

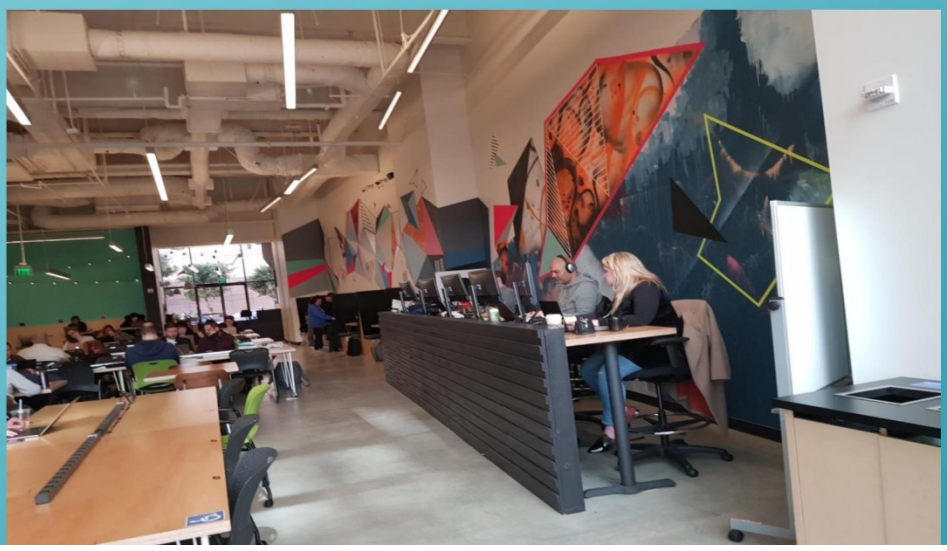
2 부: https://youtu.be/y-_4AN_MCoE


Lecture. Blockchain and Financial Policy
: Cryptocurrency and Financial Policy
sources: Principles of Economcis
N. Gregory Mankiew/ seventh edition, 2018
Joongoo, Lee, Principles of Economcis, 2018
Sung Kim & Kiheung Kim, Principles of Economcis
BOK , Cryptocurrency Asset & Central Bank,, 2019
Prof. Kiheung Kim (sghkim@hanmail.net)
1

Sillcon Valley

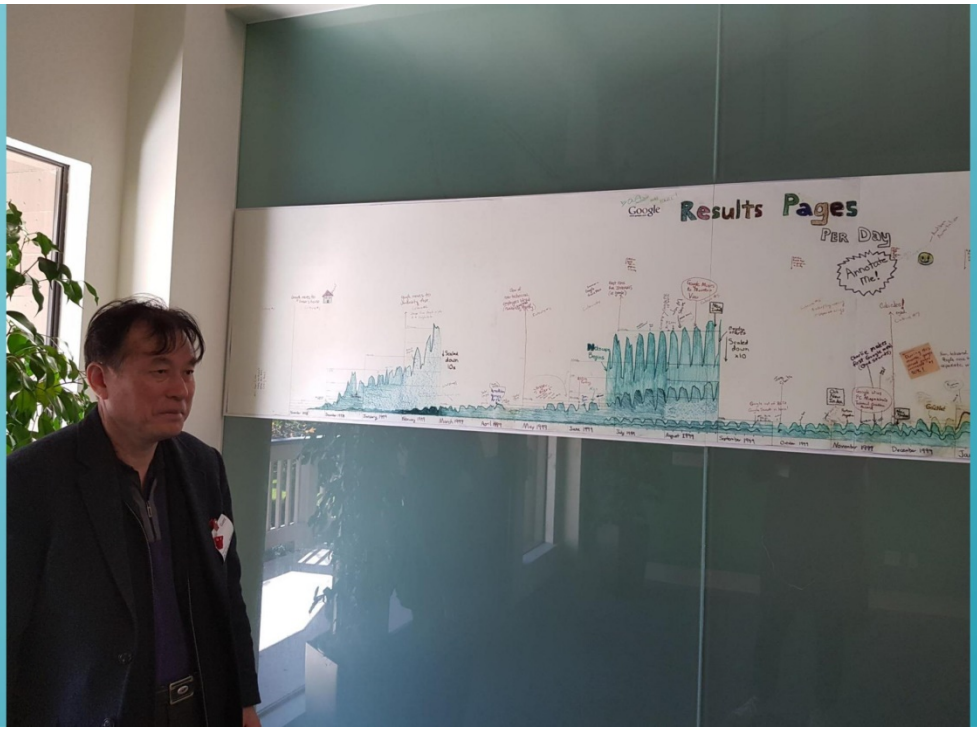


Stanford Statup 2018/2/14



Google co-founder:
Larry Page.
Sergey Brin

5


Google
Results Pages
PER DAY

6

7

Lecture

1. Monetary System, Banks, Bitcoin and Financial Policy
-What are the functions of money? The types of money?
-What role do banks play in the monetary system?
-How do banks "create money"?
-How does the BOK Reserve control the money supply?

2. Blockchain and Financial Policy
Cryptocurrency and Financial Policy

3. Blockchain and Central Bank Digital Currency (CBDC)

8

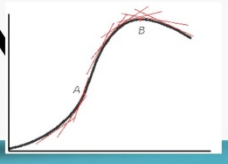
In this lecture, look for the answers to these questions

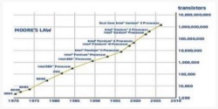
- **What assets are considered "money"?**
- **What are the functions of money? The types of money?**
- **What is the role of Bok?**
- **What role do banks play in the monetary system? How do banks "create money"?**
- **How does the BOK Reserve control the money supply?**
- **The economic value of bitcoin**
- **Financial crisis as an alternative assets, cryptocurrency**
- **Blockchain and Central Bank Digital Currency (CBDC)**
- **Effects of CBDC on Central Bank**

9

Traditional/Digital/ Crypto-Economy

- **Traditional Economy : Supply and Demand law of Goods and Services, Diminishing returns to scale, The law of scarcity**
- **Digital Economy: Digital transaction of on-line and internet: (무한 복제)- Moore's Law/ Gider's law/ Metcalfe's Law**
- **Crypto Economy: Blockchain, Distributed network, Rule of Concensus Validation, PoW, Pos, BFT, Trust; (제한 복제)**
- **(원본+분산네트워크+신뢰)**
- **N**



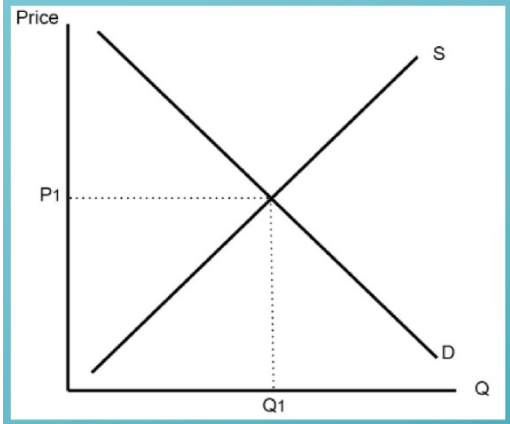


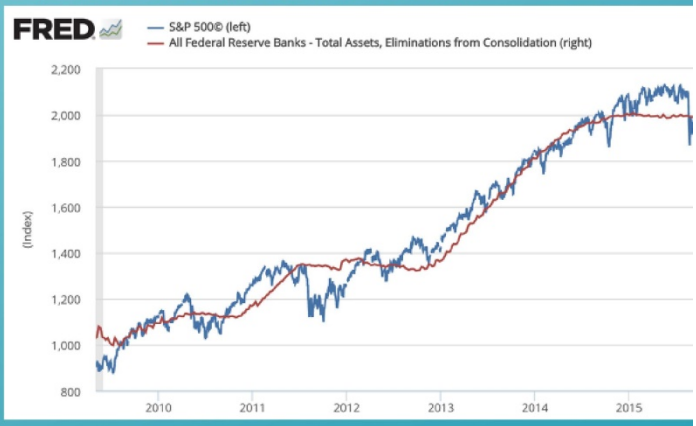
10

Supply & Demand ?

Traditional economy is not work in financial market

Why?: liquidity bubble/irrational speculative attack





11

Is Bitcoin Money? Money

Key invention

in human history: money

- here is some money for your research

12

Yap Island

The Island of Stone Money (1910)

금속물질 생산되지 않아 돌을 돈으로 사용
다듬는 수고와 공을 들인 돌은 노동의 상징

Fei – 크고 두끼운 돌바퀴 약 600km 떨어진 섬에 있는 석회 이용 채석, 가공 후 카누와 떼목으로 운송

화폐거래 시 운반하기 어려운 페이를 지불해야 할 경우 새 주인은 그 돌이 자신의 것이라 인정

매우 큰 돈을 가졌지만 페이 Fei를 가지고 있는 집안에 있지 않은 집의 페이에 검은 십자 표시

은행에 돈을 넣어놓고 거래에 이용함 a 화폐의 근간은 신뢰!

The Function of Money

- **The functions of money**
- **Medium of exchange**
  - **Item that buyers give to sellers when they want to purchase goods and services**
- **Unit of account**
  - **Yardstick people use to post prices and record debts**
- **Store of value**
  - **Item that people can use to transfer purchasing power**
  - **From the present to the future**
- **Liquidity**
  - **Ease with which an asset can be converted into the economy's medium of exchange**

Is Bitcoin Money?

- We will NOT claim it has all the characteristics of money.
  - it definitely has some!
  - they are traded against traditional currencies at a number of exchanges.
  - bitcoins are "legal" by default,
  - there were some attempts to regulate them and even ban them by governments.

15

Two Main Functions of Money

1. **Store Value**
2. **Allow Payment**
3. **Unit of Account**

- **both money and payments becomes more "virtual" with time…**

16

Evolution of - 1. Store Value

- Precious natural resources: salt etc => evolution/selection=>
- Gold, Silver, Other Metals => Coins
- Paper Money
- Money as Electronic Record +Legal Protection + Government Guarantee
- 21st century: Cryptographic E-Cash

17

Evolution of - 2. Payments

- Physical Cash (Bank Notes, Coins) = M0
- Cheques
- Electronic Bank Transfer 20 days => 15 min…
- E-Purse Systems: geldkarte, London Oyster
- Bank Cards
- Contact-less Bank Cards, e.g. MasterCard PayPass:
- 21st century: Cryptographic
- E-Cash.

•difference?

18

Crypto Currencies

Bitcoin in Germany

Bitcoin is "private money" in Germany.

Sweden:
Bitcoin = method of payment.

Finland:detailed rules, closer to a commodity

Canada

Very good environment, ATMs, start-ups

Japan

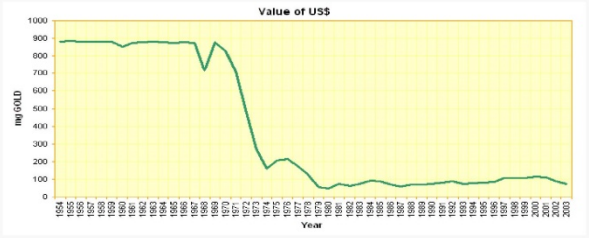
Bitcoin is used in the Market

The Kinds of Money

- **Commodity money (상품화폐)**
  - **Money that takes the form of a commodity with intrinsic value**
    - **Gold, cigarettes**
- **Intrinsic value (내재가치)**
  - **Item would have value even if it were not used as money**
- **Gold standard - Gold as money**
    - **Or paper money that is convertible into gold on demand**

Gold = "Global Single Currency"??

- Most countries abandoned the gold standard during the Great Depression,
- – one of the earliest was the Bank of England [1931].
- Much later, in 1971: the United States abandons it.Nixon Shock



21

The Kinds of Money

- **Fiat money (법정화폐)**
  - **Money without intrinsic value**
  - **Used as money because of government decree**
  - **"This note is legal tender for all debts, public and private"**
- **Fiat**
  - **Order or decree**

22

"Fiat Money"

•Def: Government-issued money not convertible for anything particular (E.g; gold, goods etc).
•Its value is controlled by the monetary policy and managed by the central bank.
•(the quantity of money in circulation can be increased or **decreased** at any moment)

• **Value of Money ?** 화폐의 가치는 어떻게 결정되는가?
•**(1) Commodity Money** 상품화폐 – 고전학파, 한계효용학파, 신고전학파
•**(2) Fiat Money** 법정화폐 – government decree /정부 공신력 혹은 공권력으로 가치 생산

•**Truth – Intrinc value** 화폐에 대한 '신뢰'가 본질적 가치 즉 내재가치 결정
• **Truth** 는 시장수용성**(market acceptibility)**을 높이고 화폐의 편재성**(遍在性, ubiquity)**을 넓힌다.
• **Truth** 의 크기는 화폐수요의 크기로 나타난다**(**달러, 금**).**
• 교환의 매개수단으로서 화폐의 거래적 수요가 본질적 수요.
가치저장기능을 하는 자산으로서 화폐는 파생적 수요임.

23

The functions of money and Cryptocurrency

- Difference of Money and Cryptocurrency :

- **• Commodity money:** 상품화폐는 화폐에 내재하는 '상품성**(goodness)**'이 가치를 결정
- **• Fiat Money : legal tender of government** 법정화폐는 정부의 신용이 가치를 결정
- **• Cryptocurrency:** 암호화폐는 내재하는 기술
- **(POW, POS** 작업증명을 통하여 **Truth** 를 증명**)**이 가치를 보증

	Dollar, Yen, Won (달러화, 엔화, 원화)	**Bitcoin** (비트코인)
Characteristics	**fiat money**	cryptocurrency
Method of transfer value	**(**물리적으로 주고받음**)** Physical transfer	**(**네트워크상 주고받음**)** **Network** transfer
Unit of money	**$, Yen, won**	**BTC**
governance	Central bank	no
Legal	yes	no
Not Double counting	특수한 종이, 인쇄 기술 증	**Blockchain technology** **Pow/ Pos (**암호 기술**),**

Why would one use Bitcoin ?

- **Reasons For and Against Wider Use of Bitcoin .....**
- **Why Would One Want to Use Bitcoins? – For/Good**
- **- Lower Transaction Costs for Electronic Economic Exchanges.**
- **- Increased Privacy**
- **- No Erosion of Purchasing Power by Inflation**
-
- **What Factors Might Deter Widespread Bitcoin Use? Against/ Bad.....**
- **-Not Legal Tender**
- **-Does Not Enjoy the Dollar's Network Externalities**
- **-Price Volatility Discourages Its Use as Medium of Exchange**
- **-The System's Long-Term Deflationary Bias Will Discourage Its Use as Currency**
- **-Bitcoins Networks Security Is Uncertain**

Crypto Currencies

More Krugman! Roubini VS Buterin For vs Against Argue of Cryptocurrency (2019.4.5 Deconomy)

- Bitcoin is …
  - "the anti-social network"
  - "bitcoin is evil" (he later claimed it was a joke
- Paul Krugman, Nobel price in economics

- Roubini
  - 북한 보더 심한 중앙 집권적 독재자
  - 누구나 쉽게 만들수 잇음, 보안성 , 펌핑 변동성 코인 결제 시스템 부족 익명성 –마약거래
- Buterin
  - -기존금융 거래 시스템 문제,
  - 확장성 프라이버스 보안 문제 해결 노력

The Evolution of Money

The Evolution of Money

- **Money (general acceptability:)**
- **1)Medium of exchange 2) Unit of account 3) Store of value -**

- **general acceptability- intrinsic value** (내재적 가치), **convenience** (편의성), **(public confidence** 공신력)이 있어야 하고 **(purchasing power** 구매력)

- **The Evolution of Money** 화폐의 진화과정: 상품화폐→금속화폐→금환화폐 → 지폐 → 예금화폐 →전자화폐 →가상화폐(?)

- 역사적으로 볼 때 화폐는 내재적 가치는 떨어지고 편의성과 공신력이 제고되어 일반적 수용성이 증진되는 방향으로 진화되어 왔음.

[History of Money][Technology]

자연화폐	
상품화폐	← 농업기술, 축산 기술
금속화폐	← 금속 정련 기술, 금속 가공 기술
주조화폐	← 주조 기술, 인쇄 기술
태환지폐	← 제지 기술, 인쇄 기술
불환지폐	
전자화폐	← IC카드기술, 암호기술 비접촉 통신 기술
디지털화폐	← 블록체인(분산형 장부 기술)

The History of Money

- 상품화폐(쌀, 직물, 조개): 내재적 가치보유, 편의성 없음,
- 금속화폐(금, 은, 동): 내재적 가치보유, 부분적 편의성, 희소성에 근거한 공신력 유지, 제한적 공급
- 금환화폐(금으로 보증한 증서): 내재적 가치, 편의성제고, 제한적 공급
- 지폐(정부가 보증한 법화): 내재적 가치 없음, 편의성, 정부 공신력에 근거한 일반적 수용성제고, 신축적 공급
- 예금화폐(은행예금으로 보증한 화폐): 내재적 가치없음, 편의성,
- 전자화폐(ic칩에 선불예금 저장된 화폐): 내재적 가치없음, 편의성 제고

- *세뇨리지 = 화폐 명목가격 - 화폐 발행에 드는 비용*

Background of Virtual Curren

r

1990 년대

2000 년대 중반

2008년 Ocupy Wall Street 운동/

나카모토 사토시

금융기관들이 송금을 위한 전자적 생태계 구축
- 넷뱅킹을 비롯한 여러 시도들 존재
- 기술적인 한계로 많은 문제점을 노출
- Intuit (1983), ProPay (1997), Paypal (1

비자, 마스터를 비롯한 신용카드 회사들을 필두
- SWIFT Institute 같은 결제기관에서 온라인
- 기술적 한계를 극복, 전자결제 시스템 부상
- Skrill (2001), Alipay (2004), WePay (200
기술력 안정화, 비즈니스 모델 확립
- 경쟁사들의 진입: Stripe (2010), Google

2008년 경제위기의 원인이 탐욕적 금융시스템이라는 믿음
- 기존 금융시스템에 대한 불신은 중앙은행을 중심으로 한 자본주의 시스템에 대한 비난으로 이어짐
- 사실 이전부터 있어왔던 비판

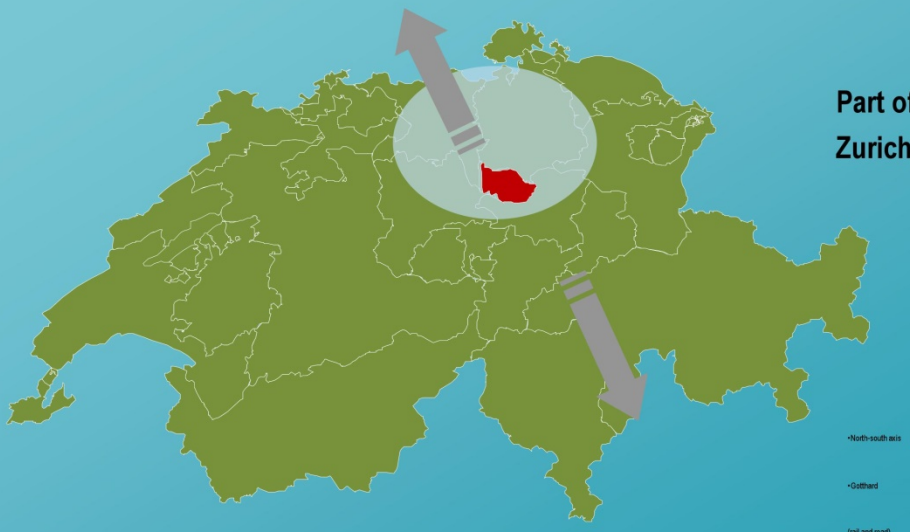
기존 화폐와 금융시스템에 대한 강한 불신
- "중앙은행이 화폐 가치를 떨어뜨리지 않을 것이라는 신뢰가 필요하나. 그런데 국가 화폐의 역사는 이런 믿음과는 다른 사례로 가득하고, 은행 또한 신뢰를 저버리고 신용버블이라는 흐름 속에서 대출했다"
- 그냥 틀린 이야기…

Crypto Currencies

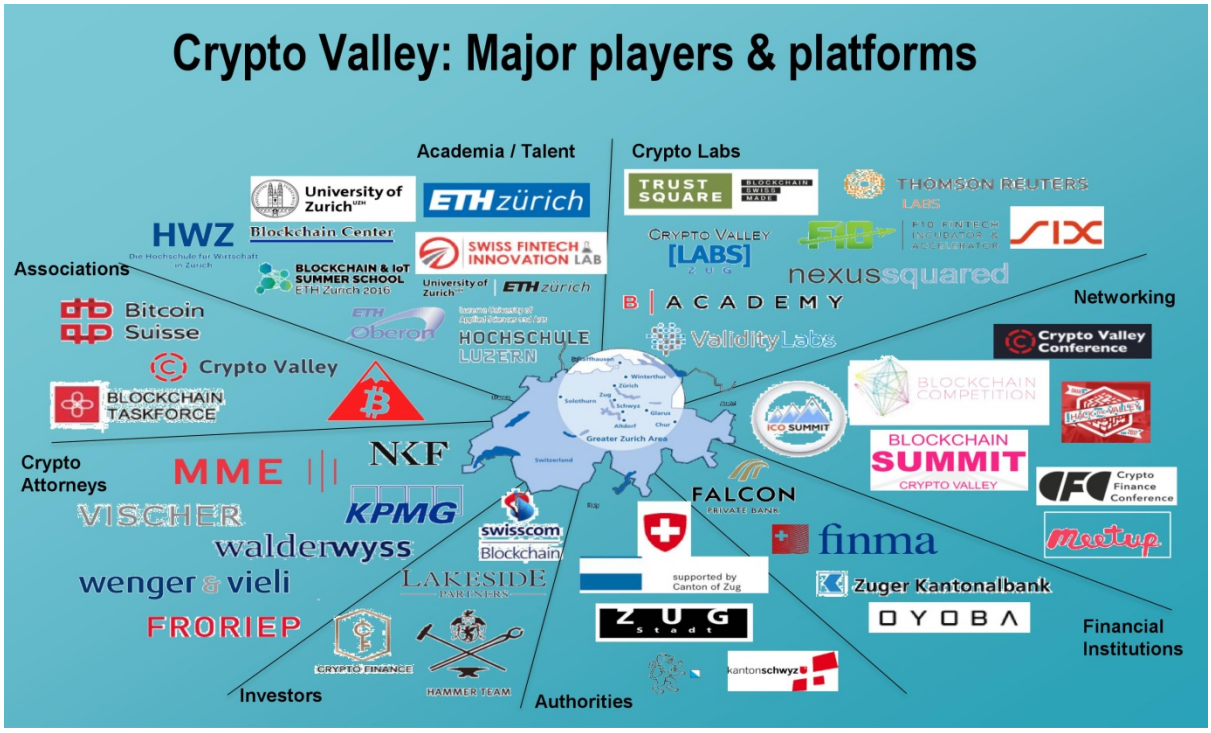
스위스
Crypto Valley

스위스 'ZUG' 전경

In the heart of Europe - in the middle of Switzerland



Access to EU Market with 700 million consumers



Crypto Currencies

Key Properties of Bitcoin

- Consensus-driven
  - consensus about the past history[blockchain]
  - consensus about the future[software spec]
- Pseudonymous, NOT anonymous
- Ledger-based. Ledger is entirely public.
- Notion of account:
  - has a balance in BTC.
- Wallet:
  - computer file which stores "the money".

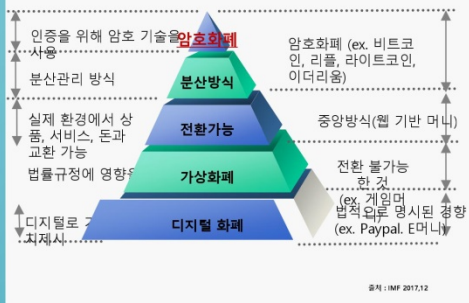
Nicolas T. Courtois 2009-2014

Cryptocurrency, Virtual currency and Digital currency

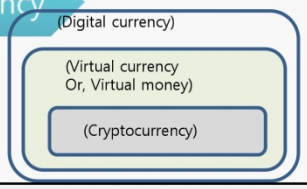
☐ **Difference of** Cryptocurrency, Virtual currency:

Cryptocurrency is truth

Smart contracting layer? (e.g., ETH)
Privacy layer? (e.g., ZEC) Remittance layer? (e.g., XLM)
Base layer for store of value? (e.g., BTC)



출처 : IMF 2017.12



구분	내용
Digital currency	o 전자적 형태로 표시된 모든 화폐 (법정 화폐발행 여부와 무관) o IC 카드 도는 네트워크에 연결된 컴퓨터에 은행예금이나 돈 등이 전자적 방법으로 자장된 것으로 현금을 대처하는 전자적 지불수단
Virtual currency	o 디지털 화폐 중 법정 화폐로 표시 되지 않은 화폐 (마일리지 등)
Cryptocurrency	o 분산화 된 가상화폐로 암호화 기술을 이용, 유효성을 인증하는 방식

37

Cryptocurrency, Virtual currency and Digital currency

☐ 금융산업의 영역들

Enabler
새로운 기술을 이용하여 기존 금융기관의 비효율성을 개선 기여

Traditional Institution
국내외의 전통 금융기관들

KB국민은행 · Standard Chartered · HSBC · IBK기업은행 · citibank · 하나은행 · 우리은행 · 신한은행 · kdb 산업은행

Disruptor
혁신 서비스를 통해 기존 금융기관 업무 대체

PayPal · venmo · TransferWise · Toss · LendingClub · OnDeck

Platform
고객과의 접점에서 다양한 기능 제공 및 통합과 중개

broccoli · policygenius · CoverHound

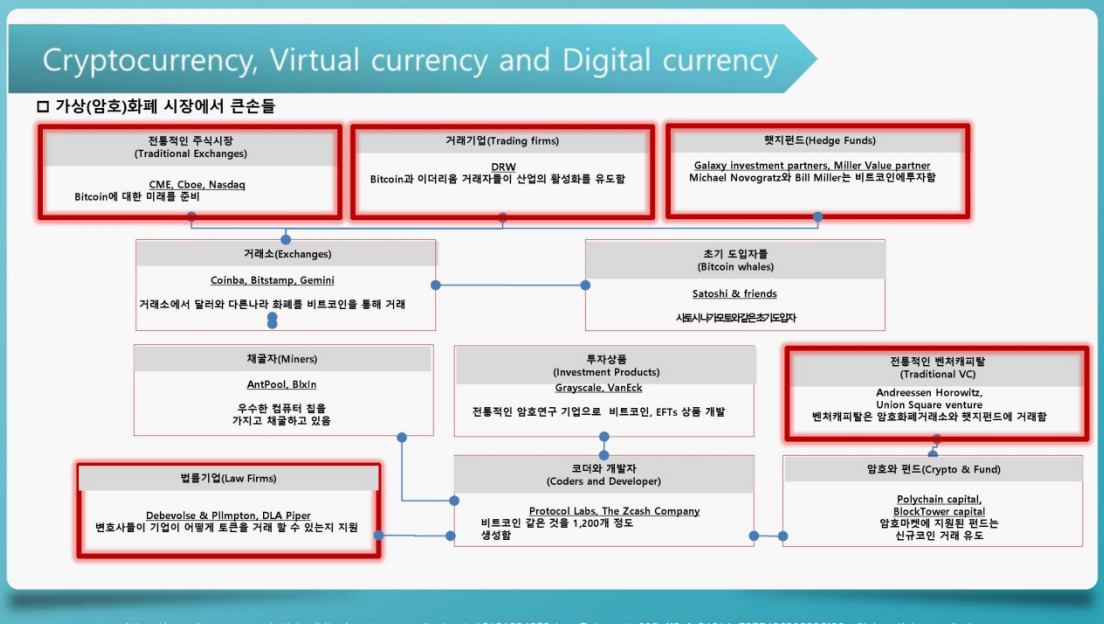
Platform changer
블록체인 기술, 가상(암호)화폐

ripple · Bitcoin BTC · Myriad MYR · Dogecoin DOGE · Dash DASH · Expanse EXP · Stellar STR

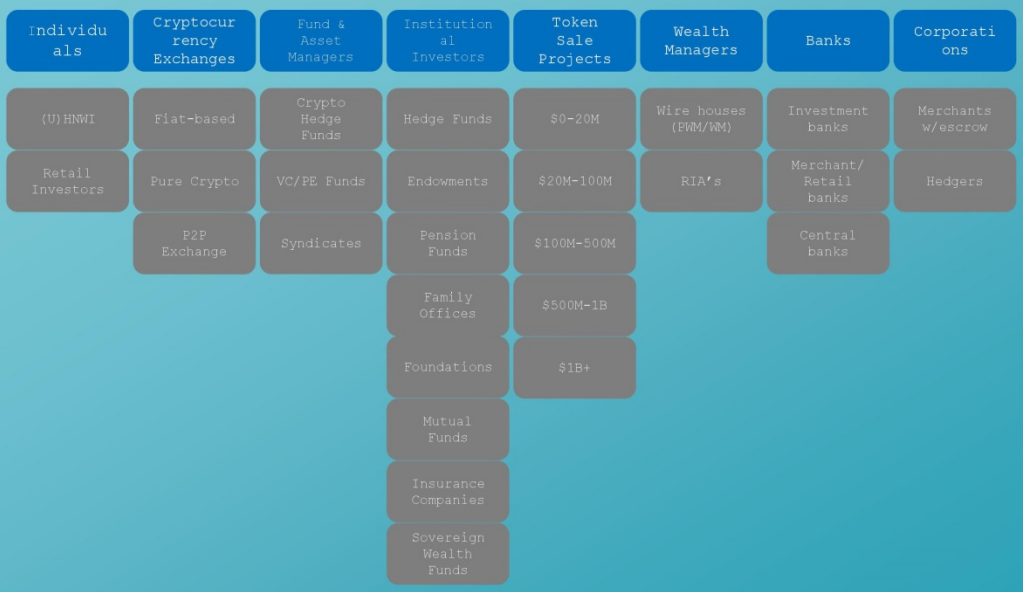
sources : https://www.barrons.com/articles/bitcoin-storms-wall-street-1512188427?shareToken=ste908cff2efa24614a7277486302236f6&reflink=article_email_share

38

출처 : Barron's, 2017,12



sources : https://www.barrons.com/articles/bitcoin-storms-wall-street-1512188427?shareToken=ste908cff2efa24614a72774863022366f6&reflink=article_email_share



Digital Currency

전자적으로 교환되는 돈이나 증서
- 전자송금, 지로, 핸드폰 결제, 디지털 화폐, 가상화폐

현금카드나 신용카드 시스템의 온라인 구현
•기존 화폐시스템의 온라인으로의 확장
•원칙적으로 온라인 상 이루어지는 전자화폐를 이용한 모든 거래는 오프라인으로도 수행 가능

오프라인의 시스템 기반
•중앙집권적 체계의 필연성
•기존 금융시스템에 기반하고 있기 때문에 규제가 용이

Characteristics of Virtual Currency

Cashless **무현금, 무수표 사회 지향**

- 신용카드, 전자결제

Transaction cost **다양한 비용감소**

- 구두창비용
- 거스름돈 수수비용
- 수수료 인하, 거래비용 저렴
- 결제시간

Decentralization **탈 집권적체계**

- 기존 화폐시스템 틀 안에 서는 환 위험 노출
- 세계적으로 통용 될 수 있는 전자화폐 수요 대두

Risk **잠재적 위험**

- 전자보안
- 화폐승수 확대와 화폐수요 불안정으로 인한 financial화폐정책의 유효성 감소
- **Seigniorage decrease** (시뇨리지 감소)

Characteristics of Virtual Currency

1

Decentralized (통제 가능한 중앙기관이 없다).

- 화폐의 발행과 유통을 담당하는 중앙기관 부재
- 법적 규제가 거의 없음
- 최초 화폐 발행 주체의 규칙에 발행 량과 가치가 결정
- 화폐공급의 제한성(비트코인 2030년 공급중단)

2

Oligopoly (다양한 종류, 과점적 시장)

- 현재 2200여종 이상이 거래소에서 등록 및 거래 중 P2P의 분권화된 거래장부형식

민간이 주도한 자유경쟁에 의한 화폐발행과 유통
- 속성상 글로벌 화폐의 성격

3

Risk of Security(보안에 대한 다양한 리스크 존재)

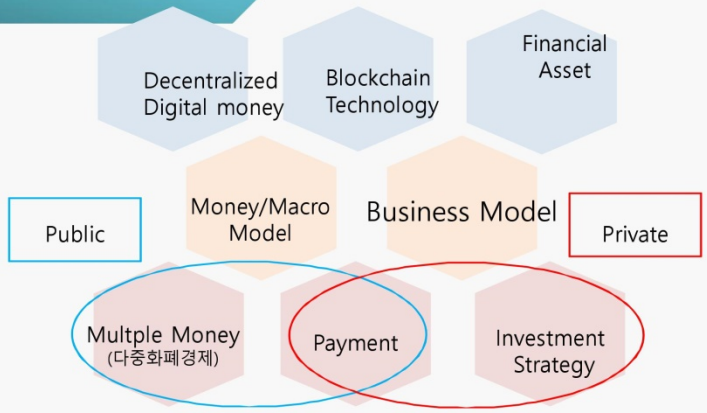
- 규모는 지속적으로 확장되나 거래소 해킹사고, 불법적 거래 부작용 또한 심각
- 가상화폐 관련 법규제의 사각지대 악용 사례

Crypto Currencies

Is Bitcoin Money?

A Currency?

Bitcoins :



Legal Definition of Virtual Currency

➢ **Virtual Currency is Currency ? commodity ? Securities ?**

- 내재적 가치가 없다는 점에서 상품은 아님
  (비트코인과 같은 가상화폐를 획득하기 위해 획득비용이 없지 않지만 일반상품 또는 상품화폐처럼 사용가치가 있지는 않음**)**
- 주식이나 채권과 같은 수익을 내는 유가증권으로 보기에도 어려움
- 교환의 매개수단으로 거래가 가능하다는 점에서 화폐의 성격
- 투자의 대상이 된다는 점에서 가치저장의 기능을 하는 화폐
- 지불의 수단이 됨으로 화폐로서의 기능

▪ **Virtual Currency is not Currency ?**

▪ 가상화폐를 화폐로 보지 않는 자의 주장

- 내재적 가치가 없다
- 법화와 같이 정부가 보증하는 공신력이 없다.
- 거래의 편의성만으로 화폐가 될 수가 없다.
- 아직 일반적 구매력이 있다고 할 수 없다.

Legal Definition of Virtual Currency

1. '**Commodity (상품)**' ?
- 거래세(Transaction Tax)를 부과: 거래의 익명성으로 추적상 어려움
- 비트코인'상품'으로 볼 경우, 가상화폐거래소의 법적지위는 '상품'을 중개하는 '상품중개소'

2. 'Currency (화폐)' ?
- 비트코인을 '화폐'로 볼 경우, 가상화폐거래소의 법적지위는 '환전기능을 겸한은행'으로 정의. 비트코인을 '지불수단'으로 볼 경우, 가상화폐거래소의 법적지위는 '서비스업체'로 정의

3. 'Securities (유가증권)' ?
- '유가증권'의 경우 소유권이 등록되어야 함. 비트코인을 '유가증권'으로 볼 경우, 가상화폐거래소의 법적지위는 증권거래소에 준하는 제3의'거래소'로서 통제됨

4. 'Intangible Asset (무형자산)' ?
- Capital gain tax. 자산상속의 경우, 상속세(inheritance tax)가 발생. 그러나 비트 코인의 익명성으로, 과세의 실효성 문제. 가상화폐거래소의 법적지위는 '자산'의 중개소로, 유가증권거래소규정이 준용되는 새로운 거래소형태로 규제될 가능성

Cryptocurrency vs Fiat Money (가상화폐 vs. 명목화폐)

Cryptocurrency is crowding out Fiat Money ? 서로 절충 진화 공존 가능성

Cooperation ? 가상화폐와 명목화폐는 쓰임이 다를 확률이 높음

변동환율제가 적용될 확률이 높기 때문에 실질가치가 같을 것이라 생각할 수 있으나
쓰임이 다르기 때문에 실질가치 다름

Implication: 가상화폐가 명목화폐를 구축할 필요는 없음
à Co-exist: 쓰임 (use) 에 따라,
경제주체의 선호 (preference) 에 따라 둘은 공존 가능!

Bitcoin: Money vs. Commodity

Why is Important?

Tax(과세기준의 쟁점): Transaction 비트코인을 거래목적으로 구매 하였는지?
Investment 투자 목적으로 구매하였는지?

Tax 과세기준: 개인의 환차익은 비과세, 법인의 환차익은 법인세,
투자재는 capital gain (양도소득세) 비과세, 금융자산은 금융소득세 등

US, German, Norway(미국, 독일, 노르웨이) 등은 법인세 과세: 화폐 불인정 (

Japan, U.K (일본, 영국)은 디지털 화폐로 인정하여 제도권으로 흡수

블록체인 정보를 분석하여 이용자 분류적 접근

Dilemma of Bitcoin:

1. Users: 화폐로 인정되기 위해서는 이용자가 많아야 함
2. Store Value (0) 3. Allow Payment (0) 4 unit of account (x)

Volitility: 높은 변동성은 비트코인을 매력적인 투자처로 만들어
많은 투자자들이 몰려 이용자가 증가

Store Value :동시에 높은 변동성으로 인하여 화폐의 역할 수행이 어려움

Digital Asset: 우리는 가상화폐가 새로운 금융자산이 되기를 원하는가?

만약 비트코인과 같은 가상화폐가 전 세계적으로 통용되는 화폐로 정착하면 어떤 일이 일어날까?
사회적 합의 및 수급이 내재 가치 (금 /예술품)/ 화폐보다는 자산

Crypto Currencies

Decentralized peer to peer payment system which works as currency:

=> has units of value which can be exchanged for "real money". Currently 1BTC= 400 USD.

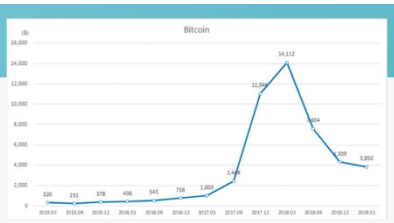
Based on cryptography and network effects.

Anarchy, not supported by any government and not issued by any bank.

"Play money", imperfect system.

화폐 발행권한의 탈중앙화
(개인의 화폐발행권한)
/발행권한남용 위변조여부
이중지불방지/분산원장

Economic Question ? Bitcoin in the Academic Economy

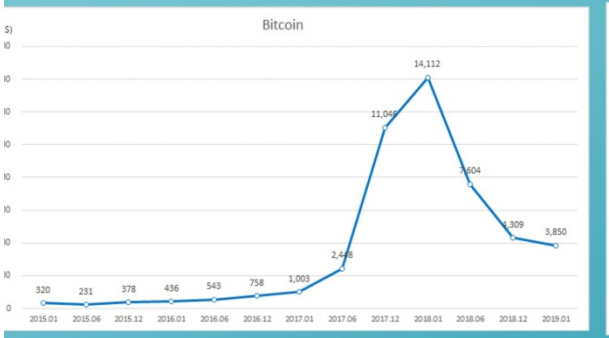


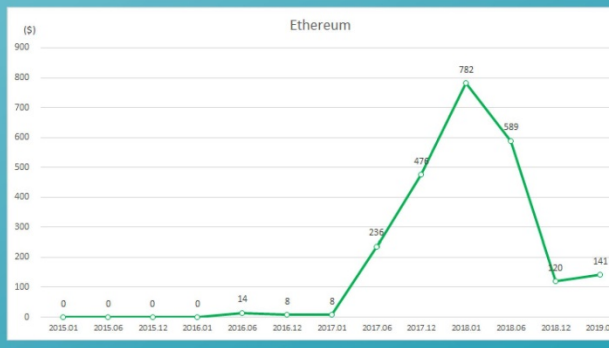
- **Are cryptocurrencies possible to replace fiat currency ?**
  - **Quantity of money circulating in the economy**
- **What is the economic benefit of decentralized system compares to the centralized system ?**
- **What is the key factor to drive the cryptocurrency price?**
- **What is the main driver on the growth of the future value of blockchain network ?**
- **The How can we obtain the equilibrium price from the equilibrium model ? How can we capture the phenomenon from the end of 2017 to the early of 2018 ?**
- **What are the economic insight about blockchain network and asset pricing ?**
- **Can we regard cryptocurrency as an alternative investment ? Yes afe assets like Gold, Yen,**
- **Price volatility predicion model : ARCH GARCH model - Time series Prediction model/ Bubble ?**
- **. GARCH Models**
- **Let Xt denote the observed financial data series; in our case, these are the log returns of the pricesof the respective cryptocurrencies. Then, GARCH models can be specified as:**
- **Xt = *mt* + *st*Zt, (1) where *mt* denotes the conditional mean and *st* denotes a volatility process. All of the GARCH-type models**

52

Price trend of Bitcoin & Ethereum

key factor OF Recent Bitcoin Price increase
1) Cryptocurrency business of and Tech company
2) Uncertanty of US –China Trade War
3) Fear of Missing Out (지금 참여 안하면 손해 심리)
4) China's VDS Coin investment





53

Cryptocurrency Market Analysis

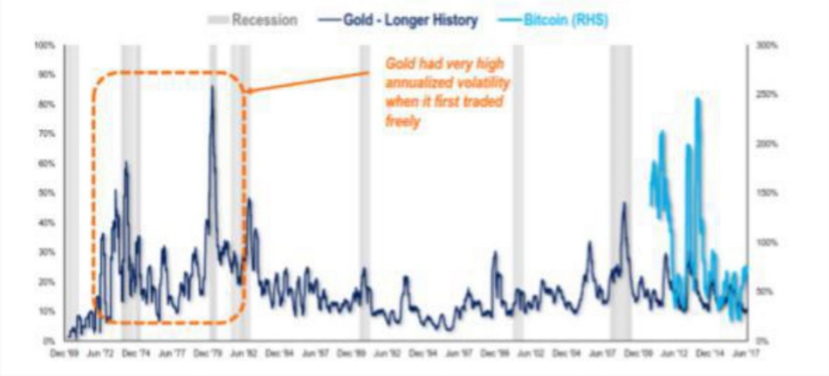
- **Modeling the time series of Bitcoin prices**
  - **Volatility analysi/GARCH Model (Dyhrberg, 2016a; Katsiampa, 2017)**
  - **Statistical properties (Barivieraet al., 2017; Chu et al., 2015)**
  - **Inefficiency of Bitcoin (Urquhart, 2016; Nadarajah& Chu, 2017)**
  - **Hedging capability (Dyhrberg, 2016b; Bouriet al., 2017)**
- **Prediction of Bitcoin prices**
  - **Linear model (Ciaianet al., 2016)**
  - **Logistic regression (I. Madan et al., 2015)**

54

Crypto Currencies

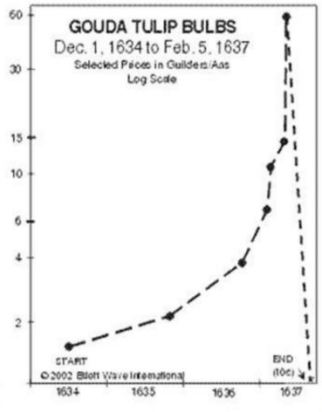
Bitcoin's Price Volatility

(2010년대 비트코인 가격 변동성 1970년대 금과 유사)



The Bubble of Tulpip /The Bubble of Bitcoin (2017-2018) ?

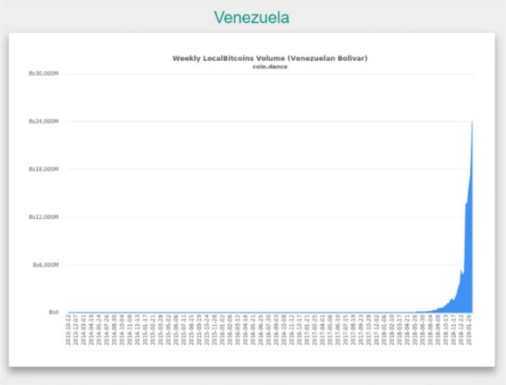
- **The Tulip of Netherland**
- **the phenomenon from the end of 2017 to the early of 2018 ?**



Crypto Currencies

Bitcoin in Venezuela
Fiat money is unstable country

Bitcoin is used



Money in the Economy

- **Money stock**
  - **Quantity of money circulating in the economy**
- **Currency**
  - **Paper bills and coins in the hands of the public**
- **Demand deposits**
  - **Balances in bank accounts; depositors can access on demand by writing a check**

Money in the Economy

- **Measures of money stock**
  - **M1**
    - **Demand deposits, Traveler's checks**
    - **Other checkable deposits, Currency**
  - **M2**
    - **Everything in M1**
    - **Savings deposits, Small time deposits**
    - **Money market mutual funds**
    - **A few minor categories**
- **Cryptocurrency vs M1, M2 ?- role is increasing**

59

Crypto Currencies

***Disruption?**

Disruptive Technology:

def:

Allows to do things which just could not be done before…

"Bitcoin Prevents Monetary Tyranny"

(화폐 발행권한의 탈중앙화)

Bitcoin Mining

Bitcoin =… the most popular peer-to-peer payment and virtual currency system as of today
belongs to no one, anarchy

화폐 발행권한의 탈중앙화
(개인의 화폐발행권한)

/발행권한남용 위변조여부
이중지불방지/분산원장

M1, M2: 우리나라의 통화지표
"Bitcoin Prevents Monetary Tyranny"?

구 분	구성내역	총량(조원)	GDP대비(%)
현금통화	민간이 보유하는 지폐 및 주화	52.7	3.7
M1 (협의의 통화)	현금통화+요구불예금+수시입출식 저축성예금	509.6	35.7
M2 (광의의 통화)	M1+정기예적금 및 부금*+시장형 상품 +실적배당형 상품*+금융채* 및 기타 (*만기 2년 이상은 제외)	1,952.0	135.3
Lf (금융기관유동성)	M2+만기 2년 이상 정기예적금 및 금융채+한국증권금융의 예수금+생명보험회사의 보험계약준비금 및 기타	2,619.0	183.4
L (광의유동성)	Lf+정부 및 기업 등이 발행한 유동성 시장금융상품(국채, 지방채, 기업어음, 회사채 등)	3,350.5	234.6

자료 : 한국은행

62

M1, M2, Lf, L :통화지표별 구성 내역 : Cryptocurrency ?

(sources: BOK)

Digital Asset: Bitcoin

Bitcoin is Digital asset/ Safe Asset: 현재 비트코인은 화폐라기 보다는 자산에 가까움
가치보존형 자산은 사회적 합의 및 수급이 내재 가치
M1 과 비트코인 자산 대체 가능한가 **?**

자산의 분류	종류	특징
자본형 자산	주식, 채권, 부동산 등	현금흐름이 있어서 가치평가 상대적으로 수월
소비재-자본형 자산	농산물, 원유 등	실생활에 쓰이는 사용가치 있음
가치보존형 자산	금, 예술품, 고급 술, 비트코인 등	얼마나 많은 사람들이 자산의 가치를 인정해주는지가 중요

US-China Trade War –driven Safe Asset UP ?
Gold-Yen-Bitcoin Price UP?

Soures: Maeil-Gyungjae, 2019.5.15

65

Digital Asset Services (디지털자산 서비스)	Digital Market (디지털 시장 마켓)	coinbase
디지털 자산 및 보관 · 투자상품 · 투자 서비스 · 자산 보관	• Digital asset custody: Fidelity, Julius Baer, Wyoming state Fidelity가 기관투자가를 위한 비트코인 거래 서비스 출시 예정 • Structured products: Julius Bare, CBOE-VanEck, Bitwise • Portfolio management: Julius Baer • Bancassurance: China Construction Bank • Tokenized securities: Banco BTG Pactual AS • Staking: Binance, Coinbase	BTGPactual MAKER TenX
신용거래 · 파이낸셜	• Portfolio leveraging: MakerDAO • Corporate finance • Structured transactions: Bitcoin ETFs, crypto-index funds, Julius Baer • Lending: ETHLend, Compound, Dharma, SALT, Celsius, Bank of China, China Construction Bank • Cards: Mocano, TenX, Change, Revolut • Trade Finance: Standard Chartered, Voltron Initiative, BNP Paribas/HSBC	TRIDENTTRUST Ledger
자산 설계 · 자산 설계 · 투자 신탁 · 금융 설계 · 유산 관리	• Trust services: Trident Trust / Ledger	IBM Blockchain MESSARI
디지털 서비스	• Research firms: Digital Assets Research, Delphi Digital, Coinmetrics, OnChainFX • Crypto-asset exchanges: Coinbase/Kraken/Binance • Payments: cryptocurrencies, World Wire • Bank-backed cryptocurrency: JPMorgan	

Crypto Currencies

Sources: WGC chainparters

Market Size of Major Assets

	Market Size
The World's Silver	$17 billion
The World's Gold	$8 trillion
Global Stock Markets	$73 trillion
Global Bond Markets	$92 trillion
Global Real Estate	$217 trillion

+ 암호화폐 (Cryptocurrency) - $123 billion

ICE, Nasdaq, Citi, Fidelity
Bank of America, Credit Suisse,
BNP Paribas, Barclays, AIA,
Deutsche Bank, Wells Fargo,
Nomura, UBS, MUFG, HSBC,
JPMorgan, BBVA, CME, Cboe,
Goldman Sachs, ING,
BNY Mellon, Santander,
Morgan Stanley, ABN-AMRO,
국민은행, 하나은행, 우리은행,
신한은행, 농협은행

Crypto Currencies

China's Power of bitcoinecosystem
(거래소 & 채굴)

CME & Cboe 합산 거래량
전체 비트코인 거래량 대비 **1%**미만
!

거래량 순위 (30 일)	국가	거래소	오픈 시기
1		BINANCE	Jul 2017
2		OKEX	Jan 2014
3		Bit-Z	Jun 2016
4		ZB.COM	Nov 2017
5		Huobi	Sep 2013

마이닝풀	BTC.com	ANTPOOL	f2pool	SLUSHPOOL
국가				
설립일	2015	2013	2013	2010
해시율	1 위 (16%)	2 위 (16%)	3 위 (10.5%)	4 위 (9.6%)
홈페이지	https://btc.com	https://antpool.com	https://www.f2pool.com	https://slushpool.com
주요 서비스	마이닝풀, 지갑, 블록체인 익스플로러	마이닝풀	마이닝풀	마이닝풀

자료: CoinMarketCap; Bitcoin.com; 체인파트너스
주석: 30days adjusted volume, 해쉬율 2019년 1월 21일 기준

Crypto Currencies

Is Bitcoin:

- A currency [like euro]?
- A commodity [like gold]?
- There is yet another very surprising application for bitcoin…

- **미국은 금 시장을 완전히 장악한 후 2004년 금 ETF 출시**
- **결국 비트코인 ETF는 시간 문제**
- **불투명한 시장, 정보 비대칭은 신종 투자자산의 특징**

Gresham's law (그레샴의 법칙)

bad money drives out good money: "악화가 양화를 구축한다"

bad money (나쁜화폐) vs. good money (좋은화폐)

일반적인 질문: 가상화폐가 명목화폐를 구축할 것인가?

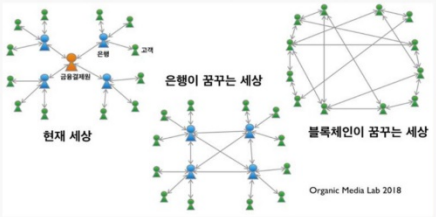
좋은화폐: 명목화폐 vs. 나쁜화폐: 가상화폐 à 가상화폐가 명목화폐를 구축

흔히 '나쁜 것이 좋은 것의 자리를 빼앗는다' 라는 말을 하고 싶을 때 자주 쓰여지는 잘못된 적용 à 가치평가의 맥락이 아님을 잘못 이해

Gresham's law (그레샴의 법칙)을 현재의 가상화폐 현상에 대입하기 위해서는 악화와 양화 에 대한 정확한 정의와 이 법칙을 이야기 하게 된 상황적 이해가 필요

The BOK's Organization

- **The BOK's jobs**
  - **Regulate banks**
  - **and ensure the health of the banking system**
    - **Regional Monetary Banks System**
    - **Monitors each bank's financial condition**
    - **Facilitates bank transactions - clearing checks**
    - **Acts as a bank's bank**
    - **The Bok – lender of last resort**



71

The BOK's Organization

- **The BOK's jobs**
  - **Control the money supply**
    - **Quantity of money available in the economy**
    - **Monetary policy**
      - **By Federal Open Market Committee (FOMC)**
- **Money supply**
  - **Quantity of money available in economy**
- **Monetary policy**
  - **Setting of the money supply**

72

Banks and the Money Supply

- **Behavior of banks**
  - **Can influence the quantity of demand deposits in the economy (and the money supply)**
- **Money**
  - **Currency + Demand deposits**
  - **BOK B/L** **Commercial Banks**
  - ---
    - **Asset** **Liabilities** **Asset** **Liabilities**
    - **Domestic Credit** **Cash** **reserves** **Deposit**
    - **Net Foreign Asset** **reserves require**

73

Fractional-Reserve Banking

- **Fractional-reserve banking**
  - **Banks hold only a fraction of deposits as reserves**
- **Reserve ratio**
  - **Fraction of deposits that banks hold as reserves**
- **Reserve requirement**
  - **Minimum amount of reserves that banks must hold; set by the Bok**

74

Fractional-Reserve Banking

CASE : Fractional reserve banking system 10%

- **Excess reserve**
  - **Banks may hold reserves above the legal minimum**
- **Example: First National Bank**
  - **Reserve ratio 10%**

First National Bank

Assets		Liabilities	
Reserves	$10.00	Deposits	$100.00
Loans	90.00		

The Money Multiplier

Second National Bank

Assets		Liabilities	
Reserves	$ 9.00	Deposits	$90.00
Loans	81.00		

Third National Bank

Assets		Liabilities	
Reserves	$ 8.10	Deposits	$81.00
Loans	72.90		

The Money Multiplier

- The money multiplier
  - Original deposit = $100.00
  - First banking l lending = $ 90.00 [= .9 × $100.00]
  - Second banking lending = $ 81.00 [= .9 × $90.00]
  - Third banking lending = $ 72.90 [= .9 × $81.00]
  - ...
  - Total money supply = $1,000.00

77

Fractional-Reserve Banking

- Banks hold only a fraction of deposits in reserve
  - Banks create money
    - Assets
    - Liabilities
  - Increase in money supply
  - Does not create wealth
  - BOK — Commercial Banks
  -
    - Asset — Liabilities — Asset — Liabilities
    - Domestic Credit — Cash — reserves — Deposit
    - Net Foreign Asset — reserves require

78

The Money Multiplier

- The money multiplier
  - Amount of money the banking system generates with each dollar of reserves
  - Reciprocal of the reserve ratio = 1/R
- The higher the reserve ratio
  - The smaller the money multiplier

79

BOK's Tools of Monetary Control

- Influences the quantity of reserves
  - Open-market operations
  - Bok lending to banks –discount rate
- Influences the reserve ratio
  - Reserve requirements
  - Paying interest on reserves

80

Bok's Tools of Monetary Control

- **Open-market operations**
  - **Purchase and sale of government bonds by the BOK**
  - **To increase the money supply**
    - **The BoK buys government bonds**
  - **To reduce the money supply**
    - **The BOK sells government bonds**

81

BOK's Tools of Monetary Control

- **BOK lending to banks**
  - **To increase the money supply**
  - **Discount window**
    - **At the discount rate**
- **The discount rate**
  - **Interest rate on the loans that the Fed makes to banks**
  - **Higher discount rate**
    - **Reduce the money supply**
  - **Smaller discount rate**
    - **Increase the money supply**

  Cryptocurrency is lending ?

82

BOK's Tools of Monetary Control

- **Reserve requirements**
  - **Minimum amount of reserves that banks must hold against deposits**
    - **An increase in reserve requirement**
      - **Decrease the money supply**
    - **A decrease in reserve requirement**
      - **Increase the money supply**
  - **Used rarely – disrupt business of banking**
  - **Less effective in recent years**
    - **Many banks hold excess reserves**
    - 지급 준비금으로서 금 /당좌예금 대신 가상 통화 사용 시 **?**
    - 지급 준비금 정책으로 가상통화 시용 가능 **?**

83

Financial System Problems

- **The BOK control of the money supply**
  - **Not precise/ Cryptocurrency ? Bitcoin Altcoin**
- **The BOK does not control:**
  - **The amount of money that households choose to hold as deposits in banks**
  - **The amount that bankers choose to lend**

암호 화폐 옹호론자**:** 정보를 소수의 은행이 독점
지급 결제 청산의 과도한 수수료**,** 화폐 시스템 비판 **Financial system problem**
결제처리 속도**.** 수수료 인하 **– altcoin** 암호 화폐개발
화폐발행의 주체를 개인에 돌려줌

84

Moneytarist vs Banking School

Moneytarist (통화학파	Banking School (은행학파
David Ricardo, Alfred Marshall, Arthur Cecil Pigou, Friedrich August von Hayek, Milton Friedman	Henry Thornton, John Fullarton, Thomas Tooke
경제에 있어 통화의 역할은 외생적이기 때문에 통화공급은 경제활동에 영향을 받지 않고 경제 외적 요인 (예를 들어 중앙은행)에 의해 결정되 며 경제활동에 영향을 미치는 지배적 요인이라 고 주장	통화를 경제활동의 결과로 간주하고 통화의 공급은 통화수요에 의해 이루어진다고 주장
중앙은행이 통화정책을 이용하여 통화량 조절 을 통한 완전고용, 물가안정, 국제수지향상, 경 제성장촉진 등을 추구	전 세계적으로 통용될 수 있는 가상화폐의 수요가 실제 그러한 화폐를 탄생시키는 현상
2008년 금융위기가 통화학파가 주도하는 화폐 정책의 결과였고 그렇기 때문에 통화학파의 몰락이라고 보는 시각이 있음 (물론 실제로 몰락 하지는 않음)	2008년 금융위기의 반동으로 중앙은행의 통제 를 벗어난 비트코인이 관심을 받게 되었고 이러 한 현상이 기존의 중앙은행 화폐정책 중심의 경 제정책을 주도해온 통화학파에서 은행학파로 패러다임을 움직이고자 하는 수요가 존재하기 때문이라 생각

Financial (Monetary) Policy : M1 vs Interest Rate

- **Final goals, Intermediate targets, and Policy Instruments**
- **Final goals:**
  - **Employment, Price, Economic Growth, Income Distribution**
- **Policy Instruments:**
  - **Required reserve ratio, Discount rate, Open market operation**
- **Intermediate targets:**
  - **M1, M2 and Interest rate (통화량, 이자율 등)**
  - 최종목표와 체계적이고 안정적인 관계를 가져야 하며, 정책수단을 통해 쉽게 통제할 수 있어야 함
  - 변수 동향의 측정이 용이해 상황 판단이 쉬워야 함

M1 and Interest Rate as Intermediate targets

- **M1 as Intermediate targets – accept the volatility of Interest Rate**

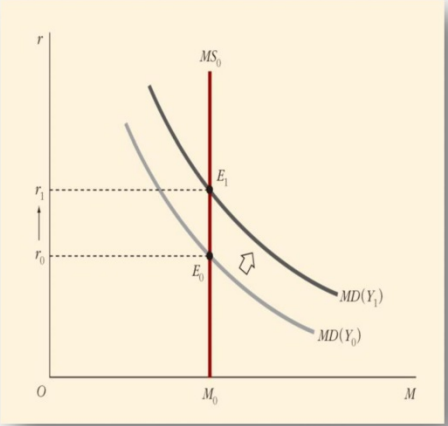
  ex. GDP increase → money demand shift right →
  interest rate increase

- **Interest Rate as Intermediate targets - accept the volatility of M1**

  ex. GDP increase → M1 increase → interest rate is stable
  (통화량을 증가 →이자율을 종전의 수준에 유지)

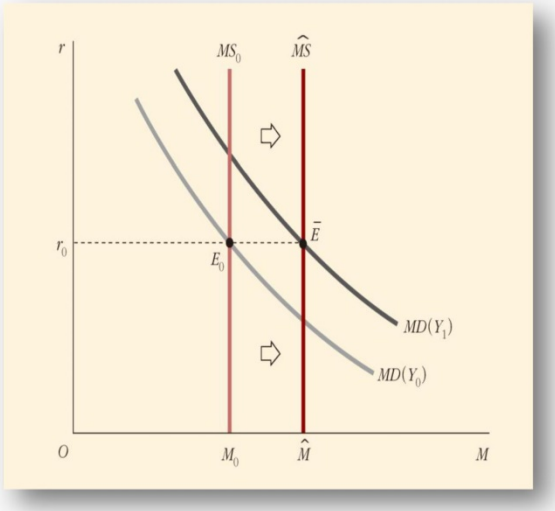
87

M1 as Intermediate targets



88

Interest Rate as Intermediate targets



59

Cryptocurrency's Impact on Financial Policy?

Financial (Monetary) Policy : M1 vs Interest Rate ?

Interest Rate Policy: 기준금리를 이용한 통화량 조절을 통한 경제 영향력 감소 예상

If BOK decrease interest rate (중앙은행이 기준금리를 내리면)

전반적 이자율 하락 a 저축이 덜 낮은 이자율을 통해 더 많은 부채매력적이 되어 저축이 감소를 감당가능

Money supply: 통화공급 증가 a 투자가 활성화를 통해 경제가 더 빠르게 성장

If saving is chaged to cryptocurrency, monetary policy is not work?전 세계적으로 통용되고 공급량이 고정되어 있는 가상화폐가 존재하면 한 국가에서 기준금리를 낮춘다면 사람들은 자신들의 저축을 가상화폐로 바꿀것 a 통화정책의 영향력 감소

Question on Bok's Interest Policy if cryptocurrency is settled ? 세계적으로 통용되는 가상화폐가 정착한다면 중앙은행의 기준금리 발표에 지금 보다는 덜 관심을 가지게 될 것

Crypto Currencies and Financial Policy

Miracle Of Bitcoin

Removes two pillars of money:

- "trust"

  => Peer 2 Peer self-regulation

  based on self-interest?

- legal/government protection and policing

  => anarchy!

  Miracle Of Bitcoin, CBDC 등장, Regional currency 등장

  Monetary Policy Problem ? – Different Target 통화정책이 과연 다양한 목표를 동시에 달성할 수 있는지에 대한 회의

Crypto Currencies: Financial Crisis problems: bank run

Cyprus vs. Bitcoin – April 2013 correlation in Google searches

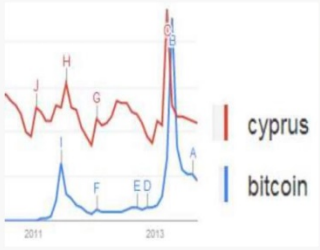
- there was a Cyprus banking crisis…

  depositors were unable to recover 100%

  of their deposits

- opinions about how crazy it was that bitcoin

  could rise…



Nicolas T. Courtois 2009-2014

Seigniorage (시뇨리지 : 주조 차익)

Seigniorage(시뇨리지) = 화폐명목가격 - 화폐 발행에 드는 비용

Seigniorage is decreased ? 흔히 중앙은행의 통제에서 벗어난 화폐의 등장은 시뇨리지 감소를 가져와 추가 세금을 발생 시킬 것 이라 말함 à 일단 '추가' 라는 말이 맞지 않음

중앙은행이 기준금리를 낮추어 통화공급을 늘려 인플레이션이 발생하면 기 존 화폐에서 실질가치가 줄어들고 그만큼의 부가 중앙은행으로 가기 때문 에 인플레이션은 시뇨리지를 통한 세금의 한 종류

비트코인이나 이더리움이 화폐로 정착한다면 위에서 말한대로 기준금리를 통한 화폐정책이 어려워지기 때문에 시뇨리지를 통한 인플레이션 세금의 규모는 감소할 것 à 시뇨리지 감소

그러나 (암호화폐를 포함한) 가상화폐 활성화를 통해 작은 단위, 특히 발행 비용이 높지만 화폐의 가치가 낮아 역(逆)시뇨리지(화폐발행을 통한 손실) 의 주요 원인인 동전의 이용 감소 예상 à 시뇨리지 증가

Seigniorage decrease 암호화폐의 정책이 시뇨리지를 증가시킬 지 감소시킬 지는 정확히 알 수 없음
à 시뇨리지 감소의 가능성은 반만 맞는 이야기

Classical Dichotomy

- **Nominal variables**
  - **Variables measured in monetary units**
    - **Dollar prices**
- **Real variables**
  - **Variables measured in physical units**
    - **Relative prices, real wages, real interest rate**
- **Classical dichotomy**
  - **Theoretical separation of nominal and real variables**

94

Classical Dichotomy

- Developments in the monetary system
  - Influence nominal variables
  - Irrelevant for explaining real variables
- Monetary neutrality
  - Changes in money supply don't affect real variables
  - Not completely realistic in short-run
  - Correct in the long run

95

Velocity and the Quantity Equation

- Velocity of money (V)
  - Rate at which money changes hands
- $V = (P \times Y) / M$

  P = price level (GDP deflator)

  Y = real GDP

  M = quantity of money

96

Velocity and the Quantity Equation

- Quantity equation: $M \times V = P \times Y$
  - Quantity of money (M)
  - Velocity of money (V)
  - Dollar value of the economy's output of goods and services ($P \times Y$)
  - Shows: an increase in quantity of money
    - Must be reflected in:
      - Price level must rise
      - Quantity of output must rise
      - Velocity of money must fall

97

Quantity Theory of Money

1. Velocity of money
   - Relatively stable over time
2. Changes in quantity of money, M
   - Proportionate changes in nominal value of output ($P \times Y$)
3. Economy's output of goods & services, Y
   - Primarily determined by factor supplies
   - And available production technology
   - Money does not affect output

98

Quantity Theory of Money

4. Change in money supply, M
   - Induces proportional changes in the nominal value of output (P × Y)
     - Reflected in changes in the price level (P)
5. When the central bank increases the money supply rapidly
   - High rate of inflation

99

Bitcoin Price Trend & Market Value

100

Economic value Model of Cryptocurrency (Bitcoin)2:

- **Future value Model and Velocity of Blockchain Coin :** 블록체인코인/토큰의유통속도와가치
- **[Velocity of coin]**블록체인기반으로 생성된코인/토큰이 재화나서비스의거래를위해 일정기간 동안 사용되는 빈도수를 말하며, 코인/토큰의가치는 일반적으로 유통속도에 반비례하지만, 건강한생태계를 위해 적정 유통 속도를 유지해야하고 초기설계에 반영

- **[Chris Burniske definition] MV=PQ**
- **M : size of the asset base**
- **V: velocity of the asset**
- **(the number of times that an average coin changes hands every day)**
- **P: price of the digital resource being provisioned**
- **Q: quantity of the digital resource being provisioned**

- **[Vitalik Buterin definition] MC=TH**
- **M : total money supply (or total number of coins),**
- **C: price of the currency (or 1/P, with P being price level),**
- **T: transaction volume (the economic value of transactions per time),**
- **H: 1/V (the time that a user holds a coin before using it to make a transaction)**

101

Economic value Model of Cryptocurrency (Bitcoin):

Future value Model:

- **1) Velocity and the Quantity Equation of Exchange**
- **MV = PQ**
- **M= Bitcoin and money supply (현재 17,398,700, 최대 21,000,000개)**
- **V = velocity of bitcoin (이전가격바탕 9를 유지 추정)**
- **P= average price level of goods (비트코인의 가격 역수)**
- **Q = total number of bitcoin transaction (** 지하경제에 공급되는 재화와 서비스**)**
- **Bitcoin price 1/P = Q/MV**
- **(1/p) = 7,000 billion dollar / 21,000,000 BTC/9 = 37,037 dollar/BTC**
- **2027**년 비트코인 **1**개당 가격은 **3**만달러 형성 추정

102

The value of financial assets: Economic value of Coin A

The value of financial assets: Net Present value(NPV)

Assumption: Utility Coin A가 **1**년 된 온라인 상에서 이용되는 유틸리티 코인
가치 평가**:** 코인 유지하기 위하여 필요한 운영비 조달 **(r** 이자율**)**
코인 매각을 통하여 현금 흐름을 추정 **NPV**를 이용하여 현재가치 추정
회사 보유 코인의 가치를 적정현금 흐름을 통하여 **NPV**추정

$$\text{Value} = \frac{CF_1}{(1+r)^1} + \frac{CF_2}{(1+r)^2} + \ldots + \frac{CF_n}{(1+r)^n}$$

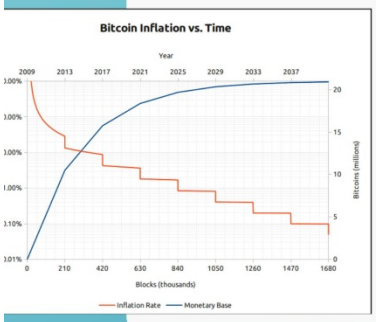
Crypto Currencies

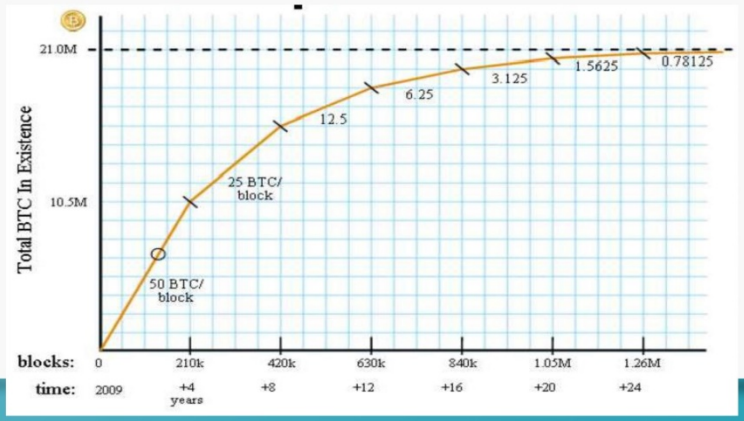
Growth Coins
vs.
Deflationary Coins

Bitcoin Monopoly Rents
Accidental, more than
deserved.

Reward Halving

Built-in Deflationary Scarcity





Crypto Currencies

Why Growth Coins Will Win???

This argument comes from Robert Sams, "The Marginal Cost of Cryptocurrency":
http://cryptonomics.org/2014/01/15/the-marginal-cost-of-cryptocurrency/

Argument: sooner or later "growth coins" vs. "deflationary currencies" which he improperly calls "log coins" will be in competition.

Then the argument is not very clear, he claims more or less that:

- in deflationary currencies, most of the profit from appreciation will be received by holders of co ins through their constant appreciation
- little profit will be made by miners who control the network nevertheless
  => they will impose high fees
- in growth coins, there will be more seignorage profit and it will be spent on hashing. M iners will make good profits and transaction fees will be lower.
- thus year after year people will prefer growth coins…

Nicolas T. Courtois 2009-2014

Blockchain and Central Bank Digital Currency (CBDC)

CBDC contents

I. Background of CBDC

II. Definition of CBDC

III. Effects of CBDC on Central Bank

IV. Legal Issue of CBDC

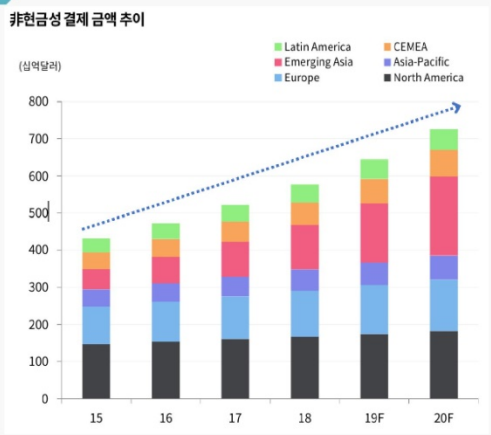
V. Position of Each Country's CBDC

107

Blockchain and Central Bank Digital Currency (CBDC)

Cashless Society

- Sweden is used cashless society
- credit is used than cash
- cashless society is realized



Sources: 암호자산과 중앙은행 , BOK, 2019

108

Blockchain and Central Bank Digital Currency (CBDC)

Sweden CBDC

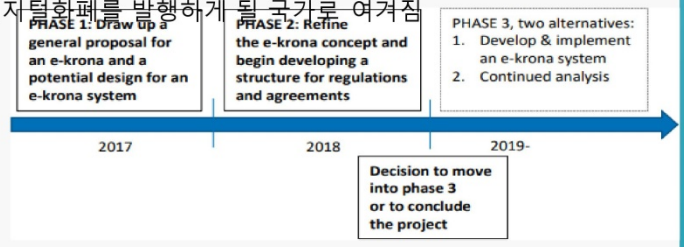
E-Krona Project 2019년
디지털화폐 발행을 목표로 추진

E-krona

The use of banknotes and coins is declining in society. At the same time, technological advances with regard to electronic money and payment methods are moving rapidly. The Riksbank has therefore started a project aimed at examining whether the krona needs to be issued in an electronic form, an "e-krona". No decision has yet been taking on issuing an "e-krona" or on what technical solution would be used.

First CBDC Country:
블록체인 기술을 포함한 **20**여 개 회사로 부터 제안을 받아 기술을 검토하고 있음

현실적으로 가장 먼저 중앙은행 디지털화폐를 발행하게 될 국가로 여겨짐



■ Central BanK Digital Currency (CBDC) Definition
- CBDC is national currency-denomiated claim on Central bank:
전자적 형태로 발행되는 중앙은행 화폐*를 말함
*기존 지준예치금**(reserves)**도 그 형태상 **CBDC**와 유사하나, 논의의 편의를 위해 중앙은행이 새로이 발행하는 전자화폐를 **CBDC**로 정의

governance / technology	Central Bank	Private (혹은 주체가 없음)
Digital Money Tech (IC카드 기술, 비접촉 통신 기술 등)	**Digital Money** (전자 현금) 전자법화(ELT)	**Digital Money: (**전자화폐**)**
Blockchain (블록체인**)** (분산형 장부 기술)	CBDC(Central Bank Digital Currency: 중앙은행 디지털화폐)	**Private digital currency** (Bitcoin)

	CBDC/ 현금형 디지털화폐	Cryptocurrency/가상화폐
governance	**Central bank**	no
governance of system	**Central bank**	no
Currency unit	Won Yen $(원, 달러, 엔)	(BTC:독자적인 화폐 단위)
legal	**yes**	no
Blockchain	**Public** Blockchain	**Public** Blockchain
거래 승인자	검토필요	누구든지
reward for mining 채굴에 대한 보상	**No**	Yes
Transaction time 거래 확정 시간	**?**	**10** minutes

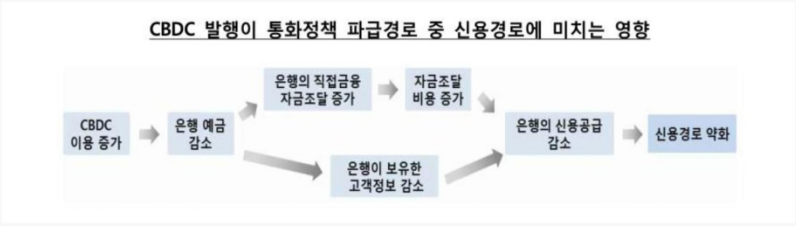
Blockchain and Central Bank Digital Currency (CBDC)

Effects of CBDC on Central Bank

1. The Effect of CBDC on Monetary Policy

■ spillover effect on Credit

- **CBDC**의 이용이 확산될 경우 은행예금 감소요인으로 작용하여 통화정책의 신용경로를 부분적으로 약화시킬 가능성이 있음
- 현금에 비해 결제 편의성이 높은 **CBDC**의 발행은 수시 입출식 예금등 일부 은행예금의 이탈 요인으로 작용
- 은행예금의 감소는 은행의 대차대조표 축소, 자금조달 및 정보획득 비용 증가 등을 통해 신용공급을 제약
- 일반적으로 자본금 확충, 은행채 발행 등 직접금융방식의 자금 조달 비용은 예금 등 간접금융을 통한 자금조달 비용을 상회



Blockchain and Central Bank Digital Currency (CBDC)

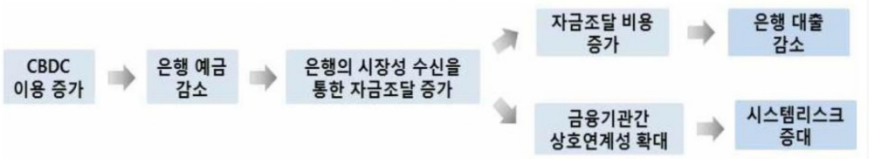
Effects of CBDC on Central Bank

2. Financial Stability

■ The function of Bank 's financial Intermediary is weakened (은행의 자금중개기능 약화**)**

- 제주체들이 은행예금 중 일부를 **CBDC**로 교환 . 보유하는 경우, 예금감소 및 이에 대응한 시장성 수신 증가가 자금조달비용을 증가시키고 그 결과 대출 등 자산운용이 위축되는 등 은행의 자금중개기능이 약화될 가능성이 큼
- 한편 시장성 수신의 증가는 금융기관간 상호연계성을 확대시켜 시스템리스크도 증대될 소지

CBDC로의 자금이동에 따른 영향



Sources:BOK , Cryptocurrency Asset & Central Bank,, 2019

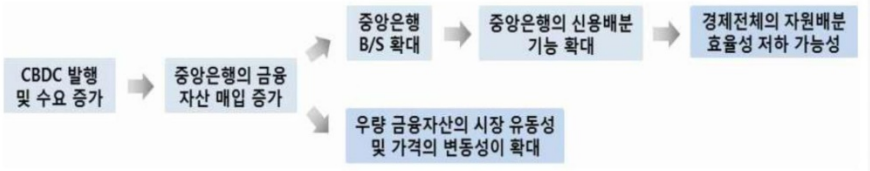
Blockchain and Central Bank Digital Currency (CBDC)

Effects of CBDC on Central Bank

3. Conflict with Fractional Reserve Banking System (부분지급준비제도와 충돌**)**
- The function of bank is weaken
4. Financial Stability : ■ Central Bank B/L Expand

- **CBDC** 발행 및 수요증가는 중앙은행의 자산·부채 규모를 확대시킴으로써 중앙은행의 신용배분 기능은 확대되는 반면, 금융시장의 신용배분 기능은 축소될 가능성이 있음

CBDC 발행 및 수요증가가 중앙은행 대차대조표 등에 미치는 영향



Sources:BOK , Cryptocurrency Asset & Central Bank,, 2019

Blockchain and Central Bank Digital Currency (CBDC)

Effects of CBDC on Central Bank

5. 부분지급준비제도(Fractional Reserve Banking System)와의 충돌

■ 부분지급준비제도는 은행이 고객이 맡긴 돈의 일정 비율 이상을 현금으로 가지고 있어야 하는 제도.

■ 부분지급준비제도의 핵심은 고객이 맡긴 예금을 보증금 삼아 중앙은행이 발행한 본원화폐보다 훨씬 많은 신용화폐를 시중은행이 발행할 수 있도록 하는 것.

■ 예금이 전액 **CBDC** 로 들어가면 시중은행의 역할은 주택담보대출 같은 장기 대출을 중개하는 정도로 축소될 것.

■ 다만 송금, 상거래 지급, 현금 인출 등 현재 은행이 제공하고 있는 대고객 지급서비스를 중앙은행이 직접 제공 또는 지원함에 따라 운영리스크 발생 경로가 확대될 수 있을 것으로 보임.

■ 중앙은행 입장에서는 자산 버블 등 위험 요소를 통제하고 뱅크런을 방지하는 데 용이해지기 때문에**CBDC** 도입이 유리한 측면 존재.

■ 화폐의 발권과 통화조절, 지급 결제를 비롯해 사실상 예금 수신 등의 업무까지 중앙은행에 집중되면 시중은행들은 존립 자체의 위협이 커지고, 이는 금융 안정성을 해칠 수도 있음.

■ 현재와 같이 고객이 시중은행에 예금을 예치하도록 하면서 금융기관간 거래에는 디지털화폐를 이용하는 중재안도 있을 수 있으며 이렇게 되면 신속하고 안전하며, 보안 유지에도 장점이 있지만, 자산 버블과 뱅크런 등 위기 대응에 취약한 것은 부분지급준비제도와 큰 차이가 없을 것으로 보임.

Blockchain and Central Bank Digital Currency (CBDC)

Ⅳ. Effects of CBDC on Central Bank

Bok's B/L (중앙은행 대차대조표에 미치는 영향)

◈ 디지털 통화 등장으로 인한 효과

Table 3: Stylized balance sheets with digital currencies

Households			Commercial banks			Central Bank	
Assets	Liabilities		Assets	Liabilities		Assets	Liabilities
Banknotes	Loans		Loans	Deposits		Foreign reserves	Bank notes in circulation
Deposits			Securities			Domestic assets	Commercial bank deposits
Securities			Central bank deposits				
Digital currencies			Vault cash				

Ⅳ. Effects of CBDC on Central Bank

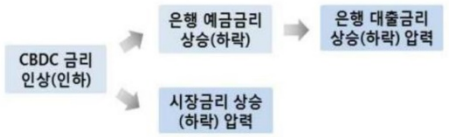
5. The Effect of Interest Rate (CBDC에 대한 이자지급시 영향)

■ **(+) Interest Rate** (금리 지급시)

- 중앙은행이 **CBDC**에 일정 수준의 이자를 지급 할 경우 은행예금 이탈이 증가 하여 은행의 신용공급 여력이 저하될 가능성이 높고 **CBDC** 금리 수준은 은행 여수신금리의 하한 및 시장금리의 기준 **(benchmark)** 으로 작동할 가능성이 큼
- 중앙은행이 **CBDC** 금리를 인상 **(인하)** 할 경우 **CBDC**보다 높은 지급 불능 위험 이 있는 은행의 예금금리는 즉각적으로 상승 **(하락)** 하고 대출금리 및 시장금리에도 상승 **(하락)** 압력을 유발

■ **(-) Interest Rate** (마이너스 금리 부과)
내수 확대

CBDC에 정(+)의 금리 지급시 금리파급경로에 미치는 영향



Sources:BOK , Cryptocurrency Asset & Central Bank,, 2019

Blockchain and Central Bank Digital Currency (CBDC)

Effects of CBDC on Central Bank

2. 통화정책(CBDC 발행에 따른 영향)

■ 통화정책수단 측면

- **CBDC** 도입으로 중앙은행이 위기시 내수 촉진, 디플레이션 압력 완화 등을 도모하기 위해 가계 및 기업에 **CBDC**를 일괄공급 **(helicopter money)** 하는 정책 집행이 용이해지는 장점이 있음
- 일괄공급 정책은 **CBDC** 계정을 통해 민간을 직접 대상으로 한다는 점에서 기존 양적완화 정책에 비해 집행이 수월하고 효과가 즉각적일 것으로 판단

■ 공개시장운영 측면

- **CBDC** 도입으로 인한 금융권역간, 금융기관간, 금융상품간 자금이동과 이로 인한 지준수요 변동 등이 발생하는 바, 중앙은행은 공개시장 운영시 이를 추가적인 외생적 요인으로 고려할 필요가 있음
- 경제주체들이 은행예금을 **CBDC**로 교환·보유할 경우 은행의 지준 수요에 변동을 초래
- 더불어 **CBDC**와 지급준비금간 일대일 교환이 허용 **58)** 될 경우 은행과 가계 및 기업간 단기 대차거래 가 늘어날 수 있어 금융기관간 지준시장에 영향을 미칠 가능성
- 다만 은행이 불특정 다수의 가계 및 기업을 대상으로 적시에 적정 규모의 자금을 차입하거나 예치하는 데에는 현실적 어려 움이 크고 거래 대상인 가계 및 기업의 신용리스크를 고려해야 한다는 점에서 이러한 가능성은 높지 않을 것으로 판단

Blockchain and Central Bank Digital Currency (CBDC)

Effects of CBDC on Central Bank

Sources:BOK , Cryptocurrency Asset & Central Bank,, 2019

통화정책에 미치는 영향

구분	현재와 비교시 영향
▪파급경로	- CBDC 발행 및 이에 대한 이자지급은 수시입출식예금 등 일부 은행예금의 이탈 및 이에 따른 신용공급능력 제약 등으로 신용경로를 통한 통화정책의 파급효과가 약화될 가능성 - CBDC에 대해 이자지급시 CBDC 금리 수준은 은행 여수신금리의 하한 및 시장금리의 기준(benchmark)으로 작동할 것으로 예상 o CBDC에 대한 금리 조정을 통해 여수신금리의 변동을 유발하는 새로운 파급경로를 활용 가능
▪정책수단	- 위기시 내수 촉진, 디플레이션 압력 완화 등을 위해 CBDC를 일괄 공급하는 정책 집행이 용이해짐 - CBDC 금리 조정을 통해 시장금리 및 은행 여수신 금리에 영향을 미칠 수 있음 o 경기침체가 심화된 상황에서는 내수촉진을 목적으로 CBDC에 마이너스 금리 부과 가능
▪공개시장운영	- 금융권역간, 기관간, 금융상품간 자금이동을 유발하여 지준수요 변동 요인으로 작용할 가능성

Blockchain and Central Bank Digital Currency (CBDC)

IV. Effects of CBDC on Central Bank

6.Traditional Financial System Threat (전통 금융시스템의 안정성 위협)

Sources: BOK , Cryptocurrency Asset & Central Bank,,2019

CBDC 의 주요 단점

단점	이유
사회 금융 중개기능 위축	중앙은행과 시중은행의 업무 중복에 따른 중개 기능 위축
시중은행 수익성 악화	시중은행 위축 → 예금 감소 → 자금조달비용 상승 → 예금 감소의 악순환
CBDC 로 자금 이동 우려	CBDC 는 새로운 안전자산으로 부상. 이에 따라 안전자산 선호심리가 강해지면 은행예금에서 CBDC 로 자금 유출 우려
금융자원배분 효율성 저하	CBDC 발행으로 중앙은행의 시장 참여도가 높아짐. 이에 따라 금융자원배분의 효율성 저하 우려 존재
신용경로 약화	시중은행 예금 감소→은행의 대차대조표 축소 등을 통해 신용공급 제약

Blockchain and Central Bank Digital Currency (CBDC)

Effects of CBDC on Central Bank

6. 지하경제 양성화 효과

■ 인도의 경우 화폐개혁이 시행되자 거래 투명성이 확보되며 소득세 납입이 크게 증가했고, 세수 기반이 확대되는 효과가 나타남.

■ **CBDC** 가발행되면 이런 긍정적인 효과는 더욱 커짐

■ **CBDC** 는 중앙은행이 컨트롤할 수있고, 유통경로와 수량을 추적할 수 있어 지하경제의 양성화효과를 가져올 수 있으며 이에 따른 세수효과의 개선

CBDC 의 주요 장점

장점	이유
신용리스크 경감	CBDC 의 송금과 거래에서 중앙은행을 이용하므로 결제은행이 다름에 따른 신용리스크 無
효율성 제고	속도가 빠르고, 처리비용 감소 효과
비용절감	화폐의 유통과 관리에 들어가는 비용 절감
지하경제 양성화	중앙은행이 현금 유통 추적이 가능해 지하경제의 양성화 효과 나타남. 세수효과 개선도 기대
통화정책	통화정책 효율성 제고와 다양한 정책수단 확보

121

Blockchain and Central Bank Digital Currency (CBDC)

Each country's Position on CBDC

Korea: Bok law (한국은행법)- negative

■ **CBDC** 도입시 법화성 및 발행의 법적 근거, 이자지급 및 마이너스 금리 부과 가능 여부 등과 관련한 불확실성 해소를 위해 「한국은행법」 개정이 필요함

Sources: BOK , Cryptocurrency Asset & Central Bank,,2019

주요국 중앙은행의 CBDC 에 대한 입장

국가	CBDC 에 대한 입장
스웨덴	현금이용 비중 하락으로 인해 E-Krona 프로젝트를 진행 중
영국	CBDC 를 주요 연구과제로 선정. 구체적인 발행계획은 미정
미국	CBDC 에 대해 부정적 입장 유지
캐나다	분산원장기술 기반 디지털토큰인 CADCoin 발행 및 도입 검토
일본	CBDC 발행계획은 없다고 언급
네덜란드	DNB Coin 개발 및 테스트 진행. 현재 발행 및 도입 계획은 없음
덴마크	E-Krone 발행 검토. CBDC 의 불확실성으로 인해 발행 계획은 미정
싱가포르	실시간 총액결제 시스템 구축을 위해 Ubin 프로젝트 진행 중
중국	은행간 결제에 CBDC 활용 시도, Digital Currency Electronic Payment 개발중이라고 언급
러시아	대통령의 암호루블 발행 계획 공식 발표 및 법정지급수단 등록을 위한 민법 개정안 의회 계류 중
베네수엘라	암호자산 Petro 를 발행. 그러나 유가 변동 노출 및 강제통용력 부재
에콰도르	미 달러화로 Dinero electrónico 를 발행. 최근 발행 및 이용 중단
브라질	Hyperledger 및 Corda 를 활용한 CBDC 개념검증 진행 중
우루과이	국영 이동통신사 고객 10,000 명을 대상으로 e-Peso 테스트
에스토니아	전자영주권과 연동되는 에스트코인 발행계획 발표

122

Fixed Exchange Rate vs Muliple Currency System

Fixed Exchange Rate 고정환율제	Muliple Currency System 다중화폐제
금본위제, 브레튼 우드 체제, EU, 현재 중국, 대 부분의 개발도상국	민간화폐제도 (북송, 근대유럽, 미국의 자유은 행시대 등), 스위스, 남미 (달러)
장점: 편리함, 단순함 단점: 금융위기라고 불리우는 조정과정, 비대칭 적인 GDP 배분	장점: 효율성, 유연성, 자율성, 안정성 단점: 정보비대칭 또는 화폐발행력 상실로 인한 화폐정책 포기
비트코인을 비롯한 암호화폐들이 새로운 고정 환율제의 기폭제가 될 것이라는 주장의 가장 중요한 가정은 명목화폐의 Crowding Out à이론적,직관적,실증적으로분석해보았을 때 사실이 아닐 확률이 높음	전세계적으로통용되는암호화폐의등장은국 제화폐+로컬화폐라는다중화폐제를촉진시 킬 확률이 높음 à민간화폐제도와비슷하나레버리지와통화 공급량이조작(?) 불가라는점에서차이있음

Fixed Exchange Rate : Bretton Woods System

Bitcoin & Bretton Woods System
비트코인을 기준으로 나머지 알트코인을 거래: 브레튼 우즈 체제 처럼.. 비트코인이 미국 달러의 역할?
역시나 브레튼 우즈 체제의 배경에 대한 정확한 이해가 선행 되어야 함

세계 2차대전으로 인해 대부분의 유럽경제는 파탄 전후 주요 국가에서 초인플레이션 발생, 화폐가치 급락

전간기에 포기한 금본위제로의 부분적 복귀 현상 à 화폐가치의 안정화 압도적으로 많은 금을 보유한 미국 달러는 우위를 차지

화이트: 채권국 (미국)의 환율안정 중시 케인즈: 채무국 (영국)의 국제신용요건 완화 — 미국 승리

완전고용과 물가안정을 촉진하는 동시에 국제무역을 제한하지 않으면서도 대외균형을 달성할 수 있게 하는 국제화폐제도를 설계

모순적: 고정환율제는 무역을 원활하게 해주지만 국내 정책목표를 달성하 려면 무역 불균형을 해소할 수단이 없어 양자택일을 해야만 함

Fixed Exchange Rate : Bretton Woods System

Bretton Woods System : 브레튼우즈를 정말 스페셜하게 만들어 주는 것은 IMF 고정환율제가 가져오는 경직성을 완화하려는 시도

1개의 기준화폐와 N-1 개의 화폐로 구성되는 금본위제
à 국제공조의 금본위제, 이미 경험했음

회원국들은 국내 경제목표를 달성하기 위해 IMF 에서 대출 가능
à IMF 펀드가 회원국들이 낸 것이기 때문에 결국 연대 보험

국제수지가 근본적인 불균형이라는 IMF의 동의가 있으면 달러 환율을 조정 할 수 있음, 단 미달러에는 적용 못함
à 상식적, 합리적, 50, 60년대 경제성장을 주도

Liquidity dilemma:
유동성 딜레마: 금의 공급은 한정되어 있기 때문에 기축통화 국가의 무역수지가 국제 유동성 결정 à 미국은 중용을 지켜야 함, 문제가 생기면?

다른 화폐는 능동적으로 평가가치 변경가능, 미달러는 안되기 때문에 미국 의 국제수지 조정이 매우 어려움

International Monetary System

	Gold Standard	Bretton Woods I	Bretton Woods II	Bitcoin Standard
FX	고정	고정	변동	고정
M/P	비효과적	비효과적	효과적	비효과적
Price	국가간 연동 (deflationary)	국가간 연동	독자적	국가간 연동
Real Output	중립적	촉진적	제약적	촉진적
Trade	중립적	촉진적	제약적	촉진적
Current Account	균형	불균형	균형	균형

Bitcoin vs Altcoin

Bitcoin is key currency : 비트코인을 기축화폐로 알트코인을 기타 통화

Gold? Fixed Exchange Rate? IMF

Implication 1 : new Bretton Woods System 새로운 브레튼 우드 체제를 탄생시킬 것으로 예상하지 않음

Implication 2 : Fixed Exchange Rate가상화폐에 유입된 자본의 투기성을 고려하면
고정환율제가 가능하지 않을 것

Crypto Currencies

Can Bitcoin Survive?

Brand+Netwok Value

Network effects (positive externality). Number of users
Their Medium of Exchange (MOE) function: sum of outstanding balances.
Trust and reputation etc…

- Scability and Security:
- Decentralization
- Governance

Problems of Cryptocurrency Scability, Decentralization and Security:

1. Scability and Security:기술적인 문제로서 확장성과 보안성 문제

- Security :트랙픽 중가에 따른 처리 시간 지체 – 보안상 문제로 이중 사용 문제

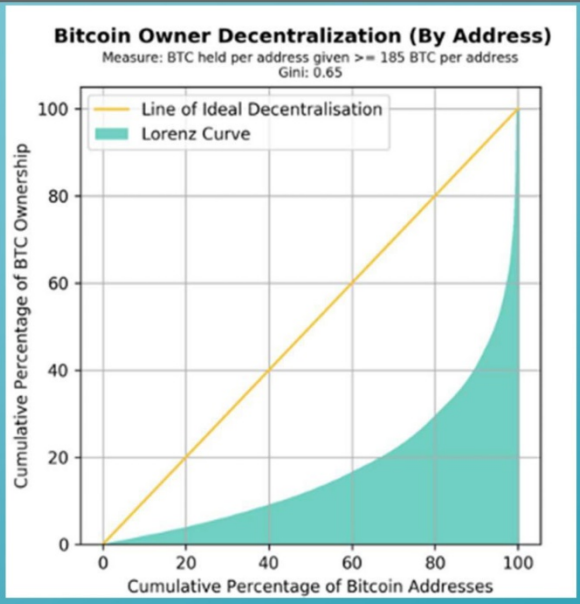
2. Deflationary Money :화폐 공급의 제한성(붕괴성) -

-비트코인은 총 2100 만개 만 채굴되도록 디자인 4년마다 보상 채굴이 반감

3. Speculations : 가격 변동성(Price Volatioity) 의 문제 ()
- 2 달러에서 시작 현재 4000 달러 – 투기수요 자극 버블 형성

4. Decentralization -Goverances: 지배구조의 문제
- 암호 화폐가 일부 소수에게 집중

Gini coefficient: 0.65 13개 전문 업체가 전 비트코인의 50%, 10개 미만의 업체가 90 % 소유



Problem of Cryptocurrency- Solution
(암호 화폐 문제점 개선방향)

1. Transaction time : 블록의 크기 확대

- **트랜잭션 처리시간은 비트코인 1시간, 이더리움 2분이상 소요, 리플(Ripple)은 4초 걸리는 암호화폐 출현**

2. volatility ? -안정적 화폐와 연동

- **Tether와 같이 안정적인 달러와 가치연동을 하여 가격변동성을 줄이는 방향(stable coin)**

3. Token coin의 발행,- Deflationary Money 문제 해결

- **(two-sided market: 양면시장)의 발전 - Steemit의 경우 컬럼의 댓글 수에 따라 토큰(steem)을 지불**

4. Decentralization -Goverances 공정한 거버넌스 구축
Seigniorage (주조차익)을 공정하게 배분

Conclusion: Blockchain and Cryptocurrency

Bitcoin is used as Asset/ Co-exist with Fiat Money

The effect of Financial Policy : 화폐로 충분히 그럴 수 있는 가능성 존재 : 금융 정책에 영향

-New Facts? :경험해 보지 못한 완전히 새로운 현상이 아님

-Demand of Crypto currency exist

- Central Bank System Problem- Macro Problem
중앙은행이나 현 제도에 대한 반발로 접근할 문제가 아님 : 훨씬 더 거시적인 문제

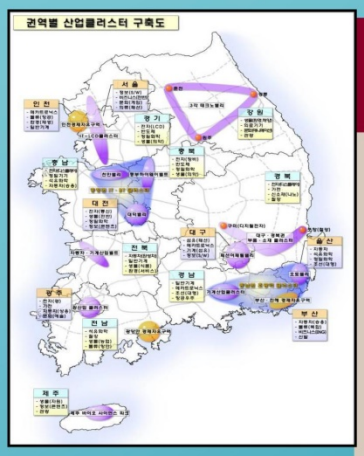
다만 가상화폐라는 특수성에 대한 고민 부족
- 다양한 시각에서 추가적인 연구 필요

Monetary Policy: impact interest rate and M1

Limit factors and The way to improve the limitations of blockchain technology

	limitations	Improvements
Technical field	(1) Lack of standardization (2) Insufficient integration (3) Lack of scalability (4) Unclear cancellation or correction policies (5) Excessive verification costs (6) Insufficient personal information protection (7) Not enough to respond to hacking defense.	(1) Ensuring standardization (2) Secure integration (3) Securing scalability (4) Establishing cancellation or correction policies (5) Transaction verification cost efficiency (6) The protection of personal information (7) Countermeasure against hacking.
Service field	(1) Lack of utilization of the blockchain (2) Security threat (3) Shortage of skilled workers (4) Lack of legal liability.	(1) Suggesting various application methods (2) Against security threat preparation (3) Training professional manpower (4) Securing legal responsibility.
Legal system field	(1) Inadequate legal compliance (2) Lack of relevant regulation (3) Uncertainty in the regulation.	(1) Preparation of legal responses (2) Preparing of relevant regulations (3) Clarification of regulations.

GIST's Innovation Industrial Cluster Valley ?
Blockchain and Cryptocurrency cluster ?



유람선 과 뗏목

Homework 1

- **What is The functions of money ? The Kinds of Money**
- **Measures of money stock**
- **The Money Multiplier**
- **Bok's Tools of Monetary Control**
- **Velocity and the Quantity Equation**
- **Financial policy instruments**
- **Explain why banks can influence the money supply if the required reserve ratio is less than 100 percent.**
- **List two examples of commodity money**
- **Is Bitcoin Money**
- **Key Properties of Bitcoin**

135

Homework 2

- 가상화폐 공급 증가시 화폐 공급에 미치는 영향은 무엇인가 ?
- 가상화폐의 특징은 무엇인가 ?
- 가상화폐가 출현하게 된 배경은 무엇인가 ?
- 비트코인은 상품인가 ? 화폐인가 ? 자산인가 ?
- 시뇨리지 이익이란 무엇인가 ?
- 그레샴의 법칙은 무엇인가 ?
- 통화학파와 은행학파의 주장은 무엇인가 ?
- 고정환율제하에서 브레튼 우즈 체제란 무엇인가 ?
- 비트코인과 알트코인의 관계 ?
- 고정환율제와 다중환율제란 ?
- **Problems of Cryptocurrency** 개선방안 ?

136

Homework 3

- 중앙은행의 디지털 화폐 **(CBDC)** 란 **?**
- **CBDC**가 통화 정책에 미치는 영향 **?**
- **CBDC**가 통화 정책 중 신용 경로에 미치는 영향 **?**
- **CBDC**로 자금이동에 따른 영향 **?**
- **CBDC**가 중앙은행의 대차대조표에 미치는 영향 **?**
- **CBDC**가 화폐 유통시스템에 미치는 영향 **?**
- **CBDC**에 대한 각국 중앙은행의 입장 **?**
- **CBDC**가 출현 배경**?**
- **CBDC**의 장점은 **?**

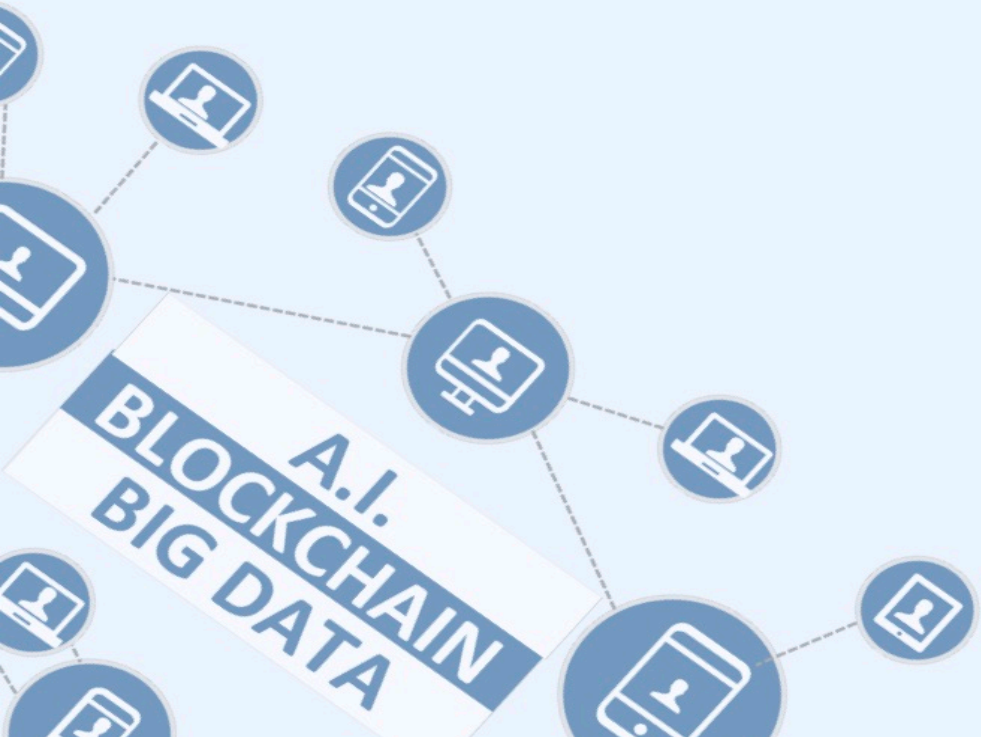
137

11강

디지털 혁신의 규제환경과 네거티브 법률 시스템

구 태 언 변호사

(로펌 Tek&Law)



강의 동영상 URL

1 부: https://youtu.be/lv6UMa7OjGY

2 부: https://youtu.be/MsoNow_jPsM

디지털 혁신의 규제환경과 네거티브 법률 시스템

2019.5.23.

법무법인 린
TEK&LAW 부문장
구태언 변호사
tekoo@law-lin.com

목차

I. 각국 블록체인 산업 관련 규제 최신 동향
II. 정부규제 관련 현황과 전망
III. 증권 형 토큰과 유틸리티 형 토큰에 대한 주요국 입장

생각해봅시다 : 블록체인과 암호화폐가 현실 경제에 미칠 영향

2

I. 각국 블록체인 산업 관련 규제 최신 동향

3

영국령	버뮤다	몰타	지브롤터	
북미	미국	캐나다		
유럽	영국	스위스	독일	프랑스
	리투아니아	우즈베키스탄	에스토니아	
아시아	일본	캄보디아	태국	중국
	싱가포르	인도	필리핀	중국 홍콩

4

I. 각국 블록체인 산업 관련 규제 최신 동향

영국령 블록체인 산업 관련 규제

5

버뮤다

Digital Asset Business Act (DABA) 2018 시행

디지털자산사업 허가 신청 및 취득 절차

➢ 본 법에 의거, 허가가 없는 개인 또는 기업이 디지털자산(암호화폐, 토큰) 서비스 및 거래를 기행 할 시, 본 법을 위반하는 것으로 벌금 또는 형벌 및 기소 처분을 받을 수 있음 (제10조).

➢ 디지털자산사업 희망 시, 허가신청서를 버뮤다 통화청(Bermuda Monetary Authority)에 제출해야 하며, 다음과 같은 사항이 적용됨.

A. 허가를 위한 최소 규준 (Schedule 1)

I. 허가를 받기 위해 허가신청 기업은 최소한 유능한 경영진 및 관계자를 보유해야 하며, 통화청은 경영진의 과거 전과기록 등을 참고 함.
II. 또한, 기업은 신중한 정책 및 태도로 운영되어야 하며, 본국 통화청은 관련기업의 진실성, 경영 구조 및 정책, 회계내역, 보험 및 본법 또는 타 법과 저촉하는지/했는지의 여부를 확인 및 참고 하여 단속 함.
III. 본 규준에 못 미치는 기업 또는 신청인은 자동 탈락 (제13조2항)

6

버유다

Digital Asset Business Act (DABA) 2018 시행

B.면허유형 (제12조)

I. F급 면허: 하나 또는 모든 디지털자산사업 행위를 시행할 수 있음 (시간적 제한이 없음).
II. M급 면허: 하나 또는 모든 디지털자산사업 행위를 시행할 수 있으나, 시간적 제한을 두어 만료기간 전 통화청을 통해 갱신해야 함.

※ 참고로, 신청서에 희망하는 면허유형을 기재하여 제출은 하지만, 통화청에서 신청서와 무관하게 단독적으로 유형을 정할 수 있음.

C.신청서와 첨부해야 하는 자료 (제12조)

I. 사업기획안, 신청인 또는 경영진에 대한 상세정보, 신청인이 도입할 정책 및 절차, 이외 연관된 타 자료.

D.고위급대표자 정보 및 대표자의 의무

I. 버유다 권할 지역에 소재한 기업은 고위급대표자를 의무적으로 보유해야 하며, 본 대표자에 대한 정보 (예: 거주지역, 사무실 소재지 등)를 통화청에 제공해야 함. (제19조)
II. 고위급대표자는 버유다통화청에게 주요사항 및 정보(예: 채무초과 및 파산 또는 허가 하 적용되는 의무)를 보고해야 함. (제20조)

7

버유다

Digital Asset Business Act (DABA) 2018 시행

E.버유다에 본사가 소재해야 하는 의무 (제21조)

I. 디지털자산사업을 가맹하기 요망하는 기업은 버유다에 본사를 보유하고 있어야 하며, 통화청에서 분석 및 단속 시, 기업의 경영체제 및 회의장소를 가만하여 허가를 기각 또는 취소할 수 있음.

F.허가증의 승인 및 제한 절차 (제13조)

I. 허가는 버유다통화청의 승인과 함께 본 기관에서 발급되며, 승인과정에 소요되는 시간은 나타나지 않음.
II. 허가를 승인 시, 위에 언급했듯, 신청인 또는 기업이 희망하는 허가 유형과 달리 통화청이 일방적으로 정할 수 있음 (제14조1항)
    1. 통화청의 소견에 따라 허가증에 기업이 준수 또는 충족시켜야 하는 조건을 개조할 수 있음. (제13조 4항)
    2. 또한, 통화청의 소견에 따라 허가증의 범위 또한 제한할 수 있으며, 예를 들면 모든 암호화폐를 다루지 못하게 하거나, 일정 기간마다 제한된 액수의 암호화폐를 거래 및 환전할 수 있는 규제를 적용할 수 있음. (제13조 3항, 제23조)
III. 면허증이 취소될 수 있는 상황
    1. 면허를 취득한 기업이 본 법을 준수하지 못하거나 않을 시, 면허증이 취소될 수 있음. (제24조)
    2. 또는, 위급사항 시에는 사전 통보 없이 면허증이 취소되거나 정지될 수 있음. (제26조)

8

버뮤다

Companies and Limited Liability Company(Initial Coin Offering) Amendment Act 2018 (2018년 회사 및 유한회사 ICO 개정 법률, 2018.07.09 발효)

I. 본 법안의 발효로 인하여, 버뮤다 내에 ICO를 개최 희망하는 기업은 기업기록관(Registrar of Companies)에 등록해야 함.

II. ICO 발행 전, 전자포맷의 ICO 공시(흔히 '백서' 또는 'white paper'라고 칭함; 이하 '백서')문서를 대중에게 제공해야 하며, ICO 개최기업의 이사 및 대표자들의 서명이 포함된 사본을 기록관에 제출해야 함.

III. 백서에는 본 ICO---의 목적 및 타깃 금액, 모금 사용 기획안, 투자로부터 일어날수 있는 리스크, 사업 및 임원 구성 등이 포함 되야 하며 대중 투자자들에게 최대한 투명도를 높여 안전성을 유도하는 것으로 보임.

IV. ICO 개최기업은 투자자들이 서로 게시글을 통해 소통하며 정보를 얻을 수 있는 수단 및 공간을 제공해야 하며, 투자자들의 신원을 확인해야 함 (KYC 정책).

V. ICO 개최기업의 백서에 허위진술이 있을 경우, 본 당국의 수사기관 및 법률기관을 통해 처벌 받을 수 있으며, 투자자들이 허위진술에 의존하여 투자를 가맹했을 시, 민사소송 또한 가능 함.

VI. 재무부장관은 본 법에 의거하여 핀테크 자문위원회를 설립 및 임명해야 하며, 향 후 개선 및 제정해야 하는 입법은 수동적 입법절차(negative resolution procedure)의 체제로 이행됨. 특히 이 점은 ICO관련 법규를 신속히 제정해 나아가는데 필수요원으로 보임

버뮤다

Companies and Limited Liability Company(Initial Coin Offering) Amendment Act 2018 (2018년 회사 및 유한회사 ICO 개정 법률, 2018.07.09 발효)

ICO 백서에 포함 되야 하는 필수사항 (제34E조)

A. 기업의 지정 또는 기록된 명의 및 주소, 또는 기획자(promoter)의 주요사무실 명의 및 주소;
B. 기획자 상관(上官) 경영자의 명의, 상세내용 및 직함;
C. 사업(business)구성내용 또는 제안된 사업기획
D. 제안하는 프로젝트(project)의 상세내용 및 시각표(timeline);
E. ICO로 모으기 목표하는 금액;
F. 예상되는 모금의 사용 및 지출 기획안;
G. 디지털자산과 연관된 권리 또는 제한;
H. 디지털자산의 공시(offer)를 개최, 마감하는 날짜 및 시각;
I. ICO 공시와(offer) 연관된 주의사항을 설명하는 내용;
    I. 본 주의점에 관한 내용은 다음과 같은 사항이 포함됨 (제34G항):
        1. 합리적으로 예상할 수 있는 주요 리스크에 대한 정보;
        2. ICO가 중도 포기되거나 취소될 시, 투자자의 권리 또는 선택의 여지;
        3. 디지털자산과 연관되는 권한;
        4. ICO 투자 기획과 관련된 보증 포기 각서.
J. 개인정보가 어떻게 사용될 지에 관한 설명서.
K. 위 내용 외, 재무부장관의 견해에 따라 추가적으로 요구되는 사항이 발생 할 수 있음.

10

버뮤다

Companies and Limited Liability Company(Initial Coin Offering) Amendment Act 2018 (2018년 회사 및 유한회사 ICO 개정 법률, 2018.07.09 발효)

ICO 관련 범죄 유형 및 형 (제34J조)

A. 기록관에 접수하지 않거나 관련문서를 제출하지 않을 시, 또는 ICO에 관련하여 허위진술을 범할 시, 즉결처분 (최대 $50,000 또는 1년 징역 또는 둘 다) 또는 기소 및 유죄선고 (최대 $250,000 또는 5년 징역 또는 둘 다) 판정을 받을 수 있음.

ICO 백서에 포함된 허위진술로 인한 민사상 책임 (제34K조)

A. ICO 개최업체 관계자(예: 경영진, 기획자, ICO 백서를 승인한 자 및 본 백시에 기여하거나 내용을 보증한 전문가 포함)는 백서에 기재된 허위진술에 의존하여 디지털자산을 구매한 투자자들에게 민사적 책임이 따르며, 허위진술에 의존하여 투자한 행위를 입증 시, 피해자는 손해배상을 청구할 수 있음.
B. 제외되는 사항은 본 법에 나열되어 있으며, 예로는 백서를 작성할 시, 모든 내용이 사실이라는 것을 합리적으로 믿었을 때 법적 책임을 면할 수 있음. 소송 시, 본 규제를 준수했다는 증거는 피고 측 부담임.

11

몰타

블록체인 섬, 암호화폐 법안 3개 승인

2017. 9 블록체인 워크팀 구축, 국가 전략 제정
2017. 4 세계 최대 암호화폐거래소의 하나인 OKEx 몰타로 업무 이전

암호화폐 관련 법안 3개 승인

- 법안 43 : Malta Digital Innovation Authority Bill(몰타 디지털 혁신 관리 당국 법안)
- 법안 44 : Technology Arrangements Service Bill(기술 안배도 및 서비스 법안)
- 법안 45 : Virtual Financial Assets Act (가상 금융 자산 법안)

12

몰타

블록체인 섬, 암호화폐 법안 3개 승인

법안 43
몰타 디지털 혁신 관리 당국 법안
Malta Digital Innovation Authority Bill

- 몰타의 혁신 기술 부문을 발전을 추진하기 위해서 설립함
- 도덕 표준을 제정하며 소비자와 투자자의 이익을 보호하며 유럽연맹의 표준과의 협조, 조화에 힘씀

법안 44
기술 안배도 및 서비스 법안
Technology Arrangements Service Bill

- 몰타의 디지털혁신관리당국이 사용하는 법안임
- 목적은 관리당국이 혁신적 기술과 서비스를 식별하고 관리하는 것을 지도하는 데 있음
- 과학 기술 서비스 제공자 등록하는 데 또한 과학 기술의 인증에 대해 원칙을 세움

13

몰타

블록체인 섬, 암호화폐 법안 3개 승인

법안 45
가상 금융 자산 법안
Virtual Financial Assets Act

- 회사가 **ICO**를 발행할 때 꼭 지켜야 하는 원칙을 세움
- **ICO**를 **VFA(Virtual Financial Asset)**로 통칭함
- 회사가 **VFA**를 발행하려면 우선 회사가 어떤 일을 하고 있는지 또한 몰타의 법률에 따라 어떻게 할 생각인지에 대한 백서를 작성해야 함
- **VFA**를 발행하려는 회사가 광고 업체에 대해 감독 관리를 해야 함.
- 프로젝트를 감독하기 위해서 **VFA**를 발행하려는 회사가 독립적이고 등록된 **VFA** 대행업체를 지정해야 함
- 이런 **VFA** 대행업체기 발행하는 자와 주관 당국(미정) 간 **VFA**기 **DLT**거래소에서 등록하고, 백서 작성, 거래 때 연락인을 맡을 것임

14

몰타

상위 암호화폐 거래소 블록체인 섬으로 이동

거래 가치 세계 5위 거래소: ZB 거래소

- 몰타에서 새로운 거래소를 시작하면서 유럽에서 사업을 시작하게 됨
- 몰타 중심부의 분주한 상업 중심지인 세인트 줄리안에 사무소를 열 예정
- 처음에 암호화폐-암호화폐 거래를 시작하여 결국 유럽 국가에 기반을 둔 새로운 플랫폼을 통해 신용화폐-암호화폐(거래 쌍)을 제공할 계획

"몰타는 DLT, 암호화폐, 핀테크에서 아마도 세계에서 가장 진보적이고 미래 지향적인 국가일 것입니다. 그리고 우리는 블록 체인 섬의 일부가 되는 것에 매우 흥분됩니다. 우리는 조만간 라이브 운영을 곧 발표할 수 있을 것으로 확신합니다.." --공동 창업자 지미 자오

- 가상통화는 '화폐'나 금융상품이 아니라는 점, 정부가 가치의 적정성을 보장하지 않는다는 점 재확인
- 법무부가 주관부처가 되어 추가 규제대책을 마련하겠다고 발표

15

지브롤터

ICO 친화적인 정책

간단한 법인설립 절차

- 주주나 이사의 국적 또는 거주지가 지브롤터에 없어도 괜찮으며 1명 이상이면 됨
- 법인설립을 위해 지브롤터를 직접 방문할 필요가 없음
- 법인 설립에 필요한 시간이 3~5일 정도이며 설립 비용이 비싸지 않음
- 부가세, 양도소득세, 금융소득에 관한 세금, 비거주자 배당에 대한 세금 없으며 지브롤터 내에서 이뤄진 영업에서 발생한 이익이라면 법인세(세율: 10%)를 부과하고 지브롤터 외에서 생긴 이익이 과세대상이 아님

"우리는 규제 당국으로서 어떤 토큰이 좋은 토큰인지 정하고 싶지 않다. 우리는 공인 스폰서들 중심의 자유 시장이 그것을 정할 수 있게 정책을 추진하고 있다. 블록체인과 분산원장 기술은 오랫동안 이용될 기술이라고 한다. 이 기술은 기업/소비자 관계와 정부-시민 간 존재하는 신뢰 관계의 의미를 근본적으로 바꿀 수 있다고 기대한다." -지브롤터 금융당국의 Sian Jones 지문위원

16

I. 각국 블록체인 산업 관련 규제 최신 동향

북미 블록체인 산업 관련 규제

17

미국

새롭고 중앙화된 증권 규제

- SEC는 토큰이 증권일 경우 증권법에 따른 규제를 받아야 하며, 기존 모든 토큰은 증권일 가능성이 있으니 면밀한 주의 당부
- 증권이 아닐 경우에는 별다른 규제 없으며, 암호화폐 거래소도 상장시 토큰이 증권이 아니라는 로펌 의견서 요구

암호화폐 & 거래
- 50개 주가 모두 각자의 규정을 만들 수 있음(예, **BitLicense**)
- SEC는 증권형 토큰의 정의 및 ICO 에 대한 관할권을 보유
- **FinCEN** - 모든 거래소가 등록해야 함

ICO
- 엄격한 SEC 규정으로 인해 ICO를 발행하는 회사들이 미국 내 참가자들에게로부터 자본 모집을 하지 못함
- 증권의정의의 범위가 매우 넓음(예, 투자계약증권 - **Howey** Test)
- 최근 적격투자자(연소득20만불이상)로 참가자를 한정하는 사례 **有**

시사점
- 증권형 토큰 ICO(STGE)도 등장
- 센트라코인 등 사회적 피해가 큰 토큰에 대해서는 SEC, USAO 등이 적극적 법적용

18

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets

- ICO를 진행할 때는 미국 연방 증권법이 적용되는지 확인하여야 함.
- ICO를 진행하는 코인이 미국 연방 증권법상 "증권"(Security)의 정의에 부합하면 미국 연방 증권법이 적용됨.
- 증권의 개념에는 주식, 채권뿐만 아니라 "투자계약증권"(Investment contract)도 포함됨.
- 디지털 자산이 증권에 해당하면 증권을 제공하거나 판매할 때 SEC에 등록하여야 함.
- **이 SEC 가이드는 디지털 자산이 투자계약증권인지 여부, 그리고 디지털 자산에 대한 제공이나 판매가 증권거래인지 여부를 판단하는 기준을 제공하는 것임.**
- **투자계약증권 해당여부를 판단할 때 Howey Test를 기준으로 삼는 것은 기존의 미국 연방 대법원 입장과 같으나, 그 구체적인 기준들을 제시하였다는 데에 의미가 있음.**
- 기존의 미국 SEC의 입장에서 크게 진보한 것은 아님.

19

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets

- **원문 URL :** https://www.sec.gov/files/dlt-framework.pdf
- **투자계약 증권 해당여부 판단 기준 : Howey test**
  - **투자계약 증권 : 타인의 노력으로부터 발생하는 이익을 합리적으로 기대하면서 공동의 사업에 금전을 투자할 때 투자계약이 존재함.**
  - **1. 금전의 투자(The Investment of Money)**
    - 디지털 자산을 현실 통화나 다른 디지털 자산 등을 통해 구매하면 이 요건이 충족됨.
    - 대부분 디지털 자산의 경우 이 요건을 충족함.
  - **2. 공동의 사업(Common Enterprise)**
    - 법원은 공동의 사업 요건은 투자계약의 특유한 요건으로 분석하고 있음.
    - 대부분 디지털 자산에서 공동의 사업 요건도 충족함.

20

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets (2)

- **투자계약 증권 해당여부 판단 기준 : Howey test**
  - **3. 타인의 노력으로부터 발생하는 이익에 대한 합리적인 기대(Reasonable Expectation of Profits Derived from Efforts of Others)**
    - 구매자가 타인의 노력으로부터 발생할 이익(또는 다른 금전적인 보상)에 대한 합리적인 기대가 있었는지 여부로, 보통 Howey test에서 가장 중요한 부분임.
    - 홍보자나 스폰서나 제3자들이 사업 성공에 필요한 경영적 노력을 제공할 때 투자자들은 이익에 대한 합리적인 기대를 하게 되고, 이 조건이 충족됨.
    - 이 요건 충족여부를 판단할 때에는 거래시 경제적 현실이 어떠한지, 어떠한 경제적 유인이 고객에게 전달되는지 등을 고려함.
    - 즉 이 요건은 거래 자체와 디지털 자산이 어떻게 제공되고 판매되는지에 관련된 것임.

21

미국

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets (3)

- **타인의 노력으로부터 발생하는 이익에 대한 합리적인 기대(Reasonable Expectation of Profits Derived from Efforts of Others)가 있었는지 판단하는 구체적 기준**
  - **1. Reliance on the Efforts of Others**
    - 구매자가 합리적으로 타인의 노력에 의지할 것을 기대할 수 있었는지 여부를 고려함
      - 디지털 자산의 네트워크 완성을 위해 타인의 노력이 필수적인 경우, 그 타인이 디지털 자산과 네트워크의 가치증대를 위해 노력할 것을 기대할 수 있는 경우 등을 고려하여 판단
    - 그 노력이 사업 성패에 영향을 미칠만한 부인할 수 없는 중요한 필수적인 경영 노력인지 여부를 고려함.
  - **2. Reasonable Expectation of Profits**
    - 이익은 초기 투자나 사업 개발로부터 자본 이득이나 구매자의 자금의 사용의 결과로 얻어지는 이익에 대한 참여가 포함됨.
    - 전적으로 수요와 공급에 영향을 주는 시장 외부적 요인에 의한 가격상승은 포함되지 않음.

22

2019. 4. SEC의 ICO 가이드라인 발표

Framework for "Investment Contract" Analysis of Digital Assets (4)

- **타인의 노력으로부터 발생하는 이익에 대한 합리적인 기대(Reasonable Expectation of Profits Derived from Efforts of Others)가 있었는지 판단하는 구체적 기준**
  - **2. Reasonable Expectation of Profits**
    - 이익은 초기 투자나 사업 개발로부터 자본 이득이나 구매자의 자금의 사용의 결과로 얻어지는 이익에 대한 참여가 포함되며, 전적으로 수요와 공급에 영향을 주는 시장 외부적 요인에 의한 가격상승은 Profit에 대한 기대에 포함되지 않음.
    - ①디지털 자산이 소유자에게 회사의 수입이나 이익을 나눌 권리를 주거나 디지털 자산의 가격상승으로 인한 이익을 현실화할 기회를 주는 경우, ②디지털 자산이 이동 가능하고 플랫폼이나 2차 시장에서 거래 가능하거나 장래에 그럴 것으로 기대되는 경우, ③그 타인들이 네트워크나 디지털자산의 가치를 증대시키기 위해 지속적으로 돈을 쓰는 경우 등에 해당하면 Reasonable Expectation of Profits가 있는 것으로 해석될 가능성 높음.

23

미국

TKJ 토큰에 대한 '비규제 조치 의견서'(No-Action Letter) 발행

- 원문 URL : https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm
- SEC는 항공 서비스업체 TurnKey Jet가 ICO를 통해 발행한 TKJ 토큰에 관하여 '비규제 조치의견서'(No-Action Letter)를 발행함
- TKJ는 '비규제 조치 의견서'를 받기까지 SEC 담당자와 50회 가량 통화하는 등 노력을 기울임
- 비규제 조치 의견서를 발행한 것은 규제의 명확성 측면에서 바람직한 일임

24

캐나다

암호화폐 규제 법률 초안 발표

암호화폐 & 거래

- 캐나다 정부가 지난 2015년~2016년 자금세탁방지국제기구를 통해서 자금세탁 및 금융테러방지관리라는이름으로 암호화폐 산업에 대한 조사 시행
- 2년 간의 조사 결과를 바탕으로 2018년 6월 초 암호화폐 거래소 및 암호화폐 결제 처리업체를 현금 서비스 사업체로 규정하고, 이들로부터 철저한 보고 체계를 갖추는 법률 초안 발표
- 업체들은 미화 약 1만 달러(한화 1073만원)를 초과하는 거래는 당국에 보고해야 하며, KYC로 고객에게 미화 약 770달러(한화 82만원)의 초기 금액 증명을 요구해야 함
- 비용편익분석을 하기 위해서 정부가 향후 10년 동안 약 4700만 달러(한화 504억원)를 투자할 계획

25

I. 각국 블록체인 산업 관련 규제 최신 동향

유럽 블록체인 산업 관련 규제

영국, 스위스, 독일, 프랑스, 리투아니아, 우즈베키스탄, 에스토니아

26

영국

글로벌 금융 혁신 네트워크GFIN 창설

암호화폐 파생 상품에 대한 거래 및 자문이 EU가 발표한 금융 정책에서 언급된 금융도구 지침 시장 II(MiFID 2)에 속함.

암호화폐 파생상품은 거래 허가를 받아야 한다고 함.

--영국 금융업무 행위감독기관(FCA, Financial Conduct Authority)

GFIN(Global Financial Innovation Network 글로벌 금융혁신 네트워크) 8월 창설됐음

- FCA가 주도해 11개국 금융규제기관들이 협력해 만든 단체
- 각국 금융 당국과의 밀접한 의사소통 지원 목표
- 블록체인의 분산 원장 기술 및 인공지능 증권 ICO 자금세탁방지 등 글로벌 협력이 필요한 분야에서 가시적 성과를 낼 예정
- FCA를 비롯해 프랑스금융감독기관, 아부다비글로벌마켓,미국 소비자금융보호국, 두바이 금융서비스국, 건지금융서비스국, 홍콩 통화 당국, 싱가포로 통화당국, 캐나다 온타리오증권위원회 등 총 11개국이 회원으로 등록했음
- GFIN 회원국 중 싱가포르통화청(MAS), 홍콩통화 당국(HKMA), 아부다비글로벌마켓(ADGM) 등 일부 국가들은 DLT 기반으로 구축된 해외 송금 결제가 운영되고 있음

27

스위스

ICO 생태계 구축 집중

- 증권형 토큰이 아니면 특별한 규제를 하지 않는 태도
- 비영리법인을 통한 ICO를 허용해 많은 ICO프로젝트가 집중됨(기부 방식으로 모금 가능하므로)

암호화폐 & 거래

- 암호화폐 비즈니스를 위한 특별한 라이선스가 필요하지 않음
- 스위스 자금 세탁방지법 (Swiss Anti-Money Laundering Act)에 따른 호의적인 대우

ICO

- 스위스 금융 시장 감독 관리 당국 (Swiss Financial Market Supervisory Authority, FINMA)이 새로운 ICO를 검토하여 허가
- AML 및 증권 규정에 집중
- 규정은 토큰의 기능 (지불형, 유틸리티형 또는 자산형/증권형 토큰)에 따르며 증권형이 아닌한 허용적 태도

시사점

- 크립토밸리로 잘 알려진 Zug/ Zurich
- 많은 ICO 프로젝트들 (특히 EU와 아시아 기반 프로젝트)이 선호하는 나라

28

독일

암호화폐 과세 가이드라인 공개

2018년 2월 27일 독일 연방 당국은 유럽사법재반소가 지난 2015년 내린 결정문을 바탕으로 암호화폐 과세 가이드라인을 공개했음

- 독일연방재무부는 독일에서 비트코인 등 암호화폐로 서비스나 물건을 사서 결제하는 경우 암호화폐를 법적인 결제 수단으로 인정했음
- 암호화폐가 결제 수단으로 쓰는 경우 별도의 과세 대상이 되지 않음
- 결제 서비스를 제공하는 지갑업체 등이 결제 수수료를 받게 된 경우 과세 대상이 됨
- 채굴을 자발적으로 행해지는 서비스로 규정하므로 암호화폐 채굴자가 블록은 생성한 보상으로 받은 암호화폐가 면세대상이 됨

29

독일

암호화폐의 영향력에 대한 정부의 입장

- 암호 토큰이 돈의 세가지 기능을 구비하지 않으므로 통화가 아니라 암호 토큰으로 여긴다.
- 암호 토큰은 일상 생활, 가치 저장고 또는 단위에서 지불 수단으로 사용되지 않는 다고 보았다.
- 암호화폐를 금융 안정성을 위협하는 것으로 보지 않지만 암호 토큰의 높은 성장률로 인해서 이 분야의 발전을 모니터 할 계획이다. 이를 통해서 향후 비트코인 선물 계약 등 제도권 상품 거래가 확립될 경우 엄격한 개입을 예고했다.
- 암호 화폐 거래 시장은 아직 규모가 작기 때문에 가격 변동성이 높고 시가총액이 급증했지만 암호화폐가 국가의 재정적 안보에 위협이 되지 않는다.

--독일 재무안정위원회(Financial Stability Committee)

암호화폐 거래 규모가 매우 작기 때문에 암호화폐가 글로벌 금융시스템에서 중요한 역할을 하지 않는다.

--독일 연방정부 대표

30

프랑스

암호화폐 정책 방향 급선회 중

암호화폐 강력 규제 → 블록체인과 암호화폐 선도주자

7월 4일 프랑스 암호화폐 규제 TF는 재정부에 제출한 보고서를 통해서 암호화폐 중요성을 강조했다

블록체인은 스타트업(창업초기기업)에게 새로운 기회를 제공할 것이다. 스타트업은 암호화폐공개(ICO)를 통해 토큰(암호화폐)을 발행함으로써 자금조달을 할 수 있다.

블록체인 혁명은 중개자 없이 '신뢰의 네트워크'를 구축해 우리 경제를 더욱 효율적으로 만들 것이다.

프랑스는 블록체인 혁명을 놓치지 않겠다. 지난해 12월 금융증권 전송에 블록체인기술 활용을 허용한 바 있다. 여기서 멈추지 않고 암호화폐 영역에서도 앞서나갈 것이다.

31

프랑스

ICO 신규 법안 정부 승인 : PACTE 법안 제26조

ICO 법안의 목적

프랑스 시장에서 ICO를 통해서 자금을 모집하고자 하는 회사가 프랑스의 관련 규칙을 준수하고 시장을 남용하지 않고 투자자를 보호해 줄 수 있으면 AMF에서 이런 회사에게 ICO를 발행할 수 있게 하는 허가를 발급함

토큰의 정의

any intangible asset representing, in a digital form, one or more rights, that can be issued, registered, kept or transferred using a shared electronic registration device through which it is possible to identify, either directly or indirectly, the owner of said asset

ICO의 법적 프레임워크가 될 법안이 프랑스 의회 소관 상임위원회에서 통과됐다
이 법은 세계의 블록체인 혁신가들을 끌어들일 수 있을 것이다
-프랑스의 브루노 르메리 재무장관

32

프랑스

ICO 신규 법안 정부 승인 : PACTE 법안 제26조

허가를 받을 수 있는 조건

- 토큰의 pre-sale단계 진행 전 미리 발급받아야 하지만 private sale단계 진행 후 발급받아도 됨
- 발행인의 의무 아니라 자원해서 신청하는 방식 도입 구체적인 조건은 곧 발표할 RGAMF에 포함시킴
- AMF는 백서의 내용과 정보를 리뷰하며 발행인의 다른 교류 문건과 담보를 주는 지원 문건을 모두 리뷰함

발행인의 의무

- 발행인은 프랑스에서 설립된 법인이어야 함며 조달한 자금을 감독하고 보장하는 에스크로 계좌 같은 메커니즘을 구축해야 함
- 백서에 대중에게 발행과 발행인의 정보를 포함한 유용한 정보를 포함해야 함. ICO에 대한 정보, 문건과 홍보에 관한 소통은 정확하고, 명확하고, 오도하는 의도가 없어야 함. 또한 발행의 리스크도 포함시켜야 함.

33

프랑스

ICO 신규 법안 정부 승인 : PACTE 법안 제26조

AMF의 권한

- AMF는 허가를 발급받은 토큰의 발행인에게 화이트 리스를 발급할 것임.
- AMF는 일반적 규정에 따라 새로운 구매나 발행을 정지시킬 수 있으며 발행에 관한 모든 홍보에 대한 소통을 중지시킬 수 있음.
  하지만 이런 권한은 이미 허가를 받은 발행인에 한하며 외국인 발행인에 적용하지 않음

비주

- 허가를 받지 않은 ICO는 금지되지 않을것임.
- 하지만 허가를 가지면 발행인은 자금 모집의 사용에 대해서 투자자에게 특정의 담보를 제공해야 함을 뜻함

34

우즈베키스탄

디지털 경제 도약

- 샤브카트 미르지요예프 대통령이 **7월 3일** 블록체인 기술 촉진을 위한 대통령인 **"On measures for the development of the digital economy in the Republic of Uzbekistan "** 을 선포했음
- 블록체인 기술, 디지털자산, 암호화폐 채굴 산업을 육성하며 신기술을 통해 국가 행정 시스템을 재정비하려는 목적
- 블록체인, 인공지능, 암호화폐 그리고 슈퍼컴퓨터 분야를 핵심 기술로 지정하고 지원할 것이라고 밝혔음

Shavkat Mirziyoyev
대통령

법인과 자연인이 암호화 자산의 유통과 관련된 거래에서 얻은 수익에 대해 세금을 징수하지 않음

암호화 자산의 유통에 관한 활동에 대해 허가제도를 시행함.
새로운 거래 플랫폼은 **10월 1일**부터 허가증을 발급하며 허가증의 발급을 감독 관리 해주는 당국은 대통령이 관리하는 국가 프로젝트 관리 기관일 것임.

35

리투아니아

ICO 가이드라인(2018. 6. 6.)

1. 적용 법률

- **토큰을 가지는 자에게 경영권이나 이윤을 부여하지 않는 경우**

(예로, 토큰을 가지면 어떤 제품을 사용하거나 어떤 서비스를 받을 수 있는 권리만 부여함)

--민법, 돈세탁방지법, 반테너주의융자법

- **토큰을 가지는 자에게 경영권이나 이윤을 부여한 경우**

--증권형 토큰인 경우: 증권법
--크라우드 펀딩형 토큰인 경우: 크라우드펀딩법
--토큰의 2급 시장에 참여하거나 구축하는 실체, 금융 도구의 특징을 가지는 ICO인 경우: 금융도구시장법
--ICO를 통해서 자금을 모집하고 모집한 자금을 다른 프로젝트에 투입한 실체인 경우: 집합투자주체법, 내부투자자에대한집합투자기관법 , 전문투자자에대한집합투자기관법

36

ICO 가이드라인(2018. 6. 6.)

2. 세금 문제

암호화폐의 거래의 성질과 경제적 의미에 따라 암호화폐에 관한 세종도 다름

기업소득세

- 암호화폐가 화물이나 서비스에 대한 결제도구라고 해서 유동 자산으로 간주하므로 기업소득세를 납부해야 함. 하지만 아래 경우에는 ICO를 통해서 모집한 자금은 기업소득세의 목표가 아님:

--발행한 토큰은 민법전 제1.101조부터 제1.108조까지에 나와있는 증권의 정의에 부합한 경우
--발행한 토큰의 소유자가 어떤 제품을 사용하거나 어떤 서비스를 받는 권리만 가진 경우, 이때는 모집한 자금은 선금으로 여기며 이런 토큰을 발행하는 것은 수익에 대한 확인 아니라 현금의 이전으로 여김. 구체적인 수익은 시장에서 제품을 판매하거나 서비스를 제공할 때 확인 받을 예정.

37

리투아니아

ICO 가이드라인(2018. 6. 6.)

개인소득세

- 개인이 암호화폐 거래로부터 수익을 얻은 경우 이런 거래 활동이 연속성, 자원성, 경제 이익 추구성 등 3개의 조건을 부합하면 이런 수익에 대해서 15%의 개인소득세를 납부해야 함
- 이 이외, ICO의 창업팀에게 배당한 토큰은 활성화되지 않거나 locked된 경우 만약 창업팀이 이런 토큰을 위해서 결제를 해본적 없으면 이런 토큰이 판매되기전 창업팀은 개인소득세를 납부할 의무가 없음

부가가치세

- 제품을 제공하거나 서비스를 제공하기 위해서 토큰을 발행한 것 아인 경우 부가가치세를 납부할 의무가 없음
- 채굴을 통해서 암호화폐를 얻은 경우 만약 암호화폐를 취득하는 것이 제품이나 서비스를 대가로 하지 않으면 채굴 행위 그 자체가 부가가치세 규칙에 적용되지 않음. 하지만 만약 채굴자가 다른 사람을 위해서 채굴 서비스를 제공하며 부가가치세에 있어서 이런 서비스가 리투아니아 내 제공받은 서비스로 여기면 이런 채굴 서비스에 대해서 부가가치세를 납부해야 함
- 채굴을 통해서 얻은 암호화폐를 판매하면 부가가치세와 연관성이 있다고 함. 하지만 지금 리투아니아에서 암호화폐를 판매할 때 부가가치세 면제를 받을 수 있는 규정이 있음

38

리투아니아

ICO 가이드라인(2018. 6. 6.)

3. 회계 기준

- 토큰에 대한 회계 준칙은 회계 부문이 제정함.
- 토큰에 대한 회계기장은 토큰이 결제형 토큰, 공용사업용 토큰, 증권형 토큰에 속하냐에 따라 다름

4. AML

- 지금 1차 수정안을 제정하고 있음
- 감독 관리의 투명성과 금융 시장의 안정성과 안전성을 제고하기 위해서 1차 수정안을 제정할 때 암호화폐 거래소와 지갑 서비스 제공자에 대한 규정을 집중적으로 제정할 계획임

39

에스토니아

새로운 암호화폐 친화적 나라

법인 설립 절차 간편화:
전자시민권(E-Residency)을 가지지 않은 외국인도 쉽게 법인을 만들 수 있음
직접 현지 방문을 한 해도 법인 설립 가능함
법인 설립 절차 간단하고 비용이 저렴함: 현지인 이사가 필요하지 않고 주주에 대한 신원확인절차가 복잡하지 않으며 변호사 비용이 낮음.

ICO 가이드라인 있는가? 없음.
다만 단순한 유틸리티 토큰만 발행이 간편하지만 다른 토큰인 경우 다른 나라와 마찬가지로 엄격한 법적 절차를 거쳐야 함.
에스토니아의 증권시장법(Securities Market Act)은 증권의 범위를 정해 놓지 않았지만, 다른 나라처럼 자주 미국 SEC가 적용하는 Howey Test를 인용해 증권 여부를 판단하는 것임. 그래서 순수한 유틸리티 토큰이 아니면 증권에 해당될 가능성이 높을 수 있음.

40

에스토니아

새로운 암호화폐 친화적 나라

암호화폐거래소를 운영하려면 라이선스가 필요한가?
라이선스 1: Provider of a virtual currency against a fiat currency exchange service
라이선스 2: Provider of a virtual currency wallet service

암호화폐 관련 규제:
EU에 속해 있는 에스토니아는 EU의 금융 규제도 적용해야 함.
EU의 암호화폐에 대한 금융 규제가 강화되면서 에스토니아 은행도 암호화폐를 취급하는 업체들의 은행 계좌 개설이나 이용을 엄격하게 제한하기 시작했음.
사업 내용에 대한 심사도 까다로워졌고 현지에 직접 가서 개인 인증을 받아야 할 수도 있음.

암호화폐 관련 세금 정책
이윤세를 적용하지 않고 비트코인과 알트코인인 경우 부가가치세를 낼 필요가 없음.

41

I. 각국 블록체인 산업 관련 규제 최신 동향

아시아 블록체인 산업 관련 규제

일본, 캄보디아, 태국, 중국
싱가포르, 인도, 필리핀,
중국 홍콩

42

일본

투자자 보호와 투명성을 높이기 위해 입법조치

암호화폐 & 거래

- 2016년 자금결제법 개정으로 암호화폐 거래소 등록제 시행
- 거래소 자체 정책 규정에 따라 투자자 보호와 투명성을 높이며 내부 거래 및 보안문제 해결 노력
- 산업 혁신을 위해 기존의 상대적으로 약했던 규제에서 코인체크(거래소) 해킹 사태 이후 강한 규제를 시행
- 투자자 보호를 위해 방대한 규제조치가 제안되었고 암호화폐 거래가 금융상품 거래만큼 엄격한 규정을 적용 받고 있음.
- 새롭게 출시 되는 코인 관계자들이 정보를 활용하여 이익을 얻지 못하도록 내부자 거래 금지조항이 포함됨
- 돈세탁, 마약 밀매 및 기타 악용 우려가 있는 Monero, Augur, Dash, Zcash와 같은 코인의 거래 금지.
- 해킹의 위험을 최소화하기 위해 거래소 감사결과를 JVCEA에 제출, 개인 키는 cold storage에 오프라인으로 저장.
- 디지털 자산이 급등하거나 급감할 경우를 대비해 차단조치 의무적 도입.

43

캄보디아

기본적으로 암호화폐에 대한 부정적 입장

암호화폐 & 거래

- 이전부터 암호화폐에 대해 부정적인 입장(예: 14년- 비트코인을 화폐로 인정하지 않음, 17년 12월 - 자국 내 금융 기관의 암호화폐 거래, 홍보 및 관련 계좌 개설 금지)
- 암호화폐가 가격 변동성, 사이버 범죄, 소비자 보호책 미비에 따른 투자 리스크를 일으킬 수 있으므로 관할 당국의 라이선스를 받지 않은 상태에서 암호화폐를 홍보, 유통, 매입, 매각, 거래, 청산하는 행위는 불법화
- 몇가지 특정 코인(OneCoin,KH Coin,Suncoin)을 잠재적 위험요소로 지목
- 구체적으로 어떤 라이선스가 필요한지, 또 라이선스 발급을 위해 어떤 조건이 필요한지는 밝혀진 바가 없음
- 국가발행 디지털 화폐에 대해서는 포용적인 입장

44

중국

날로 심해지는 중국의 암호화폐 규제

8월 28일 중국핀테크고발정보플랫폼(中国互联网金融举报信息平台)에서 "핀테크고발범위"에 토큰발행자모집(ICO)"에 관한 활동을 추가

- 법정화폐와 토큰, 암호화폐 간의 환전 업무
- 토큰이나 암호화폐를 매매하거나 사고파는 행위
- 토큰이나 암호화폐를 위해서 정가라 정보 중개 등 서비스를 제공하는 행위
- ICO나 암호화폐를 위해서 계좌 개설, 등기, 거래, 청산, 결산 등 서비스를 제공하는 행위
- 토큰이나 암호화폐와 관련된 보험을 맡거나 토큰이나 암호화폐를 보험 책임 범위에 포함시키는 행위
- 토큰이란 명칭을 사용하여 전개하는 불법 금융 활동

중국 핀테크 고발 정보 플랫폼이란?

- 2016년 10월 중국핀테크협회에서 만든 플랫폼
- 공중은 이 플랫폼이나 중국핀테크협회의 위챗 플랫폼을 통해서 개인이나 단체의 명의로 핀테크 업체의 위법 행위에 대해서 고발할 수 있음
- 플랫폼은 핀테크의 여러 세분화된 분야에 따라서 고발 범위를 열거함

45

중국

중국 중앙은행 블록체인 사기 경고령 발표

경고령의 요점 :

1. **최근 금융 혁신이나 블록체인이라는 명목을 걸고 소위 암호화폐, 암호재산이나 디지털재산 등 방식으로 자금을 흡수하여 공중의 합법적 권익을 침해하는 불법 행위자들이 있음. 블록체인을 명목으로 하지만 실제로는 불법 자금 모집, 다단계 마케팅, 사기임.**

2. **어떤 불법 행위자가 ICO, IFO, IEO 등 명목으로 토큰을 발행하거나 공유경제의 명목으로 IMO의 방식으로 암호화폐 투기.**

3. **공중들은 블록체인에 대해 이성적으로 대해야 하며 절대 번지르한 빈말을 믿어서는 안 됨.**

中国银行保险监督管理委员会

关于防范以"虚拟货币""区块链"名义
进行非法集资的风险提示

银保监会、中央网信办、公安部、人民银行、市场监管总局提示：

近期，一些不法分子打着"金融创新""区块链"的旗号，通过发行所谓"虚拟货币""虚拟资产""数字资产"等方式吸收资金，侵害公众合法权益。此类活动并非真正基于区块链技术，而是炒作区块链概念行非法集资、传销、诈骗之实，主要有以下特征：

一、网络化、跨境化明显。依托互联网、聊天工具进行交易，利用网上支付工具收支资金，风险波及范围广，扩散速度快。一些不法分子通过租用境外服务器搭建网站，实质面向境内居民开展活动，并远程控制实施违法活动，一些个人在聊天工具群组中声称获得了境外优质区块链项目投资额度，可以代为投资，极可能是诈骗活动。这些不法活动资金多流向境外，监管和追踪难度很大。

二、欺骗性、诱惑性、隐蔽性较强。利用热点概念进行炒作，编

46

중국

중국 법정디지털화폐(CBDC) 연구 적극적으로 추진

중국
CBDC(Central Bank Digital Currency)
출시 예정

What?	센터화된 기구인 중국 중앙은행에서 발행된 블록체인을 기반으로 한 법정디지털화폐
What?	프로그램 가능, 프라이버시 보호 강화 가능, 화폐 유통에 대한 추적 가능, 실물 경제와 더욱 기밀하게 결합할 수 있기 때문임
What?	납세, 법률, 서비스 시설 등 상응하는 변화가 있을 예측

47

중국

중국 법정디지털화폐(CBDC) 연구 적극적으로 추진

- **2017년 10월** 중앙은행이 발행하는 법정 디지털화폐 디지털어음거래플랫폼에서 시범 운영 시작
- **2017년 32개** 특허 공개됐으며 **2018년 14개** 특허 공개됐음.
- 특허는 주로 디지털 화폐의 개통 방법과 시스템, 디지털 지갑의 로그인 방법, 단말기, 시스템, 디지털 화폐 지갑을 바탕으로 관련 계좌를 조회하는 방법 등을 포함한 디지털 지갑 분야에 집중하고 있음
- 중국중앙은행 **8월** 말 개최한 전국 회의에서 중국 중앙은행 은행장이 중앙은행 디지털 화폐의 연구와 개발을 확실히 추진했다고 밝혔음
- 중국 중앙은행 **3년**전부터 디지털 화폐에 대한 검토회를 개최했고 그 추 바로 중앙은행 산하 디지털 화폐 연구소를 구축했음. 지금 민간 시장과 공동으로 디지털 화폐를 연구하고 있음.
- 중국 중앙은행은 **8월** 쯤 개최한 **ITU** 법정 디지털 화폐 회의에서 백서를 발표했음

ITU법정디지털화폐초점회의는 세계 주요 나라 중앙 은행 간 법정 디지털화폐를 검토하는 유일한 플랫폼입니다.

48

홍콩

다른 나라에 비해 규모는 작지만 비트코인에 대한 열기가 높은 곳 중 하나

암호화폐 & 거래	➢ 적극적인 규제의 부재가 암호화폐 산업의 성장을 가로막고 있음 ➢ 투자자 보호를 위해 홍콩 증권선물위원회(SFC)는 암호화폐와 ICO 관련 산업을 주시하고 있으며 필요에 따라 개입한다는 입장 ➢ 암호화폐 거래소 개설에 라이선스를 받아야 함
ICO	➢ 투자자 보호를 위해 관련 산업을 주시하고 필요에 따라 개입한다는 입장
시사점	➢ 홍콩 SFC가 암호화폐와 블록체인 교육을 추진하고 있으며 투자자 교육 기관과 협력하여 새로운 기술과 투자위험성에 대한 대중의 인식을 개선해 나가는 중

49

태국

암호화폐 & 거래

- 7개의 암호화폐 합법화와 규제안 세부 사항 공개
- 태국증권거래위원회(SEC)에 암호화폐 규정 위임, 암호화폐에 대해 국가의 과세 공고를 따르도록 함
- 규제 범위에는 ICO, 암호화폐 거래소, 중개 회사, 거래자 및 재무부가 허용한 기타 당사자 포함
- SEC는 ICO에 사용되는 7개의 암호화폐(BTC, ETH, LTC, BCH, ETC, XRP, XLM) 거래를 합법화

ICO

- 디지털 자산 거래와 관련된 ICO 발행자, 거래소, 중개인 및 딜러를 포함한 모든 참여자는 발효일로부터 90일 이내에 SEC에 등록을 해야 하며 태국정부의 승인을 받아야 함
- SEC의 승인을 받기 위해 토큰 발행인은 발행되는 토큰의 유형과 투자 정보를 명확하게 명시해야 함
- ICO 포털은 500만 바트의 자본을 등록해야하며 1년동안 ICO 제공을 돌봐야 함
- 태국 법인만 승인신청을 할 수 있음
- 기관 및 초고가치 투자자에게 제공할 수 있는 ICO 금액에는 제한이 없지만 개인투자자에게는 ICO 프로젝트 당 30만 바트 또는 제시된 토큰 총 가치의 70%를 초과해 투자할 수 없음
- 토큰 배포와 암호화폐 운영을 위해 각각 250만 바트씩 총 500만 바트의 선불금이 있으며 중개회사와 디지털 자산 거래자에게는 250만 바트와 200만 바트임
- 승인되지 않은 디지털 토큰을 판매하는 업체와 암호화폐 투자를 유도하기 위해 승인되지 않은 세미나를 개최하면 거래 가치의 두배 또는 50만 바트 이하의 벌금과 최대 2년의 징역형을 선고 가능

50

인도

법률 개혁 위원회, 암호 화폐 유효한 지불 수단 인정

도박 거래는 현금을 제외한 신용카드, 지불카드, 온라인 은행, 암호화폐 등과 같은 전자적인 결제 수단을 이용해야 합니다.

-Legal Framework: Gambling and Sports Betting Including in Cricket in India

정부가 임명한 단체가 암호화폐에 가치를 부여하고 거래에 사용할 수 있는 권한을 부여한 것은 이번이 처음이다.

-인도의 암호화폐 거래소 WazirX의 창립자 겸 CEO인 Nischal Shetty

인도의 법률 개혁 위원회: 스포츠 도박의 타당성을 연구해 온 기관

51

필리핀

경제특구, 암호화폐 거래소 라이선스 최대 25곳 발행

카가얀 경제특구(CEZA):

암호화폐 거래소를 최대 25개까지 승인 및 수용할 계획 발표

요구:

- **거래소는 운영 2년 내 최소 100만 달러를 특구에 투자해야 함.**
- **실제 특구에 물리적 실재가 있어야 함.**
- **각 거래소는 브로커, 거래업체를 위한 20~30개의 하위 라이선스를 가지게 됨**
- **필리핀 중앙은행이 거래소 설립 의사를 밝힌 10여 개 운영업체의 신청서를 검토하고 있음.**

카가얀 경제특구가 스캠 범죄자의 소굴이 되지 않기를 바라며 정직성과 진실성 검증을 통해 암호화폐 투자를 유인하는 거래인지 여부를 확인해야 합니다.
모든 ICO 운영업체가 코인을 발행할 때 자산 근거를 가지는 것을 의무화할 것입니다.

--CEZA의 Raul Lambino 수석

52

필리핀

증권거래위원회 ICO법안 제시(2018.8.2.)

필리핀 증권거래위원은 2018.8.2 ICO를 규제할 법안을 제시하며, 은행, 일반 투자자 밑 타 관련 기관들로부터 2018.8.31까지 본 법안에 대한 의견을 요청함. 본 법안은 아직 통과된 법령이 아니며, 준비단계 중 마무리 단계로 사료됨.

Initial Coin Offerings: 펀드레이징을 위해 유통되는 레져 기술로, 현금, 타 암호화폐 또는 자산을 거래할 시 토큰이 주어짐. ICO는 코인 또는 토큰을 발행함으로 투자금/자본을 대중으로부터 위치 함. 펀드레이징 프로젝트로 희망하는 자금이 모일 때, 투자자에게는 다음과 같은 혜택이 부여됨:

- 토큰 가치상승 및 판매로 인한 이익
- 경영 투표권 또는 기업 관리 규범 기여
- 이용 권리

Coin: 블록체인을 기반으로 거래에 사용되는 단위이며, 네트워크에 기여하는 사용자에게 인센티브로 지급됨.

Token: Smart contract로부터 생성된 가상화폐로, 거래수단 외 자산 또는 타 기능을 개발자에 따라 수행함

53

필리핀

증권거래위원회 ICO법안 제시(2018.8.2.)

주요사항

1. 본 법안은 전환용 증권형 토큰(convertible security token)을 개최 및 발행하는 필리핀 기업의 ICO또는 필리핀 시민을 타깃으로 하는 ICO 범위에서 적용 됨.
2. 제시된 법안은 두 갈래로 ICO를 평가하는 방안으로 (a) 초기 평가(initial assessment)와 (b) 공식 등록(registration proper)이 요구됨.
3. 필리핀에서 개최되거나 필리핀 스타트업 또는 기업이 실행하는 ICO는 기초 평가를 통과해야 하며, 이에 관련된 모든 문서 및 내용(백서 포함)을 제출해야 하며, 발행 토큰이 증권형이 아니란 것을 증명해야 함.
4. 필리핀 증권거래위원회는 모든 자료를 받은 후 20일간의 기간내로 본 토큰이 증권형인지 아닌지 판단해야 함.

- 증권거래위원회의 의견상 증권형 토큰으로 간주될 시, 발행기업은 토큰 발행 전 토큰을 증권형으로 등록해야 함 (법안에서 지정하는 제외항목은 면제됨).
- 향후 발행되는 코인이 증권과 상이할 경우가 있을 수 있으므로, 증권과 성격이 다른 ICO때 발급되는 증권형 토큰은 본 법안에 기재된 절차를 통해 등록돼야 함.

54

필리핀

증권거래위원회 ICO법안 제시(2018.8.2.)

주요사항

5. ICO를 개최하는 기업은 의무적으로 법인을 설립해야 하며, 외국기업의 경우 필리핀에 지사를 설립 및 보유해야 함.

6. 필리핀 증권거래위원회는 백서의 내용을 법안에 계시된 의무사항에 맞도록 수정하게 지시할 수 있는 권리가 부여됨 (예: ICO campaign timeline, 토큰의 가치/가격, 발행되는 토큰/코인을 구매하기 위해 거래 가능한 암호화폐/신용화폐 등).

7. ICO 발행 기업의 경영팀 및 자문팀 멤버들은 모두 본 법안에 기재된 자격조건을 보유해야 하며 실격사유 (본 법안을 위법하는 경우, 허위진술 할 경우 등)에 해당하는 조건이 없어야 함.

55

필리핀

증권거래위원회 ICO법안 제시(2018.8.2.)

주요사항

8.증권형 코인 발행자는 제출문서 중 코드 감사 보고서(code audit report)를 제3자를 통해 이행/발송해야 하며, 본 업무는 소스코드, 고객신분확인(Know Your Customer)/자금세탁방지(anti-money laundering) 체제, 기술적 위험요서 (technology risks) 및 보안 방침(security protocol)이 포함됨. 코드 감사는 또한 프로젝트 감시를 위해 본 법안에서 요구하는 타 제출문서와 함께 규칙적으로 이행 및 제출 되어야 함.

9.증권거래위원회 또는 협력기관은 증권형 토큰 등록절차 중 규칙적으로 필리핀에 소재한 발행인/발행기업의 사무실 또는 OS 시스템 검토회를 시각적으로 검사할 수 있는 권한이 부여됨.

10.본 법안은 허용 및 금지하는 홍보 방법을 정하고 있음 (허위광고 포함).

56

필리핀

증권거래위원회 ICO법안 제시(2018.8.2.)

주요사항

11.본법안의 효력 전 ICO를 개최한 기업은 발효시점으로부터 3개월 내에 기초평가 신청서를 제출 해야 함.

12.증권형 토큰 ICO를 개최하는 업체의 수익은 독립적인 명성의 제3자 예탁 에이전트에게 맡겨야 함. (keep the proceeds under escrow with a reputable independent escrow agent).

예탁동의서/계약서는 등록 명세서에 첨부된 증거자료의 일부로 제출되어야 하며,
(1) 본 수익금은 발행기업의 프로젝트 진행 보고서의 제시 시에만 인출될 수 있고, (2) 예탁 에이전트는 본 프로젝트가 1차 희망 수입(소프트 캡 (soft cap))에 도달하지 못했을 경우 또는 프로젝트가 완료되기 전에 발주자에 의해 포기된 경우, 비례 기준을 적용하여 투자자들에게 수익을 돌려줘야 함.

57

싱가포르

ICO 생태계 구축에 집중

- 증권형 토큰이 아닌 이상 당국의 허가 없이 ICO 가능

암호화폐 & 거래

- 전반적으로 유리한 규제
- 싱가포르 금융 감독청 (Monetary Authority of Singapore, MAS) 이2017년 11월에 지침을 발표했음
- 암호화폐를 관리 감독 하지 않지만 관련 활동을 감독 관리 할 것
- MAS는 암호화폐 거래 중개자가 (ICO 포함) 더욱 엄격한 법률실사와 AML 절차를 시행해야 한다고 함

ICO

- MAS는 ICO 산업을 계속해서 모니터링할 것
- AML 의무로 은행들이 영리법인의 ICO에는 사업자통장개설 거부, 비영리법인이 ICO하는 관행으로 정착
- 비영리법인에 2명 이상 직원, 그중 1명은 싱가폴인이어야 함

시사점

- ICO진흥을 통해 국부창출, 일자리창출(블록체인 개발자 양성)
- 크립토/블록체인 생태계를 선도하는 나라가 됨

58

I. 각국 블록체인 산업 관련 규제 최신 동향

각국 암호화폐에 대한 세무제도

59

미국과 캐나다

미국:

- 암호화폐는 자본 자산으로 사용 되므로 암호화폐 거래로 얻은 소득은 자본소득으로 간주하여 납세함
- 회사가 암호화폐의 형식으로 직원에게 월급을 줄 때도 납세 의무가 있음

캐나다:

- 캐나다의 세법이 디지털 화폐의 거래에 적용될 수 있음. 디지털 화폐를 사용하는 것이 소비자의 납세 의무를 면제한다는 것은 아님.
- 올해 4월 21일 캐나다 세무국이 디지털 화폐의 사용자에게 디지털 화폐를 판매하거나 교환하여 수익을 얻은 경우 플랫폼이 어디든 4월 30일까지 반드시 관련 세금을 내야 한다는 경고신을 보냈음.
- 미국과 마찬가지로 암호화폐의 거래로 얻은 소득은 자본소득으로 간주함.

60

일본과 대한민국

일본:

- 2017년 4월 1일 일본결제서비스법안의 수정안은 발효하면서 비트코인은 일본에서 합법적 결제 수단이 됐음.
- 2017년 7월 1일 새로운 소비세법이 발효했음. 이로써 8%의 비트코인소비세는 취소됐음. 하지만 투자자가 여전히 디지털 자산의 투자 이윤에 대해 신고를 해야 하며 주식 투자15%~55%의 세금을 내야 함.
- 일본 국세청은 2017년의 암호화폐 거래로 얻은 자본소득은 잡소득으로 여기며 20%의 세율에 따라 납세함.

한국:

- 암호화폐에 대한 명확한 납세 프레임 없지만 올해 1월부터 암호화폐거래소가 기존 세법에 따라 납세해야 함.
- 구체적으로는 암호화폐거래소가 22%의 기업소득세와 2.2%의 지방소득세를 내야함. 또한 암호화폐거래소가 중소기업에게 제공하는 세금 감면 정책을 누릴 수 없음.

61

태국과 이스라엘

태국:

- 2018년 3월 태국이 현지 암호화폐 거래 시장을 규범화하고 투자인의 소득에 대해 납세하기 위해서 2개의 법안을 발표했음.
- 자산 거래를 할 때 7%의 부가가치세를 납부해야 하며 자본소득과 투자 수익에 대한 원천징수 소득세 세율은 15%임.
- 5월 14일 태국 왕실이 암호화폐를 가지거나 거래해서 얻은 소득은 모두 15%의 자본소득세를 납부해야 한다고 밝혔음.

이스라엘:

- 암호화폐 자본소득세의 세율은 205~25%이며 개인적 마이닝이나 암호화폐에 대한 비즈니스를 한 경유 17%의 부가가치체를 납부해야 함.

62

러시아, 프랑스, 우크라이나

러시아:

- 암호화폐 거래인 경유 13%의 세율을 적용함. 지금 의회와 재정부가 관련 수정 작업을 하고 있으며 올해 말까지 수정안이 발효할 예정임.
- 새로운 세율이 나오기 전에 러시아 국민이 반드시 암호화폐 소득에 대해 정부에 신고해야 하며 이를 위해서 13%의 일반 소득세를 납부해야 함. 광부인 경우 개인창업자나 법인의 명의로 납세를 할 수 있음.

프랑스:

- 5월 1일부터 프랑스국가세무위원회에서 비트코인 등 암호화폐 소득에 대한 세율은 45%에서 19%까지 낮췄음.

우크라이나:

- 2019년부터 암호화폐의 매매차익금에 대해서 5%의 세금을 징수할 예정임. 개인 같은 경유도 매매차익금의 1.5%를 세금으로 납부해야 함.

63

폴란드, 남아프리카, 호주

폴란드:

- 암호화폐 거래에 대해서 1%의 경제세를 징수함.
- 암호화폐 소득은 소득세법을 적용해서 18%와 32%의 소득세를 징수함.

남아프리카:

- 2018년 7월 남아프리카세무국이 암호화폐세법 초안을 발표했음. 이에 따라 암호화폐를 무형 자산으로 여기므로 소득세를 납부해야 함.
- 암호화폐 거래가 서비스로 간주하므로 부가가치세와 연관성이 있지만 비과세금융서비스로 여기므로 암호화폐의 발행이나 거래 등에 관한 부가가치세가 면제됨.

호주:

- 암호화폐에 대해서 최초로 징수하는 나라의 하나이며 세무 정책도 계속해서 변하고 있음.
- 비트코인 같은 암호화폐는 호주에서 금전 아니라 자산으로 여기므로 자본소득세를 납부해야 함.

64

2018년 각국 암호화폐 규제 현황 일람표

나라	ICO 허용 여부	암호화폐 거래 허용 여부	암호화폐거래소 라이선스 유무	ICO 가이드라인 유무
싱가포르	O	O	O	O
스위스	O	O	O	O
중국	X	X	N/A	N/A
한국	X	O	X	X
미국	O	O	O	X
일본	O	O	O	X
영국	O	O	O	X
프랑스	O	O	X	O
몰타	O	O	X	X
루마니아	O	O	X	X

65

2018년 각국 암호화폐 규제 현황 일람표

나라	ICO 허용 여부	암호화폐 거래 허용 여부	암호화폐거래소 라이선스 유무	ICO 가이드라인 유무
우크라이나	O	O	X	X
캐나다	O	O	O	X
유럽연합	O	O	X	X
독일	O	O	O	O
호주	O	O	O	O
태국	O	O	O	O
브라질	O	O	X	X
러시아	O	O	X	O
베네수엘라	O	O	O	X
에스토니아	O	O	O	X

66

II. 정부규제 관련 현황과 전망

67

정부 규제 관련 현황

2017.9.4. 가상통화 대응방안(관계기관 합동)

- 가상통화는 '통화'도 '화폐 ' 도 '금융통화상품 ' 도 아니다는 입장
- 가상통화 취급업자 이용자 본인확인 등으로 거래투명성을 강화하겠다는 입장을 밝힘
- 가상통화 투자 등도 '유사수신행위'에 포함되도록 입법할 것임을 밝힘 **(입법필요사항 / 입법 안됨)**
- 증권형태로 ICO를 발행하는 것은 자본시장법 위반으로 처벌하겠다고 밝힘

2017.9.29. 가상통화 관계기관 합동 TF

- '모든 ICO를 금지'한다는 제목의 보도자료를 배포하였으나, 실상 ICO 금지 법안**(현재까지 입법 안됨)**을 입법추진하겠다는 것이었음
- 가상통화 투자 등도 '유사수신행위'에 포함되도록 입법할 것임을 재차 밝힘

2017.12.4. 가상통화 관계기관 합동 TF

- 가상통화는 '화폐'나 금융상품이 아니라는 점, 정부가 가치의 적정성을 보장하지 않는다는 점 재확인
- 법무부가 주관부처가 되어 추가 규제대책을 마련하겠다고 발표

68

정부 규제 관련 현황

2017.12.14 가상통화 관련 범죄 엄정대처 지시

- (법무부)다단계, 유사수신 형태의 투자금 모집, 채굴을 빙자한 투자사기, 가상통화 거래자금 환치기 등 외국환거래법 위반, 가상통화 이용 마약거래, 가상통화 이용 불법 자금 세탁, 가상통화 이용 범죄수익은닉, 거래소 해킹 등 관련 범죄 엄정 대처를 검찰에 지시

2017.12.28 가상통화 투기근절 위한 특별대책

- 가상계좌 대신 '실명확인 입출입계정 시스템'을 구축하여 활용 **(현재 시행됨)**
- 가상화폐 시세조종, 환치기 등 불법행위 유무 집중 점검하고 엄정 대처할 것임을 밝힘
- 법무부 건의대로 특별법 제정하여 가상화폐 거래소 폐쇄 방안을 검토할 것임을 밝힘

2018.1.12 법무부 장관, 가상화폐 거래소 폐쇄 방침을 밝힘 **(입법필요사항 / 입법 안됨)**

2018.1.15 가상통화 정부입장

- 12일 법무부장관이 언급한 거래소 폐쇄 방안은 범정부 차원에서 의견조율 중이라고 밝힘
- 가상통화는 법정통화가 아니며, 가치보장 주체가 없으므로 신중히 투자할 것을 당부
- 향후 국무조정실이 가상화폐 관련 부처입장을 조율할 것임을 밝힘

69

정부 규제 입장 정리

정부 발표 이슈	일시	분류	경과
가상화폐 이용 유사수신행위 처벌	2017.9.4	입법필요사항	입법 안됨
ICO 전면금지	2017.9.29	입법필요사항	입법 안됨
가상화폐 거래시 실명계좌 사용 의무화	2017.12.28	정부시행가능사항	시행됨
거래소 폐쇄를 위한 특별법 제정	2017.12.28	입법필요사항	입법 안됨
가상화폐 거래에 세금 부과	입장 없음	개인소득세 :입법필요 상속증여, 법인세 즉시 부과가능	입법 안됨

70

정부 규제 관련 전망

- **정부는 지난해 ICO를 전면 금지하겠다고 발표하고, 올 1월에는 암호화폐 거래소를 폐쇄하겠다는 입장을 밝힌 후 2018. 1. 이후 공식 입장 없음**
  - 최근(2018. 5.) 김동연 부총리는 지방선거(6.13.) 후 암호화폐에 대한 정부정책이 마련될 것이라고 언급
  - 2018.6. 26. 금융위원회, 가상통화 거래소 자금세탁방지 가이드라인 발표
    - 가상통화 거래 양성화의 토대
- **검찰은 암호화폐 거래소들의 불법에 대해 지속 수사중**
  - 2018. 4. 코인네스트 등 3개 거래소 구속 기소(허위 코인 매매 등), HTS거래소, 업비트 압수수색 등
  - 자본시장법 등 적용 곤란하므로, 사기/횡령/배임으로 기소 중

71

통계청 암호화폐 거래소, 산업분류 기준 발표

암호화폐 거래소→암호화 자산 매매 및 중개업

이더리움 등 블록체인 플랫폼 개발업체→블록체인 기반 시스템 소프트웨어 개발 및 공급업

블록체인 기술 산업 분류 조정안

분류코드	분류 명칭
581	소프트웨어 개발 및 공급업
58211-1	블록체인 기반 유선 온라인 게임 소프트웨어 개발 및 공급업
58212-1	블록체인 기반 모바일 게임 소프트웨어 개발 및 공급업
58221-1	블록체인 기반 시스템 소프트웨어 개발 및 공급업
58222-1	블록체인 기반 응용 소프트웨어 개발 및 공급업
620	컴퓨터 프로그래밍, 시스템 통합 및 관리업
62010-1	블록체인 기반 컴퓨터 프로그래밍 서비스업
62021-1	블록체인 기반 컴퓨터 시스템 통합 자문 및 구축 서비스업
62090-1	블록체인 기술 관련 기타 정보기술 및 컴퓨터 운영 서비스업
63	정보서비스업
63112-1	블록체인 기술 관련 호스팅 서비스업
63999-1	블록체인 기반 암호화 자산 매매 및 중개업
63999-2	블록체인 기술 관련 기타 정보서비스업

72

통계청 암호화폐 거래소, 산업분류 기준 발표

1. 소프트웨어 개발 및 공급업

1.1 블록체인 기반 유선 온라인 게임 소프트웨어 개발 및 공급업	블록체인에 기반한 인터넷 게임을 개발하고 공급하는 업종
1.2 블록체인 기반 모바일 게임 소프트웨어 개발 및 공급업	블록체인 기반 모바일 게임 개발과 모바일용 크립토게임 개발하는 업종
1.3 블록체인 기반 시스템 소프트웨어 개발 및 공급업	디앱 개발용 운영체계 개발하는 업종
1.4 블록체인 기반 응용 소프트웨어 개발 및 공급업	블록체인 기술이 적용된 특정 업무 처리 소프트웨어 개발하는 업종

73

통계청 암호화폐 거래소, 산업분류 기준 발표

2. 컴퓨터 프로그래밍, 시스템 통합 및 관리업

160여개 기관들의 의견을 수렴한 후 7월 말 최종안 확정하고 공개할 예정

2.1 블록체인 기반 컴퓨터 프로그래밍 서비스업	주문형 블록체인 소프트웨어 개발업
2.2 블록체인 기반 컴퓨터 시스템 통합 자문 및 구축 서비스업	블록체인 기술을 적용하기 위해 시스템통합(SI) 자문, 설계, 구축하는 분야
2.3 블록체인 기술 관련 기타 정보기술 및 컴퓨터 운영 서비스업	암호화 자산 취득용 하드웨어 및 소프트웨어 설치·운영, 블록체인 네트워크 참여를 통한 신규 블록 생성 지원 서비스

74

통계청 암호화폐 거래소, 산업분류 기준 발표

3. 정보서비스업

3.1 블록체인 기술 관련 호스팅 서비스업	블록체인 기술 사용과 개발을 위한 클라우드 서비스 제공 사업
3.2 암호화 자산 매매 및 중개업	암호화 자산을 매매 및 중개를 하는 분야빗썸, 업비트, 코인원, 코빗 등 암호화폐 거래소가 해당됨
3.3 블록체인 기술 관련 기타 정보서비스업	블록체인 기술 적용과 관련해 제공하는 달리 분류되지 않은 각종 정보서비스 활동

75

금감원, 국내 ICO 실태 점검 조사

점검 대상	ICO를 진행하였거나 진행중인 회사	
점검 범위	**I. 회사 개황 관련**	**1. (국내) 기술보유 회사 개황:** 일반 현황, 재무현황, 벤처 기업 지정관련, VC 등 투자 관련, 상장여부 등
		2. (발행지) 발행 회사 개황: 소재지 국가, 법인 등록번호, 발행회사의 법인형태, 일반현황, 재무현황, 주요주주 등
		2. (발행지) 발행 회사 개황: 시술보유회사의 발행회사 접촉경위, 투자관계, ICO 후 취득(예정) 코인의 향후 배분 계약 내용, 양 사간 계약서상 주요 계약 내용
	II. 양 사간 계약 관계	**1. 프로젝트의 주요내용:** 구체적인 사업 내용, 기반이 되는 블록체인 기술, 기존 블록체인 기술 사용 또는 독립 블록체인 개발 이유, 수익구조 및 현재 수익발생여부
		2. 프로젝트 진행경과: 주요 진행경과, 계획에 따른 진행여부, 지연시 지연사유, 향후계획 및 일정, 관련 회사와의 업무제휴 등 계약현황

금감원, 국내 ICO 실태 점검 조사

점검 범위	III. ICO 진행 관련	1. **코인(토큰)의 성격:** 발행 대상이 코인인지, 토큰인지 여부, 코인(토큰)으로 발행하는 이유, 코인(토큰)을 어떤 경우에 사용 가능한지, ICO후 취득(예정) 코인에 대한 양 사의 회계처리
		2. **코인(토큰) 발행물량:** 코인(토큰)의 총 발행가능 물량, 총 ICO 물량, ICO 물량 중 국내 거주자에게 배정된 물량, 향후 추가 발행계획 및 발행방식
		3. **ICO 진행경과:** ICO 관련 백서 공개 여부, ICO 진행경과, 가상화폐취급업소 상장여부 및 상장내역, ICO로 조달한 통화, 발행지 국가에서 진행한(진행중인) 행정처리 절차, 해외에서 ICO를 진행한 이유, ICO를 통해 모집한 코인(이더리움 등) 중 세일 관련 인건비, 홍보비 등 블록체인사업 외적인 부분으로 제출한 비용

77

금감원, 국내 ICO 실태 점검 조사

점검 범위	IV. 국내투자자 대상 홍보 관련	1. **국내투자자 대상 홍보 주체:** 누가 계획 및 진행하였는지
		2. **국내투자자 대상 홍보 현황:** ICO 관련 한국어 백서 공개 여부, 국내 거주자를 대상으로 어떤 방식으로 홍보하였는지, 국내투자자 대상 온라인 홍보내역, 국내투자자 대상 설명회 개최내역
	V. 코인(토큰) 투자자에게 부여되는 혜택 (권리)	1. **백서에 기재되어 있는 사항:**코인(토큰) 또는 포인트 추가 지급여부, 프로젝트 수행으로 발생하는 이익의 투자자 배당 여부, 기타 방식 있는지 여부, 코인(토큰) 보유자의 경영참여 여부(의결권 행사 등), 코인(토큰)의 가치를 보장하는 내용
		2. **백서에 기재되어 있지 않은 사항:** 기재되어 있지 않지만 실제 코인(토큰) 또는 프로젝트에서 발생한 이익을 추가지급한 적이 있는지 여부, ICO 이후 투자자는 발행회사 및 프로젝트와 완전히 단절되고, 코인(토큰)의 가치변동(취급업소 시세) 이익만 향유하는지 여부

78

금감원, 국내 ICO 실태 점검 조사

점검 범위	VI. 그 외 사항	1. 코인(토큰) 지갑생성 가능 여부 및 전송 방법
		2. 코인 개발자(개발팀)의 가상화폐 관련 이력 및 코인보유 현황(또는 계획)
		3. 코인의 의사결정 방식

79

III. 증권형 토큰과 유틸리티형 토큰에 대한 주요국 입장

80

증권형 토큰과 유틸리티 토큰의 구별에 대한 각국 입장

미국 SEC의 유틸리티 토큰에 대한 입장

- 유틸리티 토큰은 이익에 대한 기대가 아니라 사용에 대한 기대를 수반해야
  - should carry an expectation of use, not an expectation of profits
- Howey test를 충족하면 증권(투자계약증권)
  - 가) 금전의 투자가 있고(a person invests their money)
  - 나) 그러한 금전이 공공의 사업에(in a common enterprise) 투자가 되며
  - 다) 그 목적이 투자로부터 이익을 얻기 위한 것(with an expectation of profits)이고
  - 라) 투자된 금전으로부터 발생하는 수익이 오로지 사업자나 제3자의 노력에 의한 것(based on the efforts of the promoter or a third party)

81

증권형 토큰과 유틸리티 토큰의 구별에 대한 각국 입장

미국 SEC의 유틸리티 토큰에 대한 입장

- SEC가 암호화폐를 증권으로 분류한 사례

1) SEC는 DAO token이 증권에 해당한다고 보고, 2017.7. 발표한 DAO case의 조사보고서에서, 분산원장이나 블록체인기술기반의증권은 연방증권법의 적용을 받으며, 그 증권을 발행하는 사람은 발행하는 사람은 증권의 제공 및 판매 등록을 할 의무가 있고, 등록하지 않은 제공에 참여한 사람들도 증권법 위반의 책임이 있다고 판단함
2) SEC는 리뷰 애플리케이션인 Munchee의 토큰 제공에 대하여, Howey test에 근거하여 Munchee의 토큰, 즉 MUN token 역시 투자계약이며, 따라서 증권법 제2(a)(1)조 상의 증권에 해당한다고 판단함
3) SEC는 Centra를 상대로 소송을 제기하며, Centra ICO에서 제공한 투자(investments)가 증권법 및 증권거래법 상의 증권에 해당한다고 주장함

- 이러한 SEC의 입장에 따르면 수익을 기대하고 투자하는 수 많은 ICO들이 증권에 해당하여 SEC의 규제를 받게 되나, 전반적인 금지조치는 아직 취하지 않음

82

증권형 토큰과 유틸리티 토큰의 구별에 대한 각국 입장

스위스 FINMA의 가이드라인에 따른 암호화폐 분류

스위스 금융시장감독기구(FINMA)가 2018.2. 발표한 가이드라인

Categories	Functions/purposes	ICO 당시 증권 여부	
		토큰 있음	토큰 없고 계약지위이전가능
Payment tokens(지불형)	지불수단으로서만 기능	증권 아님 스위스 자금세탁법 적용	O (자금세탁법은 적용안됨)
Utility tokens(기능형)	애플리케이션이나 서비스에 대한 디지털 접근을 제공	증권아님(오직 유틸리티형) 증권(투자적 기능을 할 경우)	
Asset token(자산형)	- 실제 physical underlyings, 회사 또는 수익흐름에 참여 - 배당금 또는 이자수급권 - 주식, 채권, 파생상품과 유사	증권(증권법 및 민법 적용)	

83

증권형 토큰과 유틸리티 토큰의 구별에 대한 각국 입장

스위스 FINMA의 가이드라인에 따른 암호화폐 분류

- **유틸리티 토큰**
  - "특정 벤처가 제공하는 상품이나 서비스에 대한 사용권을 부여하는 토큰
    - Confers usage rights in a product or service offered by a specific venture
  - "특정 프로젝트를 위한 청산, 거래 또는 지불의 목적으로만 사용되는 토큰
    - Tokens that are used solely for clearing, exchange or payments for a specific project
- **증권형 토큰**
  - 지분, 채권 또는 참여단위와 같은 전통적인 증권에 대한 것과 유사한 권리를 부여하는 토큰
    - conferring rights similar to those of conventional securities, such as shares, bonds, or participation units
  - 소유자에게 미래의 현금흐름에 참여할 수 있는 권한을 주거나, 특정 벤처에 대한 소유권, 참여, 또는 회원자격을 부여하는 토큰
    - entitling the holder to the future cash flow or "ownership rights, participation, or membership in a specific venture

84

생각해봅시다

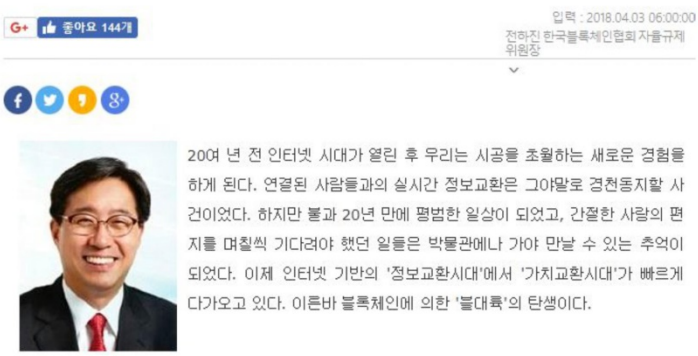
블록체인과 암호화폐가 현실 경제에 미칠 영향

85

생각해봅시다

긍정적인 시각 : 지상경제에서 하늘경제, 분산경제(Deconomy)로

[기고] 전하진 위원장 "블록체인 대륙, 기회의 땅이 되어야..."



<출처 : https://steemit.com/ico/@hajinhun/3ybtgc (블록체인협회 전하진 위원장)>

86

생각해봅시다

긍정적인 시각 : 지상경제에서 새로운 개념의 분산경제(Deconomy)로

- 세계 경제는 '지상경제 ' 에서 '하늘경제 ' 로 이동하기 시작
- 이는 지상경제가 가진 불합리함에 대한 대안 찾기임
- 2008년 세계 금융위기 이후 모럴해저드, 부의 편중이 그 원인
- 블록체인 기술에 의한 '블대륙 ' 에서 분산경제(Deconomy)라 불리는 새로운 경제시스템이 시도되고 있음
- '하늘경제'는 실물자산을 암호자산(Crypto Asset)으로 대체하는 작업에서 시작됨
- 중간자(Middle-men)이 사라지고 모든 것이 탈중앙화 됨

<출처 : https://steemit.com/ico/@hajinhun/3ybtgc (블록체인협회 전하진 위원장)>

87

생각해봅시다

긍정적인 시각 : 지상경제에서 새로운 개념의 분산경제(Deconomy)로

<출처 : https://steemit.com/ico/@hajinhun/3ybtgc (블록체인협회 전하진 위원장)>

88

생각해봅시다

긍정적인 시각 : 암호자산 중심의 경제체제로 이행

- 하늘경제는 지상경제와 달리 실물자산이 암호자산화 되어 디지털로 거래가 가능
  - 미국의 실물부동산을 한국에서 확인하고 코인으로 구입하는 것도 가능
  - 암호자산을 토큰화하여 분산경제, 공유경제를 용이하게 구현 가능
    - 전세계 유휴 컴퓨터 자원을 이용하여 대형 IDC처럼 운영 가능

- 지상경제는 '이익을 최선으로' / 하늘경제는 '가치를 최선으로'
- 적은 참여자들에게도 토큰을 정교하게 배분, 누구에게나 적절한 보상이 가능

<출처 : https://steemit.com/ico/@hajinhun/3ybtgc (블록체인협회 전하진 위원장)>

89

생각해봅시다

긍정적인 시각 : 지상경제에서 새로운 개념의 분산경제(Deconomy)로

- '블대륙'에서는 다양한 생태계가 끊임없이 탄생할 것
- 가치는 토큰에 축적되고, 가치들이 정교하게 물물교환처럼 교환될 것
- 번성하는 생태계도 있고, 사라지는 생태계도 있을 것
- 자기자본/타인자본에 의해 기업을 경영하고 이윤 극대화를 추구하는 기업과는 달리, 다수의, 다수에 의한, 다수를 위한 생태계가 구축될 것
- 현재 지상경제의 통념으로 바라보면 요원하지만, 머지 않아 '하늘경제'가 인류의 상식으로 자리잡게 될 것이고, 인류를 구원할 것임

<출처 : https://steemit.com/ico/@hajinhun/3ybtgc (블록체인협회 전하진 위원장)>

90

생각해봅시다

긍정적인 시각 : 지상경제에서 새로운 개념의 분산경제(Deconomy)로

비탈릭 부테린 "블록체인 본질은 제3자 검열 거부"

〈현장에서〉탈(脫)중앙 재강조..."누구나 접근·이용 가능해야"
올해 보안성 강화 집중..."향후 속도는 높이고 비용은 낮춘다"

2018년 04월 06일 16:36:38 임영빈 기자 sisaon@sisaon.co.kr

(시사오늘, 시사ON, 시사온=임영빈 기자)

▲ 비탈릭 부테린이 지난 4일 서울 광진구 워커힐 호텔에서 열린 '제1회 분산경제포럼 2018(DECONOMY 2018)'에서 이더리움의 향후 계획에 대해 설명하고 있다. ⓒ프레인

91

생각해봅시다

부정적인 시각 : 암호화폐 = 사기꾼들의 좋은 친구

"가상화폐는 사기" vs "기술은 계속 발전"…세기의 설전

대표적 비관론자 루비니 뉴욕대 교수 / 이더리움 창시자 부테린

입력 : 2019-04-04 21:06:16 수정 : 2019-04-04 21:06:16

누리엘 루비니(왼쪽), 비탈릭 부테린

"가상화폐는 사기다." vs "아직 초기. 기술은 계속 발전하고 있다."

대표적 가상화폐(암호화폐) 비관론자인 누리엘 루비니 뉴욕대 교수와 이더리움 창시자 비탈릭 부테린이 서울에서 맞붙었다. 블록체인을 둘러싼 '세기의 설전'이라고 할 만하다.

92

<출처 : "가상화폐는 사기" vs "기술은 계속 발전"...세기의 설전, 백소용 기자, 2019.4.4.,세계일보>

생각해봅시다

부정적인 시각 : 암호화폐 = 사기꾼들의 좋은 친구

3800여명에게서 340억!...역대급 '암호화폐' 투자사기

1년 안에 최대 1만배 차익 홍보..."암호화폐 투자 권유 시 주의해야"

조성호 기자 승인 2019.04.16 18:18 댓글 0

암호화폐 다단계 사기 범죄 흐름도. 사진=부산지방경찰청

[민주신문=조성호 기자] 가짜 암호화폐를 만든 뒤 이에 투자하면 수십배의 차익을 얻을 수 있다고 속여 투자자를 모집하는 암호화폐 투자사기 행위가 기승을 부리고 있어 주의가 요구된다.

<출처 : "3800여명에게서 340억!...역대급 '암호화폐' 투자사기", 조성호 기자, 2019.4.16., 민주신문>

93

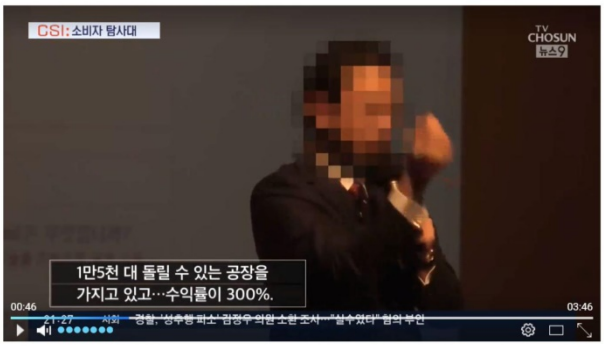
생각해봅시다

부정적인 시각 : 암호화폐 = 사기꾼들의 좋은 친구

[CSI] 가상화폐 채굴 현장 가보니, 먼지만 '풀풀'

등록 2019.04.15 21:30 / 수정 2019.04.15 21:37

기획취재부 | 송무빈 기자 | moving@chosun.com 이기자의 기사 더보기 ▸



<출처 : "가상화폐 채굴 현장 가보니, 먼지만 '풀풀'", 송무빈 기자, 2019.4.15., TV조선>

94

생각해봅시다

블록체인과 암호화폐가 현실 경제에 미칠 영향

- 암호화폐는 단지 튤립과 같은 투기자산일 뿐인가?
- 블록체인과 암호화폐가 현실 경제에 미칠 영향은?

목차

1. 국회에 제출된 블록체인/암호화폐 관련 법률안
2. ICO 관련 국내 소송 사례
3. ICO 관련 해외 소송 사례
4. ICO 프로젝트 시 유의할 점
부록1 G20 재무장관회의와 암호화폐 논의 동향

생각해봅시다 : 암호화폐 없는 블록체인, 과연 현실성이 있나

I. 국회에 제출된 블록체인/암호화폐 관련 법률안

97

국회에 제출된 블록체인/암호화폐 관련 법률안

국회 발의된 암호화폐, 블록체인 관련 법안 일람표

	대표 발의 의원 이름	법안	관련성
1	정병국	'암호통화 거래에 관한 법률안'	가상화폐 정의, 거래 및 거래소 운영
2	정태옥	'가상화폐에 관한 특별법안'	가상화폐 정의, 거래 및 거래소 운영
3	박용진	'전자금융거래법 일부개정법률안'	가상화폐 정의, 거래 및 거래소 운영
4	채이배	'전자상거래 등에서의 소비자보호에 관한 일부개정법률안'	"투자자 보호"를 위한 가상화폐 거래 및 거래소 운영
5	제윤경	'특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안'	가상화폐 금융상품으로 인정, 금융제도권 편입 규정 마련
6	신용현	'전자문서 및 전자거래 기본법 일부개정법률안'	작성된 블록의 전자문서 인정
7	신용현	'전자서명법 일부개정법률안'	작성된 블록의 전자문서 인정
8	권은희	'개인정보 보호법 일부개정법률안'	블록체인 기술의 개인정보보호법 저촉
9	오세정	'위치정보의 보호 및 이용 등에 관한 법률 일부개정법률안'	블록체인 기술의 위치정보보호법 저촉
10	하태경	'전자금융거래법 일부개정법률안 '	가상화폐 정의, 거래 및 거래소 운영

98

국회에 제출된 블록체인/암호화폐 관련 법률안

1. 정병국 의원: 암호통화 거래에 관한 법률안

- **암호화폐에 대해 직접적인 관련이 있는 법안**
- 암호통화의 정의 규정을 마련하고 안전성 확보 및 이용자 보호를 위해 거래소의 예치금 및 피해보상계약, 보안대책 수립 의무 등 마련하기 위한 법안임. 거래방식 제한, 자기매매 제한, 시세조종행위 금지, 공매도 제한, 거래소 개설 기준을 마련하였음
- <주요 내용 요약>

1.암호통화 취급을 하는 모든 업자는 금융위원회에 등록해야 한다.

2.암호통화 거래업자는 투자자 보호를 위해 피해보상 계약을 체결해야 한다.

3.암호통화거래의 안전성 및 신뢰성 확보를 위해 보안대책을 수립하고 시행해야 한다.

4.암호통화 매매등과 관련한 시세조종행위 및 자금세탁행위를 금지한다.

5.암호통화이용자에 대하여 매매권유 등을 하는 경우 설명의무를 부과하고 방문판매를 금지한다.

99

국회에 제출된 블록체인/암호화폐 관련 법률안

2. 정태옥 의원: 가상화폐에 관한 특별법안

- **암호화폐에 대해 직접적인 관련이 있는 법안**
- 가상화폐의 정의와 관련업에 대한 인가규정, 실명확인, 안전한 거래를 위한 보안조치, 이용자 피해 배상의무, 자율규제 등을 규정하는 특별법을 제정하여 가상화폐에 대한 영업의 자유를 보장하는 한편 투자자를 보호하여 가상화폐업을 건전하게 육성하고자 법안을 발의하였음.
- <주요내용 요약>

1.거래소 운영을 위해서는 금융위원회의 인가를 받아야 하고 금융감독원은 인가된 거래소를 감독.

2.거래소의 거래 기록을 일정기간 모두 보존.

3.거래소 운영방식- 투자자의 실명확인 의무 및 미성년자에 대한 거래 금지, 불건전 영업행위금지, 불공정거래행위 금지, 자금세탁행위 금지, 거래 방식의 제한 규정.

4.가상화폐 거래 안전성 확보를 위해 금융위원회가 정하는 정보기술 기준 준수.

5.사고로 인한 투자자 손해 발생시 배상할 책임.

100

국회에 제출된 블록체인/암호화폐 관련 법률안

3. 박용진 의원: 전자금융거래법 일부개정법률안

- **암호화폐에 대해 직접적인 관련이 있는 법안**
- 가상통화의 정의규정을 마련하고, 가상통화 취급업의 인가 등에 대한 규정을 신설함과 동시에 이용자 보호를 위한 의무와 금지행위 등을 규정함으로써 가상통화 이용자를 두텁게 보호하고자 법안 개정을 발의하였음.
- <주요내용 요약>

1.가상통화를 정의하고 가상통화 취급업을 분류하여 정의함.

2.거래소의 인가 요건 및 인가 신청등에 관한 사항을 정함.

3.투자자 보호를 위하여 피해보상계약을 체결하거나 예치금마련을 규정.

4.시세조종행위, 자금세탁행위 금지, 거래방식 제한, 투자자에 대한 설명의무 규정.

101

국회에 제출된 블록체인/암호화폐 관련 법률안

정병국, 정태옥, 박용진 의원이 발의한 세 법안 비교 분석(출처:대한금융신문)

- 자본시장연구원은 국내에 발의된 3개의 법안을 비교 분석하며 "세 법안 모두 가상화폐가 가진 투자성에 기초한 쟁점 해결에만 초점을 맞추고 있으며 가상화폐의 가장 기본적인 기능인 '지급결제성' 부분은 다루고 있지 않다"며 "가상화폐 '발행시장' 규제에 관한 심도 있는 검토와 국제적 쟁점 문제 또한 소홀한 부분이 있다"고 평가했다.
- 세 법안을 비교해보면 공통적으로 최근 가장 이슈가 되고 있는 가상화폐거래소를 규제영역 안으로 포섭하기 위해 '거래업'이라는 정의를 마련하고 있다. 단 정태옥 의원안에서는 ICO(가상통화공개발행)와 관련된 규제수단이 될 수 있는 '발행업'에 대한 개념이 없고 '가상화폐계좌관리업'과 '가상화폐보조업'이라는 특수한 형태의 업무를 규정하고 있다.
- 가상화폐거래소에 대한 영업규제는 크게 설명의무, 가상통화예치금의 별도예치의무, 방문판매 등의 방법에 의한 거래금지 등으로 구분할 수 있다.
- 세 법안 모두 가상통화 거래의 높은 위험성을 고려해 금융투자업의 설명의무와 유사한 규정을 도입하고 있는데, 특히 정태옥 의원안은 자본시장법의 투자권유 규제에 관한 조문을 준용하는 방식을 취해 광고를 시행령에서 정하는 요건 하에서만 허용하는 등 금융투자업에 준하는 투자권유규제를 도입하고 있다.
- 반면 박용진•정병국 의원안은 설명의무만을 규정하고 위험고지 내용 중 가상화폐는 화폐가 아니라는 사실 등을 투자자가 이해할 수 있도록 설명하고 있다.

102

국회에 제출된 블록체인/암호화폐 관련 법률안

정병국, 정태옥, 박용진 의원이 발의한 세 법안 비교 분석(출처:대한금융신문)

- 가상화폐 중개기관의 매매 및 중개방식 중 방문판매법에 따른 방문판매•전화권유판매•다단계판매•후원방문판매 등의 방법에 의한 거래도 세 법안 모두 금지하고 있다. 이는 다단계 폰지사기 등 가상화폐와 관련된 무분별한 가상화폐 판매행위를 금지하기 위한 것으로 풀이된다.
- 한편 현재 발의된 법안 모두 미국이나 일본 등 가상화폐 규제체계를 정비한 국가와 달리 가상통화거래의 불공정거래행위와 관련한 명문의 규정을 두고 있다.
- 박용진•정병국 의원안은 가상통화의 유형별 시세조종행위 금지규정을 도입해 형사처벌을 할 수 있는 근거를 마련했으며, 정태옥 의원안은 시세조종을 비롯한 자본시장법상 3대 불공정거래행위인 미공개정보이용행위, 시세조종행위, 부정거래행위 모두를 규제영역 안으로 포섭하기 위해 관련 자본시장법을 준용하고 있다.
- 자본시장연구원은 "국회에서 본격적인 입법을 위해 가상통화와 관련된 세개의 법안이 상정된 것은 매우 고무적인 일"이라며 "정태옥 의원안의 경우 자본시장법상 시장교란행위 관련 규정도 준용하고 있어 가상화폐를 준금융투자상품으로 본다면 정태옥 의원안의 접근□
- 현재 국회에 상정된 세 법안은 가상화폐의 투자성에만 중점을 둔 나머지 가상화폐의 지급결제성과 관련된 쟁점은 고려하지 못하고 있으며, 사실상 증권의 상장 및 상장폐지와 동일한 의미를 가진 가상화폐거래소의 거래대상 추가 및 제외행위 등을 어떻게 규제할 것인지에 대해서도 미비한 부분이 있다.
- "현재 거래되고 있는 가상화폐는 대부분 국제성을 가지고 있어 가상화폐의 국제성에 따른 쟁점을 감안해 자본시장법 제2조의 역외적용처럼 해당 법안을 역외적용할 수 있는지도 명확히 검토할 필요가 있다".

103

국회에 제출된 블록체인/암호화폐 관련 법률안

정병국, 정태옥, 박용진 의원이 발의한 세 법안 비교 분석(출처:대한금융신문)

◇국회에 계류 중인 암호화폐 관련 법률 현황

구분	박용진 의원안	정태옥 의원안	정병국 의원안
발의법안	전자금융거래법 일부개정법률안	가상화폐업에 관한 특별법안	암호통화 거래에 관한 법률안
명칭	가상통화	가상화폐	암호통화
중개기관 진입규제	인가제 자기자본 5억원 이상	인가제 자본금 30억원 이상	등록제 자기자본 1억원 이상

<출처: 대한금융신문>

104

국회에 제출된 블록체인/암호화폐 관련 법률안

4. 채이배 의원: 전자상거래 등에서의 소비자보호에 관한 일부개정법률안

○ **암호화폐의 법적인 성격과 정의를 내리고 거래소 해킹 등으로 암호화폐와 관련하여 피해를 입은 소비자 보호를 위한 법률임.**

○ <주요내용 요약>

1.암호화폐의 제도화가 이루어지는 동안에도 소비자 피해 방지를 위한 제도적 근거 마련.

2.암호화폐 거래소의 소비자 보호 시스템과 보안수준 조사 및 감독

3.망 분리 등 고객 재산 보호를 위해 필요한 조치 의무 부여.

4.거래소 운영업자가 조치 미 이행 중 해킹 등 사고가 발생할 경우 손해에 무과실 책임.

105

국회에 제출된 블록체인/암호화폐 관련 법률안

5. 제윤경 의원: 특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안

○ 가상통화는 거래를 통해 현금 등 금융자산과의 교환이 가능할 뿐 아니라 거래의 익명성이 높아 자금세탁 및 공중협박자금조달의 위험성이 높음에도 불구하고 현행법상 위험성을 예방하기 위한 법•제도적 장치가 마련되어 있지 않은 상황임. 가상통화취급업소에 자금세탁행위 및 공중협박자금조달행위의 효율적 방지를 위한 의무를 부과하고, 금융회사가 가상통화취급업소와 금융거래를 수행할 때 준수할 사항을 규정한 법안을 발의하였음.

○ <주요내용 요약>

1.가상통화 거래를 금융거래로, 가상통화 거래소를 금융회사에 포함한다. 따라서 거래소가 금융회사등이 지켜야 할 자금세탁행위 및 공중협박자금 조달 행위 방지를 위한 내부 절차를 마련하고 업무지침에 반영해야함을 규정했다.

2.가상통화 거래소와 금융거래를 하는 금융회사는 거래소의 신고의무 이행여부를 확인해야한다.

3.금융회사는(거래소 포함) 의심거래보고, 고액현금거래보고, 고객확인 등 의무이행과 관련한 금융거래 자료 및 정보를 5년간 보존해야 한다.

4.가상통화 거래소는 금융정보분석원의 장에게 상호 및 대표자의 성명을 신고하고 공중협박자금조달 행위를 방지하기 위한 조치를 취해야 한다.

106

국회에 제출된 블록체인/암호화폐 관련 법률안

6. 신용현 의원: 전자문서 및 전자거래 기본법 일부개정법률안

- 현행법은 전자적 형태로 되어있다는 이유로 전자문서의 문서로서의 효력이 부인되지 아니한다고 규정하면서, 기록•보고•보관•비치 또는 작성 등의 행위가 전자문서로 행하여진 경우 해당 법률에 따른 행위가 이루어진 것으로 간주하는 경우를 별표에서 제한적으로 규정하고 있음.
- 한편, 제4차 산업혁명과 관련하여 구성원 간 직접 연결 방식을 기반으로 정보를 분산 저장하는 블록체인기술에 대한 관심이 증가하면서, 블록체인기술을 활용하여 전자적 형태로 작성, 송신•수신 또는 저장된 정보 역시 전자문서에 해당하는지 여부가 논란이 되고 있음.
- <주요내용>:

전자문서가 일반적으로 서면의 효력을 가지도록 하는 한편, 블록체인기술을 활용하여 전자적 형태로 작성, 송신•수신 또는 저장된 정보가 전자문서에 포함되도록 명시하여 전자문서의 이용을 촉진하기 위한 법안을 발의하였다. (안 제2조제1호, 제4조제3항 및 안 제4조의2 신설 등).

107

국회에 제출된 블록체인/암호화폐 관련 법률안

7. 신용현 의원: 전자서명법 일부개정법률안

- 공인전자서명은 그것이 있는 경우 해당 전자문서가 전자서명 된 후 그 내용이 변경되지 아니하였다고 추정되는 등의 효력을 가지고 있어 보안성이 높고 위조가 어려워야 함.
- 따라서 구성원 간 직접 연결 방식을 기반으로 각각의 정보가 저장된 블록이 사슬처럼 연결되는 분산화된 정보 처리 기술인 블록체인기술을 공인전자서명에 활용하는 경우, 암호화된 정보가 분산 저장된다는 점에서 보안성이 높고 위조가 불가능하다는 장점이 있을 것으로 평가됨.
- <주요내용>:

과학기술정보통신부장관이 블록체인기술을 활용한 전자서명 중 일정한 요건을 갖춘 전자서명을 공인인증 전자서명으로 지정할 수 있도록 하고, 공인인증 전자서명을 공인전자서명에 포함되도록 규정하며, 공인인증 전자서명을 본인확인에 이용할 수 있도록 하여 공인전자 서명의 보안성 제고에 기여하려는 법안이다(안 제4조의2 신설 등).

108

국회에 제출된 블록체인/암호화폐 관련 법률안

8. 권은희 의원: 개인정보 보호법 일부개정법률안

- 블록체인 기술은 대부분의 ICT 기술과 연관되어 있으며, 향후 금융 및 공공 산업을 포함한 대부분의 산업 분야에 활용될 것으로 예측됨.
- 거래의 기록 및 관리에 대한 권한을 중앙기관 없이 P2P 네트워크를 통해 분산하여 기록하고 저장하는 블록체인 기술의 특성 상 개별 블록에 저장된 데이터를 완전히 삭제하는 경우 블록체인 연결고리가 끊어져 시스템이 가동되지 않는 문제가 있음.
- 그런데 현행 개인정보보호법은 개인정보의 처리 목적이 달성 된 경우 정보를 파기한다고 정하고 있어, 블록체인 기술의 적용이 제한되고 있음.
- <주요내용>:

파기의 범위를 기술적 조치를 통해 내용을 확인할 수 없는 형태로 폐기하는 범위로 구체화하여 블록체인 기술이 개인정보 처리에 활용될 수 있도록 하며, 관련 산업을 활성화 하고자 함(안 제21조제1항).

109

국회에 제출된 블록체인/암호화폐 관련 법률안

9. 오세정 의원: 위치정보의 보호 및 이용 등에 관한 법률 일부개정법률안

- 블록체인 기술은 대부분의 ICT 기술과 연관되어 있으며, 향후 금융 및 공공 산업을 포함한 대부분의 산업 분야에 활용될 것으로 예측되고 있음.
- 거래의 기록 및 관리에 대한 권한을 중앙기관 없이 P2P 네트워크를 통해 분산하여 기록하고 저장하는 블록체인 기술의 특성상 개별 블록에 저장된 데이터를 완전히 삭제하는 경우 블록체인 연결고리가 끊어져 시스템이 가동되지 않는 문제가 있음.
- 그런데 현행 위치정보보호법은 위치정보 사업을 휴지하는 경우 정보를 파기한다고 정하고 있어 블록체인 기술의 적용이 제한되고 있음.
- <주요내용>:

파기의 범위를 기술적 조치를 통해 내용을 확인할 수 없는 형태로 폐기하는 범위로 구체화하여 블록체인 기술이 위치정보 처리에 활용될 수 있도록 하며, 관련 산업을 활성화하고자 한다. (안 제8조).

110

국회에 제출된 블록체인/암호화폐 관련 법률안

10. 하태경 의원: 전자금융거래법 일부개정법률안

- 암호통화의 매도·매수·중개·교환·관리 등 암호통화취급업을 허가 대상으로 하고, 암호통화 발행은 금융위원회의 승인을 받아 할 수 있도록 하며, 보안대책 수립·시행, 시세조종행위 등의 금지, 금융위원회 및 금융감독원의 감독 및 검사 등 암호통화의 안전성, 신뢰성 및 이용자 보호에 관한 규정을 마련하려는 것임

<주요내용 요약>:

- 가. 암호통화취급업을 암호통화매매업, 암호통화거래업, 암호통화중개업, 암호통화관리업 등으로 분류하고 이를 허가의 대상으로 함
- 나. 암호통화의 발행은 금융위원회의 승인을 받은 경우에 할 수 있도록 하며, 승인 및 기준의 심의를 위하여 금융위원회에 암호통화발행심사위원회를 둠
- 다. 금융위원회가 정하는 기준에 부합하는 기술적·물리적·관리적 보안대책을 수립·시행하도록 함
- 라. 암호통화이용자를 보호하기 위하여 암호통화취급업자로 하여금 피해보상계약을 체결하도록 함
- 마. 암호통화거래에 대한 시세조종행위의 금지, 미공개중요정보 이용 등 시장질서 교란행위의 금지 자금세탁행위 등의 금지, 이용자에 대한 설명의무를 규정함
- 바. 시세조종행위 및 시장질서 교란행위에 대하여 위반행위로 얻은 이익 등에 비례하는 과징금 또는 벌금을 도입함

111

국회에 제출된 블록체인/암호화폐 관련 법률안

정병국, 정태옥, 박용진, 하태경 의원이 발의한 법안 비교 분석

	정병국	정태옥	박용진	하태경
발의법안	암호통화 거래에 관한 법률안	가상화폐업에 관한 특별법안	전자금융거래법일부개정법률안	전자금융거래법 일부개정법률안
명칭	암호통화	가상화폐	가상통화	암호통화
암호통화 발행				암호통화의 발행은 위조 방지 및 거래의 안전성 등에 관하여 금융위원회가 정하여 고시하는 기준에 따라 승인을 받은 경우에 할 수 있도록 하며, 승인 및 기준의 심의를 하기위하여 금융위원회에 암호통화발행심사위원회를 둠
암호통화 취급 요건	암호통화취급업 (매매업/거래업/중개업/ 발행업/관리업 등) 금융위원회에 등록 자기자본 1억원 이상	가상화폐거래업/계좌관리업 영위 위해서는 금융위원회 인가. 자기자본 30억원 이상	가상통화취급업 (매매업/거래업/중개업/발행업/관리업) 금융위원회 인가 자기자본 5억 원 이상	암호통화취급업 (매매업/거래업/중개업/관리업) 금융위원회의 허가 자본금 또는 출자총액이 20억원 이상
중개기관 진입규제	등록제 자기자본 1억원 이상	인가제 자본금 30억원 이상	인가제 자기자본 5억원 이상	허가제 자본금 또는 출자총액이 20억원 이상

112

국회에 제출된 블록체인/암호화폐 관련 법률안

기존 법안/개정안의 문제점 - 암호화폐의 다양성을 고려하지 않음

1. 화폐	Bitcoin, Litecoin, Bitcoin Cash 등
2. 플랫폼	Ethereum, NEO 등
3. 핀테크	Bancor, Bancera, Crypterium 등
4. 지불	Ripple, Stellar Lumens, Request Network 등
5. 익명성	Monero, ZCash, Dash 등
6. 응용	Vechain, IOTA, Cardano 등
7. 가치교환	Steemit, MaidSafe, iExec 등

- ➢ 블록체인산업 관련 법률을 제정함에 있어 통일적인 규율이 아닌, 각 암호화폐의 속성에 따라 법률상 달리 취급해야 함
- ➢ 증권형이 아닐 경우 발행한 암호화폐 거래를 금융통화상품으로 취급해야 할 필연성이 적음

113

국회에 제출된 블록체인/암호화폐 관련 법률안

토큰의 속성 및 발행단계 구별 → 규제에 반영

토큰의 분류	ICO	IEO	트레이드 마이닝 토큰	거래소
지불형	지불형/유틸리티형은 자본시장법 적용 안됨. 금융통화상품도 아님(정부 입장) 단, 비증권형이라도 블록체인 서비스 개발 자금을 공모하는 ICO는 일정한 규율 필요 • 1안) 전자금융거래법에 금융위원회가 인가할 경우 ICO를 할 수 있도록 근거와 인가제를 도입하는 방안 • 2안) 전자금융거래법에 ICO를 정의하고, 금융위원회가 정하는 고시에 따라 할 수 있도록 하는 방안(금융위원회는 시정명령 등 행정제재) • 3안) 디지털토큰에 관한 특별법 제정 / ICO를 허용 • 4안) 정부 가이드라인으로허용하는 방안 • 5안) 기 제출 법률안처럼 금융위 인가/등록제	IEO: 개발완료된 서비스의 토큰을 판매하는 것 개발자금을 미리 공모하지 않으므로 단순한 상품 또는 이용권의 판매로서, 전자상거래법 적용	해당 없음	전자상거래법 적용
유틸리티형				
증권형	자본시장법 적용 • 1안) 전자금융거래법에 금융위원회가 인가할 경우 ICO를 할 수 있도록 근거와 인가제를 도입하는 방안 • 2안) 전자금융거래법에 ICO를 정의하고, 금융위원회가 정하는 고시에 따라 할 수 있도록 하는 방안(금융위원회는 시정명령 등 행정제재) • 3안) 디지털토큰에 관한 특별법 제정 / ICO를 허용 • 4안) 정부 가이드라인으로허용하는 방안 • 5안) 기 제출 법률안처럼 금융위 인가/등록제	자본시장법 적용(금융위원회 발행 허가)	자금의 공모가 없으므로 증권발행 아님. 자본시장법 적용 안됨	자본시장법 적용

114

II. ICO 관련 국내 소송 사례

115

블록체인 관련 법 적용 사례 및 개선안-법 적용 사례

- **암호화폐의 법적 성질**
  - 지불 수단, 유틸리티 수단, 자산으로서 성격을 모두 가짐
  - 기존의 주식, 사채 등 증서에 적용되는 증권법으로 규율하는 방식은 적합하지 않음
  - 무리하게 이를 법으로 정의할 필요 없음

- **ICO(Initial Coin Offering)**
  - ICO는 암호화폐를 모집하여 신발행 암호화폐를 대가/보상으로 주는 것으로 그 자체는 매매 또는 기부에 해당
  - 암호화폐가 통화도, 화폐도, 금융통화상품도 아니라는 정부의 입장으로 이에 대해 자본시장법 적용 곤란
  - 이를 금지할 것처럼 공언한 후 입법추진을 하지 않음에 따라 규제불확실성 때문에 다수의 내국 ICO 프로젝트가 해외에 법인을 세우고 진행 중
  - 다수 국가는 증권형 토큰의 발행이 아닌 한 허용하고 있는 추세

116

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례 및 개선안-법 적용 사례

- **원코인, 리코인 등 사기성 암호화폐 매매사건**
  - 2015년경부터 기승, 2017. 범정부 가상통화 TF가 암호화폐 거래에 대해 부정적 견해를 형성하는데 기여
  - 기존 법률인 유사수신행위등규제법, 사기죄 등 적용하여 수사 가능하므로 새로운 규제 필요성 적음

- **암호화폐 거래소들의 불법행위 수사**
  - 고객예치금 전용으로 2018. 4. 코인네스트 등 3개 거래소 구속 기소
    - (코인네스트) 고객예치금이 재원인 거래소 법인의 자금을 위험거래에 사용한 배임죄가 공소사실, 고객예치금은 예치되면 거래소 법인의 소유로 전환되는 혼장임치
    - 법인이 암호화폐 거래를 하는 것이 위험거래라서 배임죄가 되는지 여부에 대해 다툼의 여지 있음(다른 금융통화상품 투자도 위험거래인 점은 마찬가지이므로 객관적 구별기준 미존재)
  - 검찰은 암호화폐 거래소에 자본시장법이 적용되지 않으므로 사기, 횡령, 배임행위 규명에 집중
    - 업비트는 자체 암호화폐 지갑이 없다는 혐의를 잡고 수사에 들어갔으나 미국 비트렉스의 대리점이라는 점을 간과한 수사 착수라는 소문이 있음

117

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례 및 개선안-법 적용 사례

- **암호화폐 거래소 마진거래**
  - 거래소의 신용부여 행위(증거금의 4배까지)가 대부업법 위반인지, 회원들의 위험거래가 도박인지 여부가 쟁점
  - 기존 도박죄로는 처벌 안될 것으로 보는 견해 다수

- **암호화폐 거래소의 미공개정보 이용 거래 등**
  - 암호화폐의 성질에 대해 금융통화상품이 아니라는 정부 입장으로 미공개정보 이용 내부자거래, 시세조종 등 자본시장법상 규제가 적용되지 않음
  - 암호화폐 거래소는 미래 토큰경제의 중심축이므로 이들에게 최소한 지켜야할 법률규제가 무엇인지 연구 필요
    - 한편, 섣부른 법률규제는 산업의 발전을 저해함
    - 현재 한국블록체인협회 자율규제위원회가 회원사 거래소를 중심으로 자율규제기준을 발전시켜 나가고 있음

118

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례 및 개선안-법 적용 사례

- **비트코인 등 암호화폐를 이용한 환치기 수사**
  - 외국환거래법상 '무등록 외국환매매업 ' 으로 보고 수사
  - 암호화폐 없는 환치기와 암호화폐를 이용한 환치기가 동일한 결론이란 점은 의문. 금을 이용했다면 관세법위반(밀수), 디지털 골드인 암호화폐를 이용한 환치기는?
  - 암호화폐는 국내외 통관 이슈 없음. 마치 디지털콘텐츠를 이용하는 것과 유사

- **암호화폐 거래소 불법행위 수사**
  - 고객예치금 전용으로 2018. 4. 코인네스트 등 3개 거래소 구속 기소
    - (코인네스트) 고객예치금이 재원인 거래소 법인의 자금을 위험거래에 사용한 배임죄가 공소사실, 고객예치금은 예치되면 거래소 법인의 소유로 전환되는 혼장임치
  - 암호화폐의 성질에 대해 금융통화상품이 아니라는 정부 입장으로 미공개정보 이용 내부자거래, 시세조종 등 자본시장법상 규제가 적용되지 않음
  - 사기, 횡령, 배임행위 규명에 집중

119

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례-수원지법 2018. 1. 30. 선고 2017노7120 판결

- **사건 요지**
  - 피고인이 해외에 서버를 둔 음란사이트를 운영하면서 회원을 모집·관리하고 대량의 음란물을 유포하는 한편, 위 사이트에 불법 인터넷 도박 사이트의 광고를 게시하여 도박개장 범행을 방조하고, 타인의 접근매체를 불법 양수하여 차명계좌를 사용하는 방법으로 회원들 및 광고주들로부터 비트코인 등을 대가로 지급받았다는 내용의 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반(음란물유포) 등의 공소사실이 유죄로 인정된 사안

- **쟁점: 암호화폐가 재물인가**
  - '범죄수익은닉의 규제 및 처벌 등에 관한 법률'은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반(음란물유포)죄를 중대범죄로 규정하여 그 범죄행위에 의하여 생긴 재산 또는 그 범죄행위의 보수로 얻은 재산은 범죄수익으로서 몰수할 수 있다고 규정.
    → 암호화폐가 '재물'에 해당하는가 여부 문제: **재물성 인정**
  - **재물성 인정 근거**

① 예정된 발행량이 정해져 있고 P2P 네트워크 및 블록체인 기술에 의하여 그 생성, 보관, 거래가 공인되는 가상화폐로서, 무한정 생성·복제·거래될 수 있는 디지털 데이터와는 차별화 됨.

120

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례-수원지법 2018. 1. 30. 선고 2017노7120 판결

② 온라인 게임업체가 발급하는 것으로 '게임머니'도 구 부가가치세법상의 '재화'에 해당한다고 할 것이므로(대법원 2012. 4. 13. 선고 2011두30281 판결 참조), 물리적 실체가 없이 전자화된 파일의 형태로 되어있다는 사정만으로 재산적 가치가 인정되지 않는다고 단정할 수 없음

③ 수사기관은 피고인이 진술한 전자지갑의 주소 및 '비밀키'를 근거로 피고인이 보유하고 있던 비트코인을 특정한 후 압수하였으며, 해당 이체 기록이 블록체인을 통해 공시되어 압수된 비트코인의 동일성이 상실되지 않음.

④ 현실적으로 비트코인에 일정한 경제적 가치를 부여하는 것을 전제로 하는 다양한 경제활동이 이루어지고 있음.

⑤ 몰수에 대한 해외 사례 존재(미국, 독일, 호주, 프랑스)

⑥ 피고인도 회원들로부터 취득한 비트코인 중 일부를 현금으로 환전하여 상당한 수익을 얻음

⑦ 압수된 비트코인을 몰수하지 않은 채 피고인에게 환부하는 것은, 사실상 피고인으로 하여금 이 사건 음란사이트 운영을 통해 얻은 이익을 그대로 보유하게 하는 것으로 범죄수익은닉의 규제 및 처벌 등에 관한 법률의 제정취지에 비추어 보더라도 매우 불합리 함.

121

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례-대법원 2018. 5. 30. 선고 2018도3619 판결

- **사건 요지**

수원지방법원 2018. 1. 30. 선고 2017노7120 판결의 상고심

- **쟁점: 암호화폐가 재물성에 대해 인정**
  - '피고인이 범죄수익은닉규제법에 정한 중대범죄에 해당하는 정보통신망법 위반(음란물유포)죄와 도박개장방조죄에 의하여 취득한 비트코인은 재산적 가치가 있는 무형의 재산이라고 보아야 한다.
  - 재물성 인정 근거

① 비트코인은 경제적인 가치를 디지털로 표상하여 전자적으로 이전, 저장 및 거래가 가능하도록 한, 이른바 '가상화폐'의 일종임.

② 피고인은 음란물유포 인터넷사이트인 "OOOOOOO.com"(이하 '이 사건 음란사이트'라 한다)을 운영하면서 사진과 영상을 이용하는 이용자 및 이 사건 음란사이트에 광고를 원하는 광고주들로부터 비트코인을 대가로 지급받아 재산적 가치가 있는 것으로 취급하였음.

122

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례-코인원 사건-마진거래 도박개장죄

- **사안의 요지**
  - 수사기관: 경기남부지방경찰청 사이버수사대
  - 범죄(공소)사실: 도박개장 및 대부업법 위반 혐의
  - 적용법조항: 형법 제246조, 자본시장과 금융시장 투자업에 관한 법률
  - 경과: 대표등 3명 불구속 입건, 기소의견으로 검찰에 송치
- **문제점**

  쟁점 1. 암호화폐가 재물인가
  - '재물'로 '도박'한자를 처벌함.(형법246조) --> 암호화폐가 '재물'에 해당하는가?(수원지방법원 형사 8부 선고를 대법원이 확정한 가상통화 몰수 판결, 수원지방법원 2017노7120)
  - '재산'이란 사회 통념상 경제적 가치가 인정되는 일반을 의미함. 수원지방법원 판결을 통해 암호화폐(비트코인)가 사회 통념상 경제적 가치를 가지고 있다고 판단했음

123

II. ICO 관련 국내 소송 사례

블록체인 관련 법 적용 사례-코인원 사건-마진거래 도박개장죄

쟁점 2. 증권가의 신용거래 기법과 유사한 마진 거래가 '도박'에 해당하는지 여부

- 금융상품으로서 공매도를 인가받은 주식시장과 달리 암호화폐는 금융상품이 아니므로 도박죄 성립 여부가 문제됨
- 도박인지 아닌지 결정적인 쟁점은 ' 참가자들이 도금을 걸고 우연한 승부에 의해 재물의 득실이 결정되는지 ' 의 여부임
- 확실히 예견할 수 없는 ' 일주일 뒤 ' 의 암호화폐의 가격에 대해 회원들이 공매수와 공매도를 취하고 그에 따른 정산을 받았지만, 공매수자와 공매도자 이외에 일반 거래자가 혼재돼 있어 이 거래를 '도박참가자'들에 의한 거래로 보기 어려우며, 위험거래의 일종으로 보임
- 선물 거래는 증권이나 국채시장에서도 이루어지고 있지만 선물거래법, 증권법 등 금융위원회의 허가를 받아야 함(한국거래소의 허가 없이 사설 선물거래 사이트를 운영하는 자를 자본시장과 금융투자업에 관한 법률 위반과 도박개장죄(형법247조)로 처벌)

124

블록체인 관련 법 적용 사례-코인원 사건-마진거래 도박개장죄

쟁점 3. 대부업법 위반 여부

- "마진거래는 투자 원금의 최대 4배까지 투자할 수 있게 하는 방식이었음"
- 당국의 허가를 받지 않은 상태에서 돈을 빌려준 것으로 볼 수 있는지 법률 검토 중
- 코인원 측은 이자를 받지 않았기 때문에 대부업이라고 보기 어려움

125

III. ICO 관련 해외 소송 사례

126

III. ICO 관련 국내 소송 사례

미국 Maksim Zaslavskiy 사건- 불법 무기명증권 및 사기혐의

- **사안 요지**
  - 수사기관: 증권거래위원회 (SEC)
  - 범죄(공소)사실: 불법 무기명/미등록 증권 (unregistered securities) 오퍼 (offer) 및 사기
  - 적용법조항:
    - 증권법 (Securities Act) 17조 (a), <사기성 주간 (interstate) 거래 위반>
    - 증권거래소법 (Securities Exchange Act) 10조 b항, <조작 및 기만한 장치 사용 규제> 위반
    - 증권거래소법 Part 240, <일반 규칙 및 규정> 10b조 5항, <조작 및 기망적인 장치 사용> 위반
    - 증권법 5조 (a)&(c)항, <무기명/미등록 증권 오퍼> 위반
  - 경과: Maksim Zaslavskiy 대표는 사기 및 증권거래법 위반으로 불구속 기소되었으며, 현재 소송 진행 중
  - 2019년 1월 7일 배심재판 예정

127

III. ICO 관련 국내 소송 사례

미국 Maksim Zaslavskiy 사건- 불법 무기명증권 및 사기혐의

- **문제점**

A. Zaslavskiy는 본인 명의로 REcoin Group Foundation, LLC 와 DRC World, Inc. (Diamond Reserve Club)을 설립하여 ICO를 개최 함.

REcoin은 부동산, DRC는 다이아몬드 투자로 부터 이익이 창출될 것으로 홍보 함.

SEC측은 관련 사업내용을 검토하여, 본 ICO는 증권에 속하는 것으로, 무기명증권, 또는 미등록 된 증권으로 간주되어 증권법 위반으로 기소 함.

B. 피고인은 투자자들에게 다음과 같은 허위진술을 한 것으로 나타남:

1.가상 토큰 또는 코인을 발행하지 않았음에도 불구하고 토큰 또는 코인을 구매하는 것이라고 속임.

2.REcoin의 경우, 30만 달러의 투자금액 밖에 모으지 못 했음에도 불구하고, 투자자들에게는 2백만, 향후 4백만 달러에 가까운 자금을 모았다고 허위 진술함.

3.투자자금을 변호사, 브로커, 회계사, 또는 타 전문가를 통해 위치하거나 투자하지 않았음.

4.수익을 보장한 것과 다르게, 위 두 회사는 사실상 운영되지 않았고, 이 때문에 투자자들에게 수익을 남겨 주지 못 했으며, 이 점을 피고인은 이미 알고 있거나 무모히 무시했음.

128

III. ICO 관련 국내 소송 사례

미국 Maksim Zaslavskiy 사건- 불법 무기명증권 및 사기혐의

- **개선방안: ICO는 과연 증권인가, 아니면 화폐 또는 상품인가?**
  - 아직까지 ICO또는 가상화폐는 증권으로 분류 또는 인정되지 않아서, 증권거래법 규제를 회피해 왔음.
  - 피고측은 미국 법원 판례상 가상화폐는 증권이 아닌, 상품으로 구분되었다고 주장 함.
    - 2018년 3월, 미국 상품 선물 거래 위원회가(CFTC) 가상화폐에 관할권을 제시 및 요구하자, 연방법원 판사, Jack B. Weinstein 판사는 CFTC의 관할권을 공인하며 가상화폐를 상품으로 분류 함.
  - 반면, 증권거래위원회는 ICO의 경우, 가상화폐는 증권의 성향과 유사하다고 주장 함.
    - 위 재판 당시, Weinstein판사는 가상화폐의 용도(예: ICO)에 따라 증권에 가깝다는 점을 고려하여, 증권거래위원회의 관할 또한 인정한바 있음.
  - Pepper Hamilton LLP의 Gregory J Nowak & Joseph C Guagliardo (기업 관리 규범 및 금융규제 하버드 로스쿨 포럼, Harvard Law School Forum on Corporate Governance and Financial Regulation 출처)에 따르면, 가상화폐가 증권으로 분류될 경우, 향후 가상화폐의 용도가 제한될 것으로 예상됨. 특히 ICO의 경우, 토큰 또는 코인을 기명식 유가증권으로 등록해야 할 것이며, 이를 우회하기 위해선 미국 관할지역 외 해외에 소재한 투자자를 겨냥해야 할 것으로 예상함.
  - 본 사건과 같은 소송을 방지하기 위해선 ICO가 증권과 유사한지 파악해야 하며, 본 업무는 법률대로 소비자 또는 투자자가 아닌, 제안자(offeror)의 몫으로 알려져 있음. 하지만 제안자가 투자금액을 갖고 탈주할 경우 기소 및 고발이 어렵기에 소비자가 이 사항을 유의해야 함.

129

III. ICO 관련 국내 소송 사례

미국/캐나다 Dominic Lacroix 사건 - 사기혐의

- **사안의 요지**
  - 수사기관: 증권거래위원회 (SEC)
  - 범죄(공소)사실: 사기혐의
  - 적용법조항:
    - 증권법 (Securities Act) 17조 (a), <사기성 주간 (interstate) 거래 위반>
    - 증권거래소법 (Securities Exchange Act) 10조 b항, <조작 및 기만한 장치 사용 규제> 위반
    - 증권거래소법 Part 240, <일반 규칙 및 규정> 10b조 5항, <조작 및 기망적인 장치 사용> 위반
    - 증권법 5조 (a)&(c)항, <무기명/미등록 증권 오퍼> 위반
  - 경과: ICO 중단, 사기 및 증권거래법 위반으로 불구속 기소.
  - 현재 캐나다에 거주 중, SEC측은 미국 법원으로 부터 피고인 증언 통고를 확보한 상태임.

130

III. ICO 관련 국내 소송 사례

미국/캐나다 Dominic Lacroix 사건 - 사기혐의

- **문제점**

A. 피고인은 캐나다에서 여러 차례 전과가 있는 금융 상습범으로 알려져 있어, 과거 사례 때문에 미국 증권거래위원회에서 더욱 심혈을 기울임. (이 부분은 생략해도 무관함)

B. 가상화폐 PlexCoin으로 ICO를 추진하여 $1천 5백만 달러의 투자금을 챙긴 혐의.

1. PlexCoin은 피고인이 설립 및 운영한 PlexCorps 비법인 회사의 가상화폐로, SNS 페이스북을 통해 홍보됐으며, 마케팅 당시, 세계적인 가상화폐가 될 것이라고 선언하였으며, 가상화폐의 이용도 및 사용자 수를 늘리는데 중점을 둔다고 제시함.
2. 이어, PlexCoin 투자 시, 투자 기간에 따라 29일 안에 1,354%, 629%, 332%, 또는 200%에 달하는 수익률을 홍보하며 투자자들에게 상당한 이익을 보장함. 이렇게 $1천 5백만 달러의 투자금을 부성실히 걷음.
3. 또한, 본 회사는 전세계 48명 이상에 다달하는 직원을 고용하며 성장하고 있다고 허위주장 함.

C. 캐나다 법원 관할 하에 법적 징계(injunction 금지명령)를 받았으나, 이를 어기며 계속 ICO를 진행함.

D. 본 사건은 가상화폐 ICO에 있어 관할권이 개입된 사례로, 미국증권위원회 또는 법원 측에 관할권이 있는지의 여부를 판정할 것으로 예상 됨.

131

III. ICO 관련 국내 소송 사례

미국/캐나다 Dominic Lacroix 사건 - 사기혐의

- **개선방안: 속인적 관할권의 적용범위**

- 피고인은 캐나다인. 미국에서 활동하지 않았음.
- 피고인측 주장: 미국 내에서 활동하지 않고 미국인과의 직접적 접촉이 없었기 때문에 미국 법원 또는 증권거래위원회는 기소할 권한이 없음.
- 증권거래위원회(SEC)측 주장: PlexCoin구매 내역 중 1,500여건이 미국인 투자자였으며, 페이스북에 개시된 글을 미국인 투자자들이 보고 투자할 가능성을 합리적으로 예측할 수 있었다고 주장하며, 속인적 관할권을 추구 함.
- 이어, SEC측은 역외적용을 제안 함. '인터넷 거래상 투자자 청구서 발송지가 미국일 경우 미국 증권법이 역외적용된다'고 발언 함 (관련 판례: *Morrison v. National Australia Bank Ltd.*, *United States v. Vilar*).
- 궁극적으로, 현재 사이버거래 및 투자는 미국 증권거래위원회가 향후 자주 직면할 수밖에 없는 것이며, 본 사건으로 인하여 미국 법 및 관할권이 어떤 방향으로 성장할 지가 쟁점임.

출처: *New Focus on Cryptocurrency, Familiar Questions of Jurisdiction and Territoriality*. New York Law Journal. <https://www.law.com/newyorklawjournal/2018/04/13/new-focus-on-cryptocurrency-familiar-questions-of-jurisdiction-and-territoriality/?slreturn=20180610011219>. 저자: Philip Patterson and Vera Kachnowski, De Feis O'Connell & Rose, P.C.

132

III. ICO 관련 국내 소송 사례

미국: SEC, 사기 ICO 하려 한 토마호크사 징계

- **개선방안: 속인적 관할권의 적용범위**

징계 대상: 토마호크라는 회사를 세워 ICO를 하려 한 데이비드 로란스

징계 이유:

- 원유 개발 허가를 받지 않았지만 받았다는 거지말로 투자자를 속였으며, 토마호크코인이라는 토큰을 판매하며 거짓 정보가 담기 홍보물을 만들어 배포했음
- 토마호크코인을 가지고 있으며 나중에 이를 주식으로 전화하거나 원유 올리는 수익을 일부 나누어 가질 수 있으며, 토큰 자체를 거래할 수도 있다고 거짓 선전했음

징계 내용:

- 로란스는 상장 기업의 임원이나 이사가 될 수 없으며, 투기에 쓰일 수 있는 저가주를 매입하거나 거래할 수 없었음.
- 이번 징계는 해제 시점이 없는 영구적인 징계임

미국 SEC의 충고:

- 석유나 천연가스와 관련한 전통적인 사기 수법에 블록체인이라는 혁신적인 기술을 어떻게든 엮어낸 사기가 많으므로 투자자들은 주의해야 함

133

IV. ICO 프로젝트 시 유의할 점

134

IV. ICO 프로젝트 시 유의할 점

ICO 프로젝트를 평가하는 7 가지 지표

재무 컨트롤
- 재무관리제도, 모집한 자금의 사용방안, 재무감독제도 평가
- 재무관리제도,자금의 유용 리스크 점검

프로젝트의 배경
- 프로젝트의 배경, 성질, 관련 법규 파악

프로젝트 백서
- 내용과 공시의 경로 분석
- 프로젝트의 핵심 경쟁력, 운영 메커니즘 파악
- 적당한 비전과 비즈니스 응용 시나리오 유무 확인

ICO 발행 방안
- ICO 발행 방안, 토큰의 성질, 자금의 사용 방안, 커뮤니티 홍보 활동 등 분석
- ICO 프로젝트의 합법성, 안전성, 투명도 평가

ICO 평가 7대 지표

프로젝트의 팀
- 프로젝트의 팀에 대한 파악을 통해서 팀은 불량 기록이 있는지 확인
- 기술 능력 수준과 팀의 종합적 능력을 평가함으로써 프로젝트의 성공의 가능성 평가

프로젝트 운영
- 프로젝트의 노선도, 공시된 정보와 치리 구조의 완전성 평가
- 프로젝트의 의사결정 방안 평가

pwc 普华永道

프로젝트의 코드
- 코드의 관리 메커니즘, 코드의 안전 심사 메커니즘 평가
- 프로젝트의 창조성, 안전성, 실행 가능성 평가

135

IV. ICO 프로젝트 시 유의할 점

ICO 기업들이 선호하는 국가?

평가할 ICO [사진=ICO 레이팅 제공]

스타트업 이름	스타트-엔트 ICO	하이프 스코어 ?	위험도 ?	간단 리뷰 ?
ValPromise (VPP)	04.07.2018 - 08.08.2018	중간	중간	REVIEW
Coinet (COT)	22.06.2018 - 28.07.2018	낮은	중간	REVIEW
Curaizon (CTKN)	08.06.2018 - 08.09.2018	낮은	중간	REVIEW
Foleum (FOL)	02.07.2018 - 31.10.2018	중간	중간	REVIEW
Namahe (NMH)	28.06.2018 - 31.07.2018	중간	중간	REVIEW
Joys Digital (JOYS)	21.06.2018 - 10.10.2019	낮은	중간	REVIEW
CryptoAds (CRAD)	16.06.2018 - 16.07.2018	중간	높은	REVIEW
AI Crypto (AIC)	04.06.2018 - 31.07.2018	중간	높은	REVIEW

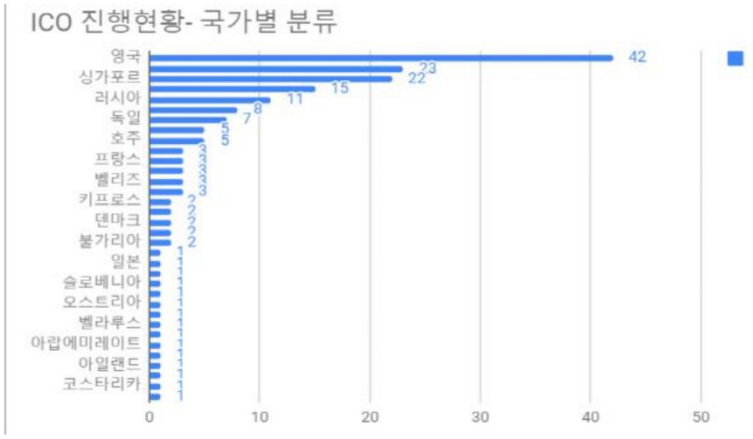
ICO 프로젝트를 확인해본 결과 413개 중 42개 업체가 영국령을 선호한 것으로 알려짐

<출처: http://decenter.sedaily.com/NewsView/1S221WVJM8, [ICO 트렌드 전수조사]①美 규제에 영국령 찾는 발걸음 늘었다 김연지 기자, 2018. 7. 12.>

136

IV. ICO 프로젝트 시 유의할 점

ICO 진행 현황-국가별 분류



ICO가 진행되는 국가들. 미상으로 기재한 국가(233개) 제외

<출처: http://decenter.sedaily.com/NewsView/1S221WVJM8, [ICO 트렌드 전수조사]①美 규제에 영국령 찾는 발걸음 늘었다 김연지 기자, 2018. 7. 12.>

IV. ICO 프로젝트 시 유의할 점

TOKEN SALE 유의점-토큰 세일 단계별 유의점

- 암호화폐 모집 관련
  - 법정 화폐 또는 금융통화 상품으로 모집할 경우 자금 관련 규제 적용 위험
  - 모든 거래를 투명하게 준비하고 기록하는 것이 바람직
  - 한국인과 미국인의 ICO 참여를 금지하는 방안도 리스크를 피하기 위한 방법 중 하나
- 기부와 보상 구조로 계약서 작성 cf. SAFT
  - 싱가폴 법인은 MAS가 계약서 및 KYC 서류 제출 요구할 수도
- 토큰이 없는 상태에서 계약자 지위를 이전할 수 있으면 증권으로 간주될 위험이 상존함
- 국내 마케팅, 로드쇼
  - 외국 법인이 실체가 없을 경우 법인격 부인으로 국내에서 ICO한 것으로 간주될 가능성
- 수익에 대한 언급은 절대 자제
  - 다단계 판매망 활용시 무리한 수익 보장 약속으로 유사수신규제법 적용 가능성

IV. ICO 프로젝트 시 유의할 점

ICO시 체크리스트-국내법에 따른 규제 대비

- ICO 자체에 대한 규제
  - 현재 관련법이 부재함에 따라 불확실한 상황이 지속될 수 있으므로 가능한 규제에 대해 대비
  - 모든 거래를 투명하게 준비하고 기록하는 것이 바람직
  - 한국인과 미국인의 ICO 참여를 금지하는 방안도 리스크를 피하기 위한 방법 중 하나
- 암호화폐 거래소 관련 규제
  - KYC가 되지 않은 암호화폐의 상장 거절 가능성
- 외환관리법에 관한 규제
  - 해외 ICO 법인 설립시 해외투자신고
- 개인정보보호 관련 규제
  - 블록에 개인정보를 기록하는 모델은 개인정보보호법, GDPR 적용 국가 서비스 불가(개인정보 파기 의무 불가)

139

IV. ICO 프로젝트 시 유의할 점

ICO시 체크리스트-국내법에 따른 규제 대비

- 자금세탁방지법에 관한 규제
  - 관련 규정
    - ✓ 특정금융거래정보의 보고 및 이용 등에 관한 법률
    - ✓ 특정금융거래정보 보고 및 감독규정
    - ✓ 자금세탁방지 및 공중협박조달금지에 관한 업무 규정
    - ✓ 공중협박자금조달금지법
    - ✓ 범죄수익규제법
  - 자금세탁방지법 내용 : KYC(Know Your Customer), 고객확인제도(CDD), 강화된 고객 확인제도(EDD)
- 기타 ICO 대상인 암호화폐의 특성상(특히 utility token) 관련되는 규제 검토
  - 신용평가업에 관한 규제, 개인신용정보에 관한 규제, 보험업에 관한 규제, 거래소 관련 규제 등

140

IV. ICO 프로젝트 시 유의할 점

ICO시 체크리스트-사기(Fraud)성 Scam으로 오인 방지

- 백서
  - 제시된 사업모델이 합리적인지, ICO 후 충실시 백서에 따라 개발 중인지
  - 개발팀, 어드바이저의 경력이 사실인지, 실제로 기여하고 있는지
- 암호화폐 모금
  - 모금상황을 사실대로 공시했는지, 부풀리거나 축소하지는 않았는지, Hardcap을 인위적으로 채우지 않았는지(자전거래 등)
  - 유사수신, 불법 다단계 조직을 이용한건 아닌지
  - 목적외 이용하고 있지 않은지(횡령, 배임)
- 암호화폐 발행
  - 충분히 개발능력이 있는지, 팀원은 역량이 있는지
  - 개발이 지연되는 사유는 타당한지
  - 정보보호를 잘 준수하고 있는지

141

IV. ICO 프로젝트 시 유의할 점

ICO시 체크리스트-전세계 주요국가의 규제 검토

- 미국법에 의한 규제
  - SEC에 적격투자자만 참여시키는 증권발행으로 등록하여 ICO를 시행하는 방법
  - 미국인의 ICO 참여를 금지하고 미국 거래소 상장 포기
  - SAFT에 대해서도 SEC는 불명확한 입장
  - 미국 거래소 상장 포기
- 기타 각국의 규제
  - 싱가폴 : Terms of Sales 등 ICO 관련 서류 철저히 요구
  - 스위스 : 비영리 법인(Foundation)에 대한 감독 강화, 감사보고서 요구

142

IV. ICO 프로젝트 시 유의할 점

ICO 진행 시 염두해야 할 법적 쟁점-자본시장법 적용 가능성

○ 자본시장과 금융투자업에 관한 법률이 적용될 지 살펴볼 필요

➢ 토큰이 투자계약 증권에 해당되는지를 살펴볼 필요

➢ 크라우드펀딩 관련 규제 적용 가능성 여부 살펴볼 필요

미국 SEC→다오 토큰을 투자 계약 증권에 해당함

▪ 토큰이 투자계약 증권에 해당한 경우?

자본시장법 제119조에 의해 토큰을 발행하고자 하는 사업자가 50명 이상의 일반투자자를 대상으로 모집할 경우 증권신고서 제출 등 공모에 관한 규제를 받을 수 있음

온라인소액투자중개업자 : 채무증권 ·지분증권 ·투자계약 증권의 모집 또는 사모를 중개하는 자(자본시장법 제9조 제27항)

→ 토큰을 중개해 소액투자자들과 연결하는 서비스인 경우: 온라인소액투자중개업에 대한 규제 살펴볼 필요

143

IV. ICO 프로젝트 시 유의할 점

ICO 진행 시 염두해야 할 법적 쟁점-외국환거래법 적용 가능성

➢ 국내 참여자가 해외에 근거지를 둔 ICO 발기인에게 비트코인 등의 암호화폐 또는 법정화폐를 보내고 ICO를 통해 발행된 코인이나 토큰을 취득할 때

➢ 국내에 근거지를 둔 ICO 발기인이 코인이나 토큰을 해외로 송금할 때

144

IV. ICO 프로젝트 시 유의할 점

ICO 진행 시 염두해야 할 법적 쟁점-유사수신행위 규제에 관한 법률 적용 가능성

유사수신행위란?

→ 다른 법령에 따른 인가·허가를 받지 않고 등록·신고 등을 하지 않고 불특정 다수인으로부터 자금을 조달하는 것을 업(業)으로 하는 행위로 장래에 출자금의 전액 또는 이를 초과하는 금액을 지급할 것을 약정하고 출자금을 받는 행위 등을 의미함

예로:

원금 보상 약정이 있음

출자금 반환 약정이 있음

ICO 과정 중에 사업자가 백서를 통해 과도한 기대 수익을 보장하거나, 실제 기술 자체가 구현 불가능함에도 구현이 가능한 것처럼 투자자를 오인하도록 했으면

➢ 사기죄 문제

145

IV. ICO 프로젝트 시 유의할 점

ICO 진행 시 염두해야 할 법적 쟁점-방문판매 등에 관한 법률 적용 가능성

146

부록1.G20 재무장관회의와 암호화폐 논의 동향

147

1. 2018년 3월 부에노스아이레스 회의 각국의 주된 관심사
2. 2018년 7월 부에노스아이레스 회의 각국의 주된 관심사
3. G20 국가 암호화폐에 대한 태도
4. AML 관련해서 국제기구의 동향
5. 한국 정부의 선택

148

1. 2018년 3월 부에노스아이레스 회의 각국의 주된 관심사

2018.03.19~03.21

회의 요지:

- ➢ 규제 조치는 잠정 보류하나 암호화폐의 위험성은 검토해야 함
- ➢ 암호화폐를 **디지털자산**으로 표기, 사실상 자산으로 분류한 것으로 확정됨
- ➢ 소비자, 투자자 보호 취약성, 조세회피와 범죄악용 가능성 관련 논쟁이 있다는데 공감대를 형성하였고 **7월**까지 각국이 별도 자산 규정안 마련
- ➢ 소비자와 투자자 보호, 시장 신뢰성, 자금세탁, 테러리스트 자금 조달 관련 문제를 중점 고려
- ➢ 자금세탁과 테러 자금 조달에 대항하기 위해 설립된 **재무대책특별위원회(FATA)** 기준을 디지털자산에 적용

149

1. 2018년 3월 부에노스아이레스 회의 각국의 주된 관심사

암호화폐에 대한 국제기구 논의사항

□□	□□□□	□□□□
5.8 □□□ □□	IOSCO	- □□□□ □ ICO□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□
6.24 □□□ □□	FATF	- □□□□ □□□□ □□ - □□□□ □□ □□ □□□□ □ □□□□ □□ □□ - □□□□ □□ □□□□ □ □□ □□ □□ □□ □□□ G20 □□□□ □□ □□
6.25 □□□ □□	FSB	- □□□□□ □□□□□ □□□ □□ □□ - □□□ □ □□□ □□, □□□□ □ □□□□ □□ □□ □□
7.18	FSB	- G20 □□□□ □□□□ □□□□ □□ □□□□□ □□ - □□□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□ - □□□□ □□□□□, ICO □□, □□□□ □ □□□□□□ □□□□ □□, □□□□ □□□□ □□□□ □□□ □□□ □□ □□□□ □□

- *IOSCO: 국제증권관리위원회기구*
- *FATF: 국제자금세탁방지기구*
- *FSB: 금융안정위원회*

150

1. 2018년 3월 부에노스아이레스 회의 각국의 주된 관심사

회의 공식 발표문 Communique

We acknowledge that technological innovation, including that underlying crypto-assets, has the potential to improve the efficiency and inclusiveness of the financial system and the economy more broadly.
암호자산을 포함한 기술 혁신이 금융 시스템과 경제의 효율성 및 포괄성을 더 광범위하게 향상 시킬 수 있는 잠재성이 있다는 것을 인정한다.

Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing.
그러나, 암호 자산은 소비자 및 투자자 보호, 시장 무결성, 탈세, 자금세탁 및 테러자금조달과 같은 문제를 제기한다.

Crypto-assets lack the key attributes of sovereign currencies. At some point they could have financial stability implications.
암호자산은 기존 정부화폐의 핵심 속성이 없다. 어떤 시점에서는 암호자산이 금융 안정성에 영향을 미칠 수 있다.

151

1. 2018년 3월 부에노스아이레스 회의 각국의 주된 관심사

회의 공식 발표문 Communique

We commit to implement the FATF standards as they apply to crypto-assets, look forward to the FATF review of those standards, and call on the FATF to advance global implementation.
우리는 FATF 기준을 적용할 것을 약속하고, 본 기준에 대한 FATF의 검토를 기대하며, FATF에게 세계적인 구현을 촉구한다.

We call on international standard-setting bodies (SSBs) to continue their monitoring of crypto-assets and their risks, according to their mandates, and assess multilateral responses as needed.
우리는 국제표준화기구들(SSBs)에게 암호자산 및 암호자산의 위험성을 본 기관들의 목적에 따라 지속적으로 감시하며, 필요성에 따라 국제 다국적 대응을 평가해주길 요청한다.

152

2. 2018년 7월 부에노스아이레스 회의 각국의 주된 관심사

2018.07.23~07.24

요지:

- 본 회의는 무역 문제에 초점이 맞춰져 있었으며 암호화폐에 대해 실제적인 컨센서스를 이루지 못함
- 블록체인 기술이 장점과 위험성을 동시에 가지고 있다고 언급했음
- 암호화폐가 아직 글로벌 금융 안정에 위험을 끼치지 않지만 이를 주의할 필요가 있음
- 오는 10월에 암호화폐 시장에 대한 명확한 기준을 마련해 달라고 FATF에 요청했음
- 현재 각국의 관심사는 여전히 암호화폐의 동향과 AML분야의 암호화폐에 대한 틀의 구축에 있음

암호화폐 규제안은 10월 G20정상회담으로 미루어졌음

153

2. 2018년 7월 부에노스아이레스 회의 각국의 주된 관심사

회의 공식 발표문 Communique

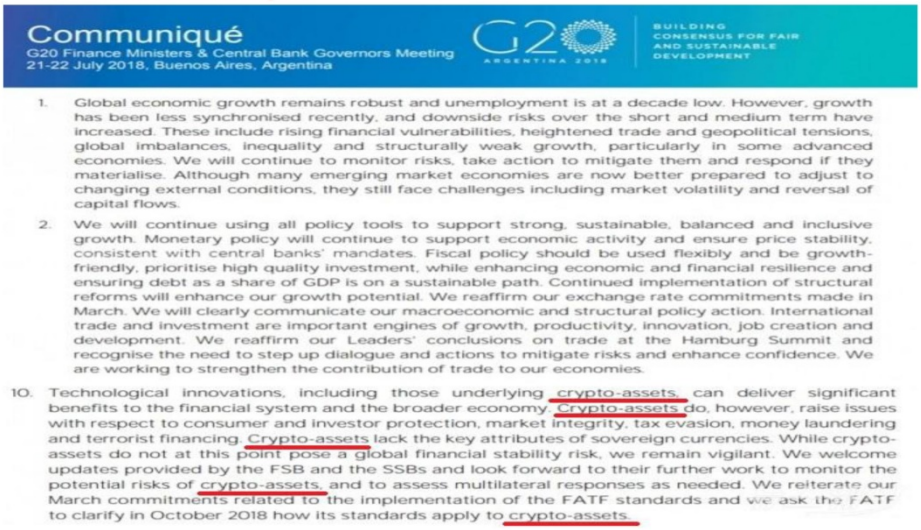
암호 자산(Crypto-assets)으로 용어 통일

- 공식발표문에서 Crypto-assets를 5회 언급했음
- 암호화폐를 통화로서의 속성이 부족하다고 함
- 투자자 보호, 세금 탈루, 자금 세탁, 테러 자금 조달 등의 문제가 여전함
- 다만, 주식, 채권 등을 대체할 수 있는 자산으로 발전할 수 있다고 함
- FATF가 암호자산의 권고기준을 10월까지 마련함

154

2. 2018년 7월 부에노스아이레스 회의 각국의 주된 관심사

회의 공식 발표문 Communique



Communiqué

G20 Finance Ministers & Central Bank Governors Meeting
21-22 July 2018, Buenos Aires, Argentina

BUILDING CONSENSUS FOR FAIR AND SUSTAINABLE DEVELOPMENT

1. Global economic growth remains robust and unemployment is at a decade low. However, growth has been less synchronised recently, and downside risks over the short and medium term have increased. These include rising financial vulnerabilities, heightened trade and geopolitical tensions, global imbalances, inequality and structurally weak growth, particularly in some advanced economies. We will continue to monitor risks, take action to mitigate them and respond if they materialise. Although many emerging market economies are now better prepared to adjust to changing external conditions, they still face challenges including market volatility and reversal of capital flows.

2. We will continue using all policy tools to support strong, sustainable, balanced and inclusive growth. Monetary policy will continue to support economic activity and ensure price stability, consistent with central banks' mandates. Fiscal policy should be used flexibly and be growth-friendly, prioritise high quality investment, while enhancing economic and financial resilience and ensuring debt as a share of GDP is on a sustainable path. Continued implementation of structural reforms will enhance our growth potential. We reaffirm our exchange rate commitments made in March. We will clearly communicate our macroeconomic and structural policy action. International trade and investment are important engines of growth, productivity, innovation, job creation and development. We reaffirm our Leaders' conclusions on trade at the Hamburg Summit and recognise the need to step up dialogue and actions to mitigate risks and enhance confidence. We are working to strengthen the contribution of trade to our economies.

10. Technological innovations, including those underlying crypto-assets, can deliver significant benefits to the financial system and the broader economy. Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing. Crypto-assets lack the key attributes of sovereign currencies. While crypto-assets do not at this point pose a global financial stability risk, we remain vigilant. We welcome updates provided by the FSB and the SSBs and look forward to their further work to monitor the potential risks of crypto-assets, and to assess multilateral responses as needed. We reiterate our March commitments related to the implementation of the FATF standards and we ask the FATF to clarify in October 2018 how its standards apply to crypto-assets.

155

2. 2018년 7월 부에노스아이레스 회의 각국의 주된 관심사

회의 공식 발표문 Communique

Technological innovations, including those underlying crypto-assets, can deliver significant benefits to the financial system and the broader economy.
암호자산을 비롯한 기술 혁신은 금융 체계 및 광범위한 경제에 상당한 혜택을 제공할 수 있다.

Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing. **하지만, 암호자산은 소비자 및 투자자 보호, 시장 무결성, 탈세, 자금 세탁 및 테러자금 조달 방지와 관련하여 문제를 제기한다.**

Crypto-assets lack the key attributes of sovereign currencies.
이어 암호자산은 기존 정부화폐의 속성을 지니지 않는다.

While crypto- assets do not at this point pose a global financial stability risk, we remain vigilant.
현재 암호자산이 글로벌 금융 체계의 안정성에 큰 위험요소로 보이지 않지만 우리는 여전히 암호자산을 경계하고 있다.

156

2. 2018년 7월 부에노스아이레스 회의 각국의 주된 관심사

회의 공식 발표문 Communique

We welcome updates provided by the FSB and the SSBs and look forward to their further work to monitor the potential risks of crypto-assets, and to assess multilateral responses as needed.
국제표준화기구들(SSBs)이 제공하는 업데이트를 환영하며 암호자산의 잠재적 리스크를 감시하고, 필요에 따라 다국적 협력에 대한 평가를 기대하고 있다.

We reiterate our March commitments related to the implementation of the FATF standards and we ask the FATF to clarify in October 2018 how its standards apply to crypto-assets.
G20은 FATF 표준의 이행과 관련된 3월의 약속을 다시 강조하며, 2018년 10월에 FATF가 본 기관의 기준이 암호자산에 어떻게 적용하는지 분명히 발표해주길 촉구한다.

157

3. G20 국가 암호화폐에 대한 태도

□□ □□/□□ □□	□□
□□□□/□□□□ □□, □□, □□ □□□	□□, □□, □□□□□
□□□ (intermediaries)□ □□ □□	□□, □□□, □□, □□□□, □□, □□□, □□
□□□□□ □□ □□ □□	□□□□□, □□□
□□ □□□	□□□, □□□, EU, □□□, □□□□, □□□, □□□□□□□□, □□, □□□, □□, □□

출처: FATF Report to G20 Finance Ministers and Central Bank Governors

158

3. G20 국가 암호화폐에 대한 태도

- **미국:**

➢ State별로 입장의 차이가 있지만 자금세탁 방지와 거래소 관리를 중시함
➢ 암호화폐를 화폐가 아니라 일반상품으로 규정해 소득세를 부과하고 있음
➢ 거래소가 자금세탁방지 의무를 가지고 있음.

- **중국:**

➢ 암호화폐 거래소 폐쇄 상태 유지
➢ 암호화폐 채굴에 세금 부과

- **일본:**

➢ Mt.Gox파산 그리고 Coincheck 해킹사건 이후 암호화폐 거래소에 존폐, 규제 등 논의가 끝이 없으며, 암호화폐 거래소 폐쇄 상태 유지중임
➢ 암호화폐 취급업소 등록제도 실시, 전세계 최초로 11개 암호화폐 거래소사업 승인
➢ 2017년 4월, 암호화폐에 대한 법 규제안이 통과하여 최소한의 규제만 적용되는 방향성을 나타냈으며, 암호화폐 채굴에 세금을 부과함
➢ 2020년 도쿄올림픽에 비트코인 거래 인프라를 구축할 예정임

159

3. G20 국가 암호화폐에 대한 태도

- **영국:**

➢ 암호화폐인 비트코인을 합법 화폐로 인정했음. 비트코인을 외화로 교환할 경우 부가가치세를 적용하지 않음
➢ 영국 중앙은행은 올해 내 국가가 지원하는 암호화폐 발행을 승인할 계획임
➢ 2015년부터 암호화폐와 블록체인 기술에 대해 적극적으로 연구해 왔음

- **브라질:**

➢ 브라질 정부가 암호화폐 투자로 인한 자금 유출 및 자금 세탁 등의 문제 때문에 국내 펀드업체가 암호화폐에 투자하는 것을 규제할 예정임

- **호주:**

➢ 투자자들을 보호하기 위해 자금 세탁 방지 및 대테러 자금 조달 개정안에 따라 암호화폐 거래소가 등록을 해야 하며, $10,000 달러 이상의 활동을 할 때 보고 의무가 따름

- **캐나다:**

➢ 비트코인 ATM의 수량(477개)은 미국(1800개)에 이어 전세계 2위를 차지함

160

4. AML 관련해서 국제기구의 동향

FATF가 G20에게 제출한 보고서

- FATF기준에 암호화폐 또는 가상화폐에 대한 정의 또는 적용범위가 불투명하여 지속적으로 검토할 예정임
- 10월 G20에 앞서 9월에 논의를 거쳐 FATF기준이 암호화폐/가상화폐에 어떻게 적용되는지 결론지을 예정임
- 현재 자금세탁방지 및 테러자금방지법을 우회하기 위해 수익소유자 (영문에서는 주로 실질상의 주주라고 풀이됨)를 대신하여 가상화폐/암호화폐 관련 사업을 해주는 대행업체 또는 전문가들 (법률 전문가, legal professionals)이 크게 가담하고 있으며, 특히 대행관련 업체(Trust and Company Service Providers, TCSP)들이 실질적 소유주주를 대신하여 ICO 또는 가상화폐/암호화폐 거래를 진행하는 것으로 나타남. 이에 따라 각국은 내국 중개업자에 대한 규정이 시급한 것으로 보임
- 자금세탁방지 및 테러자금방지법을 우회하기 위해 주로 쉘 컴퍼니(Shell company)를 규정이 미미한 관할국가에 설립함

161

4. AML 관련해서 국제기구의 동향

FATF가 G20에게 제출한 보고서

- FATF 조사에 참여한 국가중 17%가 AML/CFT (Anti-money laundering, Counter-terrorist financing) 체계가 구축되지 않은 상태로 자금세탁 및 테러자금조달에 취약한 것으로 나타남
- 몇몇 국가는 AML/CFT 규제를 암호화폐/가상화폐에 적용하고 있으며, 새로 입법 법안을 통해 규제에 나서는 국가들이 있지만, 각각 다른 규제방안을 사용할 것으로 예상됨
- 행정적 차이점 때문에 세계적인 글로벌 AML/CFT 규제를 구축하는데 어려움이 생길 것으로 예상됨
- 가상화폐/암호화폐 AML/CFT 규제에 대한 각 나라의 국회입법 절차도 요구되지만, 경찰과 같은 법 집행기관이 가상화폐/암호화폐에 대한 지식이 부족한 것으로 여겨지며, 특히 효율적인 법령을 개선하기 위해 가상화폐/암호화폐에 대한 법령을 정리하고 법원 판사 및 경찰이 새로 신설되는 기술에 대해 더더욱 숙지할 것을 추천함

162

4. AML 관련해서 국제기구의 동향

FSB가 G20에게 제출한 보고서

Financial Stability Board(FSB, 금융안정위원회)가 7월에 발표한 자료는 FSB, Committee on Payments and Market Infrastructures (CPMI, 지급 및 시장인프라 위원회), International Organization of Securities Commissions (IOSCO, 국제증권관리위원회기구), Basel Committee on Banking Supervision (BCBS, 바젤은행감독위원회)가 협력하여 진행된 업무로, 각 기구의 쟁점사항을 정리한 자료임.

FSB

- 3월에 개최된 G20를 결과로 FSB는 Standing Committee on Assessment of Vulnerabilities (SCAV, 취약성평가위원회)와 CPMI에게 암호자산에 대한 금융안정성 및 리스크를 감독할 수 있는 프레임워크를 계획하게 지시 및 승인함
- 본 프레임워크는 암호화폐로 인한 리스크를 바로 감지 및 선별할 수 있는 체제를 구성하고 해당 분석표(metrics)를 이용해 암호자산관련 산업마다 리스크를 관찰할 것으로 전망함 (예: 암호자산 성장률을 토대로 급속히 성장하는 암호자산 시장을 검토하고 급격히 하락하는 가치를 유의 및 방지할 수 있는 개념)
- FSB가 기존에 시행했던 ICO 감시체제는 불투명성 및 급격히 변화하는 암호화폐 시장 때문에 어려움을 겪음. 이와 같이 암호자산 역시 불투명성 및 시장 급성장 때문에 리스크를 항시 감시하는데 어려움을 겪을 것으로 예상 됨. 그러나 현재 개선된 감독방안은 기존 정책보다 비교적 효율적으로 사용될 것으로 전망함

163

4. AML 관련해서 국제기구의 동향

FSB가 G20에게 제출한 보고서

CPMI

- CPMI는 돈 지불(payment)에 있어 안정성과 효율성을 유지 및 개선하는 목적을 갖은 기관으로써, 돈 지불방법에 대한 연구를 이행함
- 특히 디지털 레저(digital ledger)는 광범위하게 사용될 수 있는 잠재력이 있는 점을 고려해 각 국가의 중앙은행마다 이를 인지하고 유의할 점을 촉구함. 이어 지난해 payment method(지불방법)에 대한 보고서를 여러 발표한 바 있음
- CPMI는 Economic Consultative Committee (ECC, 경제자문위원회)를 총괄하고 있으며, 디지털기술혁신이 기존 금융시장인프라에 미치는 영향을 검토하고 있음
- 본 기관은 cross-border payment (국경을 넘는 지불금)에 사용되는 암호화폐/토큰의 효율성과 리스크를 검토한바 있으며, 이러한 기술개발로 인해 각 당국 중앙은행에게 문제점 및 리스크를 선사할 것으로 예상됨. 특히 기존 화폐와 다르게 디지털 토큰은 기반 자산이 없기 때문에 각 토큰의 가치에 대한 위험성이 있음
- 본 기관은 앞으로 각국 중앙은행에게 디지털 토큰 및 암호화폐에 대한 유의점을 공지할 것으로 예상하며, 국경을 넘는 디지털 토큰의 사용을 감시할 예정임.

164

4. AML 관련해서 국제기구의 동향

FSB가 G20에게 제출한 보고서

IOSCO

- IOSCO는 2017년 11월에 각 당국정부마다 ICO에 적용하고 있는 규제 및 ICO의 위험성에 대해 발표한바 있으며, 올해 1월에 또 한번 본 기관의 염려를 대중에게 표한바 있음
- ICO Consultation Network (자문 네트워크)를 설립하여 해당 멤버들이 ICO와 관련된 유의사항 및 의문점을 논의하도록 요청 함
- 2018년 5월, 본 기관은 해당 회원이 ICO에서 발생하는 위험에 대한 규제 및 문제 (내국 및 외국 관할지역 포함)를 해결하는데 유용한 정보를 제공 할 수 있는 Support Framework (도움 프레임워크)를 설립하기로 함.
- 본 프레임워크는 ICO Consultation Network를 통해 취합한 내용을 토대로 제공할 것으로 예상함
- 특히 기존 금융시장과 ICO의 차이점에서 발생하는 의문점 및 내용을 회원 국가에 제공하여 이 차이점을 개선해 나아가는 방법을 마련할 수 있을 것으로 보임.

165

4. AML 관련해서 국제기구의 동향

FSB가 G20에게 제출한 보고서

- **IOSCO**
  - 암호자산 플랫폼이 생성되고 성장하고 있는 추세이며, 거래되고 있는 암호자산이 어떤 유형인지가 주 쟁점일 것으로 보임. 이어 암호화폐 거래소는 기존 법을 준수하지 않을 수도 있으며, 기존 감독기관들은 암호화폐 등의 시장을 접근하지 못할 수도 있음
  - 암호화폐 및 자산이 증권형으로 분류될 수 있는지 검토할 예정임
  - 위 사항 외 4개의 요소를 검토할 예정임: 투명성, 보관 및 청산 (custody and settlement), 거래 및 사이버 보안과 시스템 무결성
  - 이어 몇몇의 암호자산 플랫폼은 비중개된 방법으로 사용됨에 따라 이에 대한 안정성을 검토할 예정임

166

4. AML 관련해서 국제기구의 동향

FSB가 G20에게 제출한 보고서

- **BCBS**
- 본 기관은 세가지의 범주로 계획안을 세움

1) 암호자산과 관련된 은행의 직접적 또는 간접적 노출을 측정함
   a) 몇몇의 은행이 암호자산과 관련된 거래 및 연관된 사업에 어느정도 노출되어 있는지 지수로 나타낼 예정임

2) 암호자산에 노출되는 은행의 유의성 정책 (prudential treatment)
   a) 은행 유의/신중 행정상 암호자산을 어떻게 취급하는지. (위험한 자산을 어떻게 취급하는지 검토할 예정임)

3) 암호자산 및 FinTech 개발이 은행과 은행감독 기관에게 미칠 수 있는 영향 검토
   a) 2018.2 "Sound Practices on the implications of FinTech developments for banks and bank supervisors" 자료 발표함

167

5. 한국 정부의 선택

G20 재무장관 회의의 맥을 읽어라!

- G20에서 암호자산(Crypto-Assets)의 가치에 대한 인정에 주목
- 암호자산의 새로운 등장과 이를 중심으로 한 세계 각국의 포용적 입장 고려
- 기존 금융시스템의 단점을 보완하고, 앞으로 기술 발전에 따라 상당 부분 기존 금융시스템을 대체가능한 것으로 보아야 함

⇒ 암호자산에 대한 적절한 규제를 마련하고,
⇒ 암호자산취급업자들을 제도권으로 포용하는 입장 긴요

168

생각해봅시다

암호화폐 없는 블록체인, 과연 현실성이 있나

169

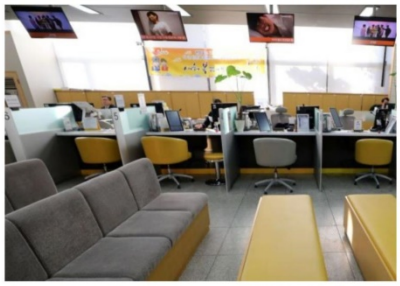
암호화폐 없는 블록체인, 과연 현실성이 있는가

정부는 암호화폐는 규제하고 블록체인은 진흥하겠다는 입장

은행권, '코인은 NO, 블록체인은 OK'

팍스넷뉴스 | 2019.03.11 14:26 | 댓글 0

[블록체인동상이몽]① 신규 계좌발급 동결 vs. 블록체인 서비스 상용화 준비 착착



[팍스넷뉴스 공도윤 기자] 블록체인과 암호화폐는 불가분의 특성을 가지고 있다. 블록체인 시스템 유지를 위해서는 자발적 참여자가 필요하고, 참여자에 대한 보상으로 암호화폐(코인)가 발행되기 때문이다. 탈중앙화의 가치 역시 코인 이코노미 생태계가 더해져야 의미가 있다.

하지만 정부와 금융당국은 일단 블록체인과 암호화폐를 떼어내고 보기로 한 듯 하다. 얼어붙은 블록체인 시장은 정부 지원 속에 녹고 있지만 여전히 ICO(암호화폐공개)나 코인거래는 여전히 동결된 상황이다.

170

<출처 : "은행권, '코인은 NO, 블록체인은 OK'", 공도윤 기자, 2019.3.11., 팍스넷뉴스>

생각해봅시다

암호화폐 없는 블록체인, 과연 현실성이 있나

- 블록체인 노드 운영의 원동력은 채굴의 보상으로 주어지는 암호화폐인데, 암호화폐 없이 탈중앙화 생태계 유지가 가능한가?

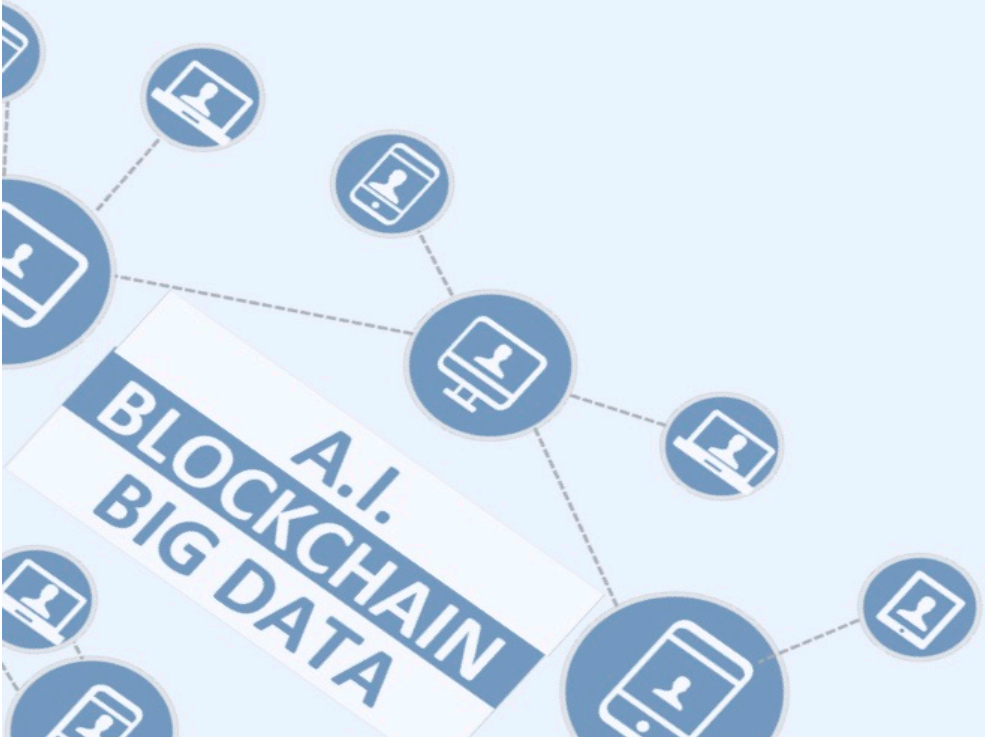
171

12강

Cryptocurrency and Regulation

황 경 태 변호사

(법무법인 헤리티지)



강의 동영상 URL

1 부: https://youtu.be/GM3y_1nyw4E

2 부: https://youtu.be/QBMYVttYTGg

법무법인 헤리티지
HERITAGE LAWFIRM

Cryptocurrency and Regulation
with Financial background

변호사 황경태

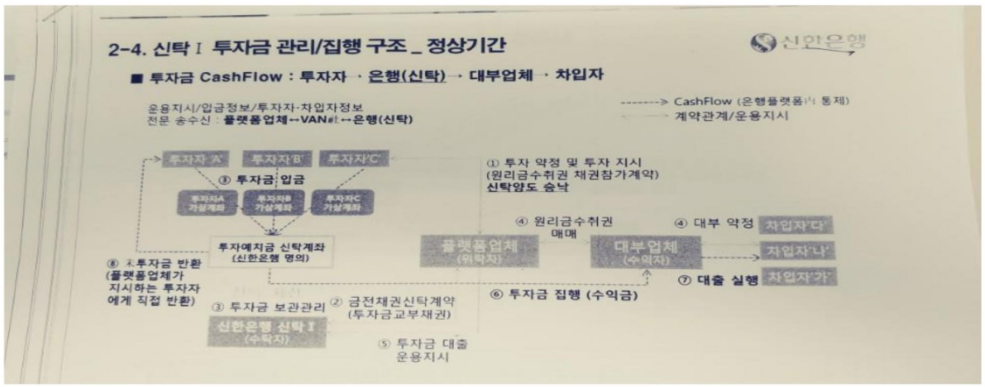
(kyoungtae.hwang@heritagelaw.co.kr ; 010-7220-3209)

Dream

1. Why 'Security'?

- Case analysis "Billy"(2019고합63)

  - Business Model (Real estate investment + p2p loan) https://www.villy.co.kr/



1. Why 'Security'?

- 10 mon. investigation by Seoul Nambu district Prosecutor office(special team for security crime)
- In Jail and being indicted on March 2019.
- Over 68,000 victim, 16 million usd damage

1. Why ‘Security’?

1. Why ‘Security’?_빌리 사태의 분석_제주 테라하우스

- **사실관계**

1. 기한이익을 최초로 상실하고도 3개월이라는 유예기간을 주고 강제집행(차주 및 연대보증인 자산압류)을 집행한점은 위법성은 없는지요? 결국 차주 및 연대보증인은 이미 100일에 가까운 시간동안 자산을 다 빼돌렸으며 3개월이라는 유예기간이 지난 후 계좌를 압류했을 때 실익은 0이었습니다.

2. 빌리 답변이라는 파일을 보시면 제가 빌리측에 문의하고 답변을 받은 것입니다. 1차 투자자를 모집하는 과정에서 총 펀딩금액은 11억원이라 밝혔으며 투자자보호방법을 보면 ‘사업지 근저당 1순위’ 이었습니다. 약 11억원에 달하는 사업지를 1순위 담보로 해서 11억원을 펀딩하기에 이정도면 원금이 손실이 난다해도 크게 나지 않겠구나 판단하였고 위 사항들은 제가 투자를 하는데 많은 영향을 끼쳤습니다. 하지만 빌리는 이미 11억원을 모두 펀딩한 상태에서 1차 투자자들에게 알리지 않고 동일 담보에 동일순위로 2차 투자자를 모집, 6.5억원을 더 펀딩하였습니다. 이로인하여 1차투자자들은 가만히 앉아서 더욱 많은 위험을 떠안게 되었습니다. 이러한 일련의 과정속에서 위법성은 없은지요?

3. 투자자모집공고상 사업지 분석정보를 보면 사업자 자본투입금 15억원이 나와있습니다. 그렇다면 빌리로부터 빌린 17.5억에 본인 자본투입금 15억원을 합치면 32.5억이라는 자금이 투입되었는데 현재 삽질한번 하지 않은채 위 돈이 모두 증발하였습니다. 그리고 나서 현재 pf를 일으키기위해 1순위를 내놓아라고 하는 상황입니다. 사업자 자본투입금이 15억원이라는 것은 투자자들이 투자를 결정하는데 매우 큰 영향을 미치게 됩니다. 차주가 큰 금액을 투자하였으니 이 사업을 어떻게 해서든 성공시키겠구나 라고 생각이 들기 때문이죠. 하지만 제가 빌리측에 모든 투자금을 어디다 어떻게 썼는지 사용내역을 알려달라하니 그건 알려줄수 없다는 답변만 받았습니다. 그렇다면 빌리로부터 돈을 빌린 차주들은 그 자금을 아무곳에나 쓰고, 극단적으로는 돈세탁을 하게 되면 투자자들은 그 정보도 모른채 그냥 모든 손실을 떠안아야 하는지요? 빌리로부터 빌린 돈은 모두 건설자금이나 토지 매입자금이었습니다. 투자자를 모집할 때 자금의 목적을 분명히 밝혔습니다. 하지만 지금 와서 생각해보면 빌리로부터 빌린 돈을 차주가 투입한 자금을 대환한건 아닌지 하는 의심이 듭니다. 이러한 일련의 과정에서 위법성은 없는지요?

1. Why ‘Security’?_빌리 사태의 분석_주유소 투자건

- 상품설명서에는 대출자가 다수의 주유소이고,
  기름구매를 위해 대출된 것이며,
  금융사의 신탁과 카드 매출을 담보로 투자자를 모집했었습니다.

  하지만, 이 상품은 상품설명서에 언급된 도표와는 다른 구조로 계약이 되어있는 것 같습니다.
  빌리 측에 방문면담하여 담당자로부터 들었던 내용은, 빌리-각 주유소들과 계약, 빌리-자산운용사간 계약, 자산운용사-각 주유소들과 계약으로 되어 있으며, 자금 흐름은 다음과 같습니다. 빌리에서 각 주유소들로 대출, 각 주유소들은 자산운용사로 카드매출금? 전달, 자산운용사에서 빌리로 원리금 상환

  자산운용사는 카드단말기 업체로 알고 있으며, PG사 법인을 설립한다고 자금을 빌리로 회수시키지 않았다하여(빌리 측 추정) 사기죄로 형사고소하였고, 형사조정 진행됐고 결렬돼서 기소여부를 기다리는 상황으로 알고 있습니다.
  빌리는 원리금 상환이 되지 않는 책임을 전적으로 차주에게 돌리며, 법적으로 압박하여 차주에게 받아낸 후 투자자들에게 상환하려 하고 있으며, 이 과정에서 얼마나 시간이 걸릴지 모르는 투자자들은 금전적 정신적 피해와 고통을 받고 있습니다.

  차주(자산운용사)가 사기를 쳤든 안쳤든, 빌리는 불완전하고 허위상품으로 투자자들을 속인 것에 대해서 투자자들에게 우선 보상해야할 것입니다. 빌리측에 핵심 요구사항은 "불완전 금융상품 판매를 진행한 빌리는 잔여원금 상환 및 연체이자를 전액 지급하라" 입니다.

1. Why ‘Security’?_자본시장법 적용가능성

- 자본시장법상 금융투자상품이란?

  이익을 얻거나 손실을 회피할 목적으로, 현재 또는 장래의 특정시점에 금전등을 지급하기로 약정함으로써 취득하는 권리로서, 그 권리를 취득하기 위하여 지급하였거나 지급하여야 할 금전등의 총액이 그 권리로부터 회수하였거나 회수할 수 있는 금전등의 총액을 초과하게 될 위험(투자성)이 있는 것(자본시장법 제3조 제1항)

- 자본시장법상 채무증권?

  증권이란? 금융투자상품으로서 투자자가 취득과 동시에 지급한 금전등 외에 어떠한 명목으로든지 추가로 지급의무를 부담하지 않는 것(자본시장법 제4조 제1항)

  그 중 채무증권은 발행주체, 담보 및 보증유무, 상환기간의 장단기, 이자지급방법이 정해진 것으로 지급청구권이 표시된 것으로 P2P회사의 원리금수취권이 이에 해당할 수 있다.(고동원, 인터넷상에서의 개인간(P2P) 금융거래에 관한 법적연구)

- 자본시장법상 투자계약증권?

  영국과 미국의 경우 한국과 구조가 흡사한 간접중개형 P2P의 경우 원리금수취권채권을 증권으로 보아 증권법에서 규율하고 있다.(이성복, 자본시장연구원)

- 온라인소액대출중개업과의 비교

  대표적 업체인 와디즈 모델의 검토

  https://www.wadiz.kr/web/winvest/main?cateOfBsns=&securtType=%27bond%27,%27etc%27&incomeDeductYn=&growthStage=intrstRate=&expirationDate=&order=undefined

1. Why ‘Security’?_자본시장법 규정적용검토

결론적으로 정상적으로 진행되어 부실이 난 투자자의 손실의 경우, 사기나 횡령의 입증의 어려움, 그리고 금전소비대차계약이 아닌 투자자의 지위에서 반환이 어려운 경우들이라 하더라도, 자본시장법 적용으로 돌파구를 마련할 수 있음

- 자본시장법상 증권신고서, 투자설명서 제출 및 공시위반에 대한 책임(허위, 부실기재)- 민사상 불법행위 책임에 비해 유리, 안날로부터 1년의 제척기간

  자본시장법은 금융투자업자에게 투자자의 합리적인 투자판단 또는 해당 금융투자상품의 가치에 중대한 영향을 미칠 수 있는 사항을 중요정보로 정의하고 있으며 대법원은 이를 합리적인 투자자가 당해 유가증권을 매수 또는 계속 보유할 것인가 아니면 처분할 것인가를 결정하는 데 있어서 중요한 가치가 있는 정보, 바꾸어 말하면 일반투자자들이 안다고 가정할 경우에 당해 유가증권의 가격에 중대한 영향을 미칠 수 있는 사실을 말한다.

- 자본시장법상 부정거래행위(부정한 수단, 계획 또는 기교)에 대한 손해배상책임

2. The origin of ‘Security’?

- Bond

  - Italian Renaissance
  - Netherland v. Spain
  - Napoleonic Wars
  - Civil War in North America

2. The origin of 'Security'?

- Inc.

- Invention of Netherland
- VOC
- Bank and Stock Market

2. The origin of 'Security'?

- The Securities Act of 1933

- 4M → 18M (1900~1928)
- $50 billion (for 10yr after 1st World war)
- Half is worthless
- The two principle of Regulation

3. The medium of financial market

- Investment Bank
- The exchange
- What's the role?
- Conflict issue
- The possibility of cryptocurrency

4. The Exchange and Regulation

- The role of the Exchange

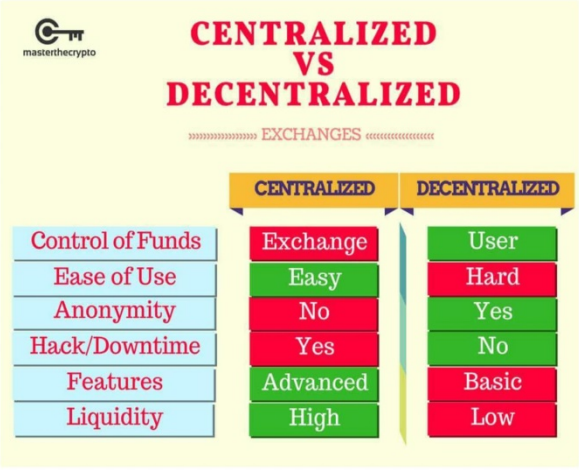
Centralized vs Decentralized

❏ Centralized Exchange

❏ Hanbitco / Bithumb / Coinone

❏ Decentralized Exchange

❏ Etherdelta



4. The Exchange and Regulation

Centralized Exchange

❏ 거래 프로세스

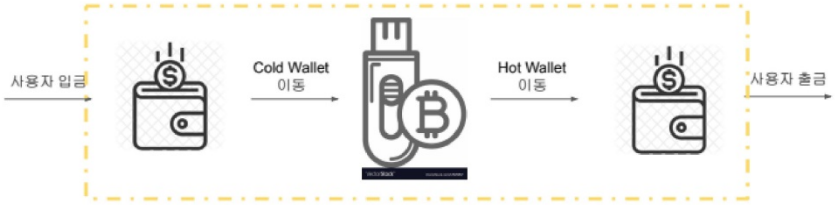
4. The Exchange and Regulation

Centralized Exchange

- ❏ Hot Wallet
  - ❏ Private Key가 Online에 보관되는 있는 지갑
  - ❏ Private Key의 형태 무관 (평문 / 암호화 된 Text / 암호화 된 File 등)
- ❏ Cold Wallet
  - ❏ Private Key가 Offline에 보관되는 지갑
  - ❏ USB / Paper Wallet / Etc.,

Centralized Exchange

❑ 지갑 관리 프로세스



Risks of the Exchange

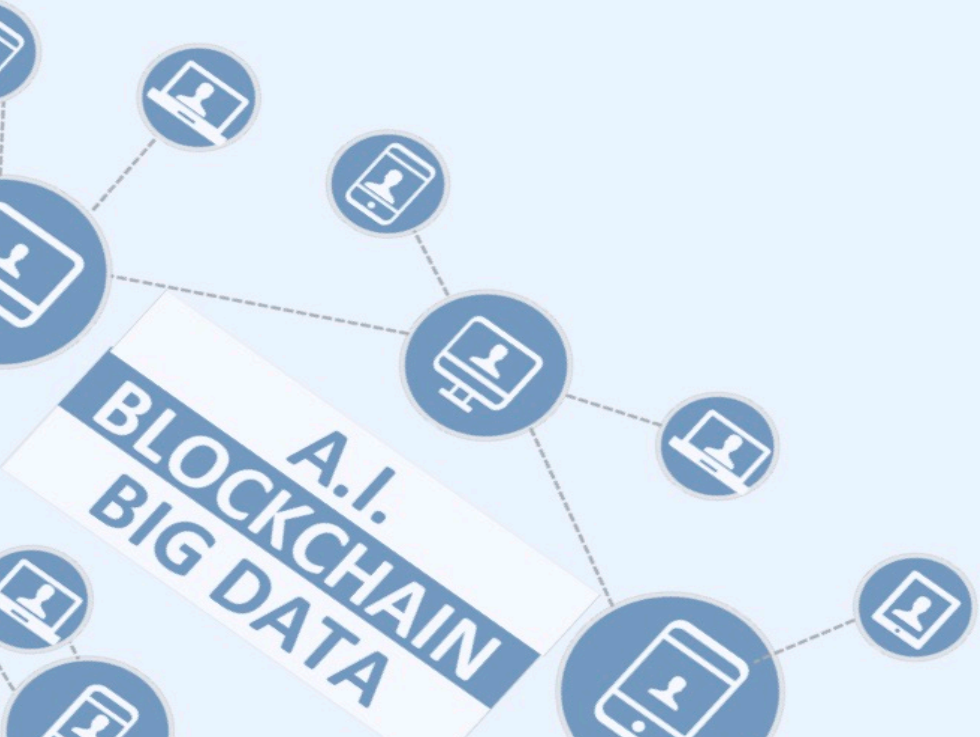
- Money laundering
- Security issue
- Transaction for oneself
- Manipulation

4. The Exchange and Regulation

- The BOOM in 2017
- The Guideline by FSS
- Control through Bank without Regulation
- Constitutional appeal(2017헌마1384)
- Bills

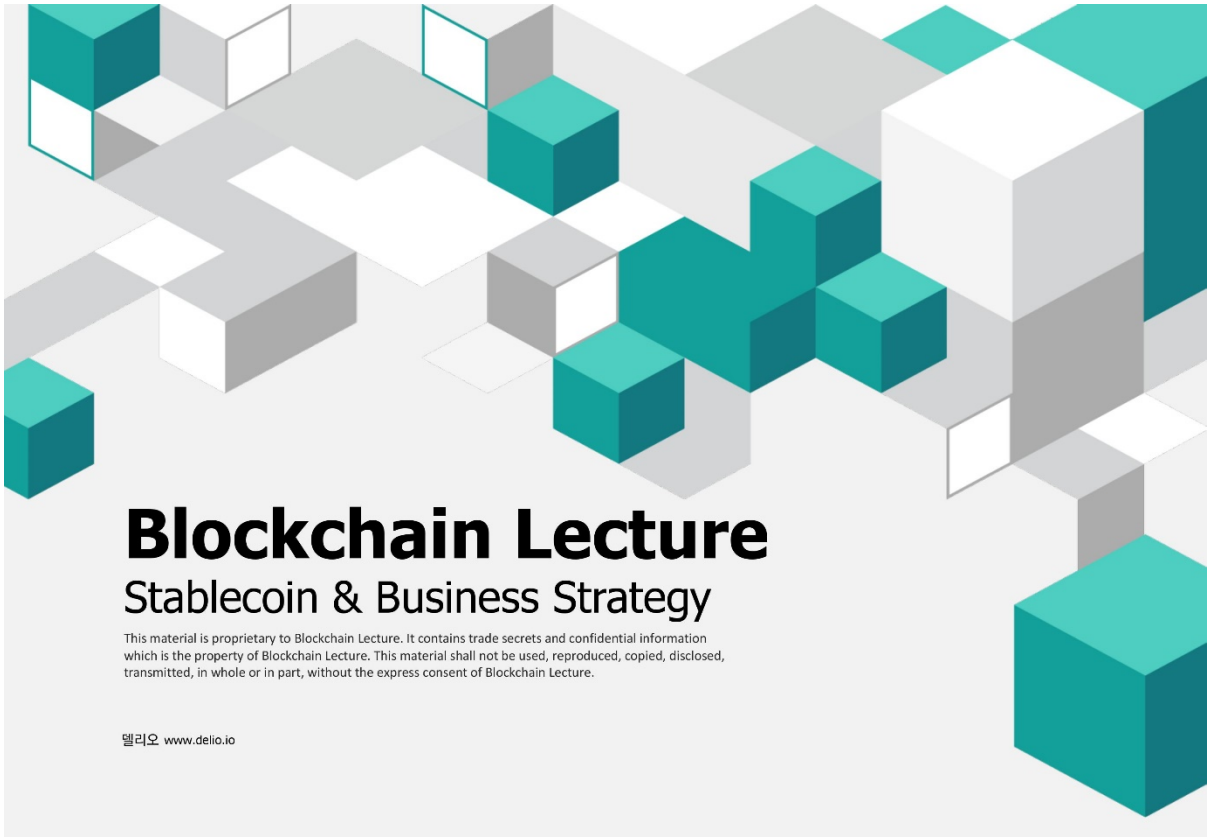
13강

Stablecoin & Business Strategy



정 상 호 대표

(주식회사 델리오)



Blockchain Lecture

Stablecoin & Business Strategy

This material is proprietary to Blockchain Lecture. It contains trade secrets and confidential information which is the property of Blockchain Lecture. This material shall not be used, reproduced, copied, disclosed, transmitted, in whole or in part, without the express consent of Blockchain Lecture.

델리오 www.delio.io

Table of Contents

This material is proprietary to Blockchain Lecture. It contains trade secrets and confidential information which is the property of Blockchain Lecture. This material shall not be used, reproduced, copied, disclosed, transmitted, in whole or in part, without the express consent of Blockchain Lecture.

01. Understanding Stablecoin

02. Business with Stablecoin

03. Q&A

Understanding CryptoCurrency

암호화폐 산업 이해하기

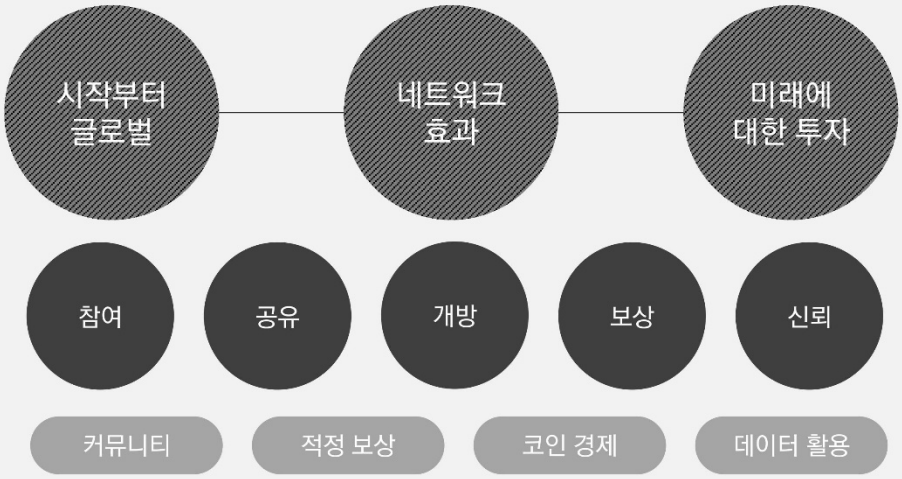
Understanding Cryptocurrency

왜, 블록체인 인가?

→ 기존 비즈니스의 한계를 뛰어넘을 수 있는 수단

Understanding Cryptocurrency

블록체인 비즈니스의 특징



Understanding Cryptocurrency

암호화폐 시장 규모는?

암호화폐 시가총액

암호화폐 전체 시가총액은 '300조원'
암호화폐 24시간 거래량 '95조원'

암호화폐 비즈니스

암호화폐에 가장 투자 많이 하는 국가 '미국,일본'
전체 암호화폐 개수 '2,200개'

Understanding Cryptocurrency

암호화폐 시장 규모는?

블록체인 성장율

블록체인 시장 **'연간 83%'**씩 성장
2018년 블록체인 투자액 '21억 달러(약2조)'

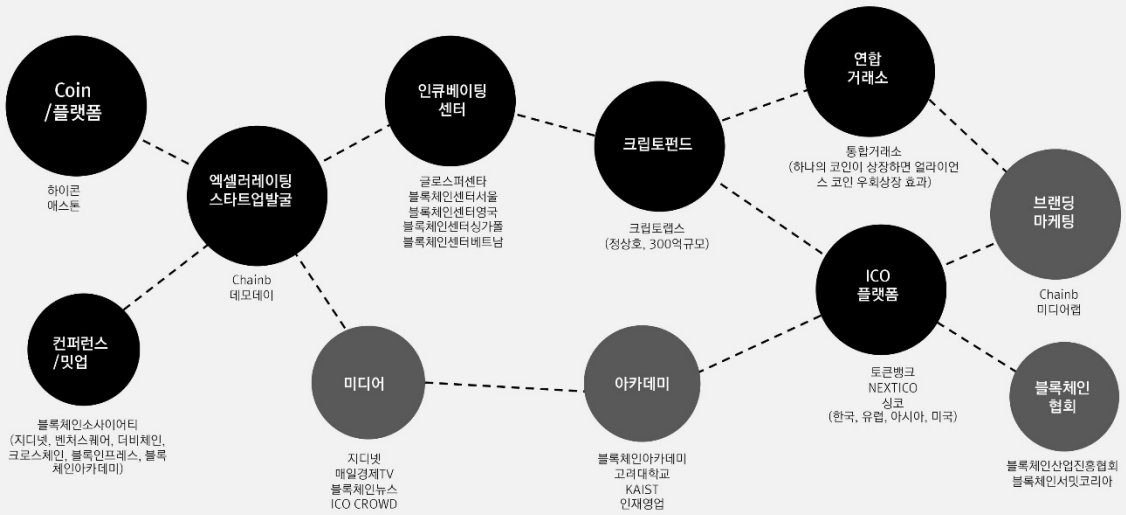
블록체인 시장규모

2025년 시장규모 '$ 1,760억원'
2030년 시장규모 '$ 3조 1천억'

Gartner

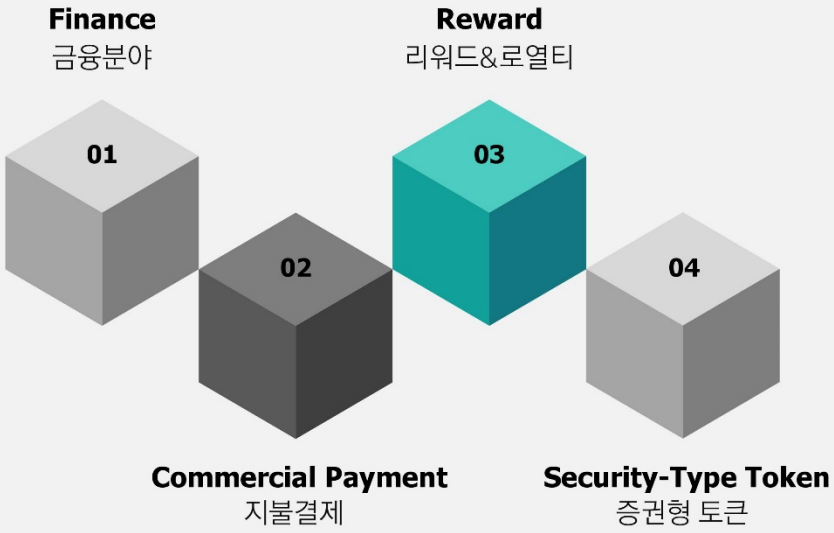
Understanding Cryptocurrency

암호화폐 관련 산업



Understanding Cryptocurrency

암호화폐 활용 분야는?



Understanding Cryptocurrency

블록체인이 비즈니스에 미치는 영향

By Authenticating Traded Goods

거래 상품을 인증함으로써 비즈니스 모델에 영향을 미친다.

By Facilitating Disintermediation

분산을 촉진하여 비즈니스 모델에 영향을 미칩니다.

By Improving Operational Efficiency

운영 효율성을 높여 비즈니스 모델에 영향을 미칩니다.
거래 소요 절차 등의 감소를 통한 효율성
작은 규모의 거래도 용이하게 함

→ 블록체인은 수많은 산업을 붕괴시킬 가능성이 있지만 CBInsights는 27개(CBInsights 블로그 2017)를 언급

Understanding Cryptocurrency

블록체인에 영향을 받는 기업들

...

[가장 영향을 많이 받는 곳은 **중계형, 서비스형** 산업
"3년 내 기업 세대교체 발생"]

Understanding Stablecoin

스테이블 코인 이해하기

Understanding Stablecoin

스테이블코인이란 무엇인가?

Bitcoin (BTC)

Tether (USDT)

Understanding Stablecoin

스테이블코인의 종류는?

1. **법정화폐 담보형 스테이블 코인**
   (Fiat-Collateralized Stablecoin)

2. **암호화폐 담보형 스테이블 코인**
   (Crypto-Collateralized Stablecoin)

3. **무담보 스테이블 코인**
   (Non-collateralized stablecoin)

Understanding Stablecoin

스테이블코인 사례와 비교

Project	Purpose	Decentralized	Stability	Investment Value	Payment Adequacy	Main-Net	Token based Ecosystem
Tether(USDT)	Exchange of Currencies	N	Y	N	N	Omni Layer Protocol (Bitcoin)	N
TrueUSD	Exchange of Currencies	N	Y	N	N	Ethereum	N
MakerDao	Exchange / Payment / Savings	Y	Uncertain	N	Y	Ethereum	N
Basecoin	Financial Services	Y	Uncertain	Y	N	Basis Protocol	N
Havven	Remittance	Y	Uncertain	N	N	Ethereum	N
Terra	Financial Infrastructure	N	Uncertain	Uncertain	N	Ethereum	Limited
Delio	**Commercial Payment**	**Y**	**Y**	**Y**	**Y**	**Independently Developed Main-Net**	**Y**

Understanding Stablecoin

스테이블코인은 상품권, 포인트와 어떻게 다른가?

No Costumer , Yes Participant

암호화폐가 상품권, 포인트의 한계를 넘어설 수 있도록 해주는 요소는
Blockchain, Programmable Money, Perfect Eco-system 이다

Business with Stablecoin

스테이블코인으로 비즈니스 하기

Business with Stablecoin

성공적인 블록체인 비즈니스 설계하기

- 원토큰 문제의 해결
- 기존 고객은 홀더가 아니다
- 토큰순환경제 생태계 구현
- 연합 생태계 구성의 중요성
- 프라이빗체인의 한계 극복
- 리워드형을 극복하자

Business with Stablecoin

비즈니스에 스테이블코인 적용 시 고려사항

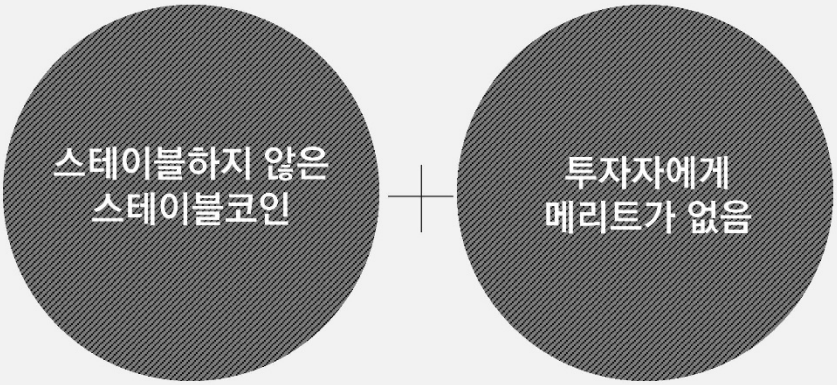
Business with Stablecoin

멀티토큰 모델의 문제점

Features 1	가격 안정화를 위한 멀티토큰 모델
Features 2	유틸리티와 시큐리티의 구분의 모호성
Features 3	토큰 또는 생태계 통합의 어려움
Features 4	부족한 토큰순환경제 생태계 구현
Features 5	폐쇄적인 생태계

Business with Stablecoin

스테이블코인의 문제점



Business with Stablecoin

스테이블코인을 비즈니스에 적용하기 어려운 이유

기업 및 소상공인들은 다양한 목적으로
토큰을 자사 비즈니스에 활용하고자 하는 니즈가 있음

첫째는, 기업이 직접 상거래용 자사 토큰, Dapp 및 Main-net 을 개발하고 운용하기에는 많은 어려움들이 있음 심지어 대기업들도 어려움을 겪고 있음

둘째는, 상거래 지불 결제용 토큰으로 마땅한 것이 없음

Business with Stablecoin

스테이블코인은 기업에게 어떤 이익을 주는가?

- 기존 카드, VAN망을 이용하지 않고도 금융 생태계 구축 가능
- 개방형의 포인트, 상품권 생태계 구축 가능
- 각 종 수수료 절감 효과가 크며, 상품을 더 저렴하게 판매할 수 있음
- 기존 포인트, 쿠폰 등을 대체 가능하며 토큰을 활용한 다양한 마케팅 활동이 가능함
- 빠른 결제 대금의 정산이 가능해짐
- 고객과 매출을 경쟁 기업에 뺏기지 않고 자사 생태계에 묶어두는 효과가 큼
- 국가간 통화 장벽이 없이 글로벌한 서비스 가능
- 블록체인과 탈중앙화로 인한 결제 신뢰성 및 안정성 증가
- 상품 판매 및 유통, 결제 이력 트래킹이 가능해져 양질의 대고객 서비스 제공 가능
- 연합 생태계를 구축해 신규 고객 확보와 매출 증대가 가능

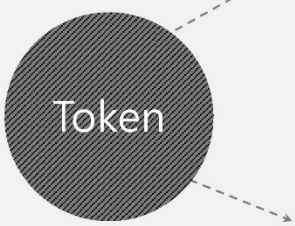
Business with Stablecoin

스테이블코인은 고객에게 어떤 이익을 주는가?

- 수수료 절감 효과로 인해 상품을 더 저렴하게 구매할 수 있음
- 현금화가 가능하고 사용 기간 등의 제약이 없음
- 다양한 프로모션 및 마케팅 혜택을 누릴 수 있음
- 부가적인 수익 채굴이 가능해짐
- 무형의 서비스나 지식 등을 판매하거나 구매할 수 있음
- 중고 상품의 사용 이력 파악이 가능해짐
- 가격 변동성 없는 안정적인 결제 서비스를 제공 받을 수 있음
- 소비자도 쉽게 개인 상점 개설이 가능함

Business with Stablecoin

원토큰 문제 (One-Token Problem) 이란 무엇인가?



유틸리티 토큰의 성격이 강할 경우

안정적인 결제용 유틸리티 토큰의 성격이 강할수록 거래소에서 이 토큰을 더 비싼 가격에 사고자 하는 매력도가 떨어질 수 있습니다

시큐리티 토큰의 성격이 강할 경우

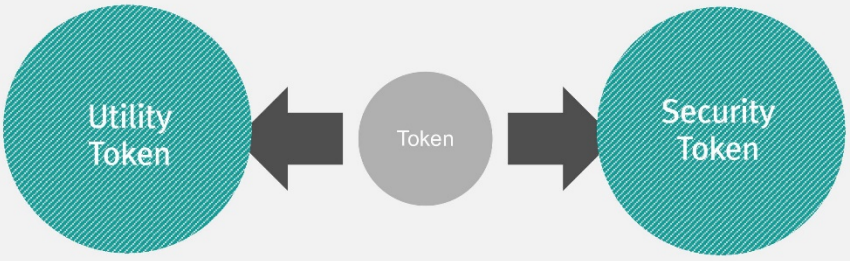
생태계의 가치를 담고 있는 시큐리티 토큰의 경우 많은 유통량을 만들어 낼 수 없으므로 결제용 토큰으로써 기능이 저하되는 문제점이 발생할 수 있습니다

Business with Stablecoin

멜리오의 원토큰 문제 해결방안

토큰 이중화

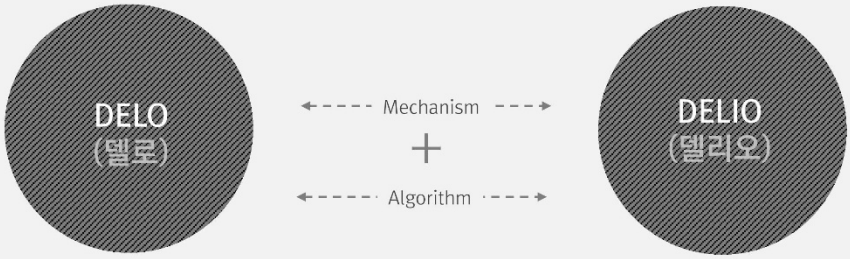
시큐리티 토큰과 유틸리티 토큰의 물리적 분리



Business with Stablecoin

델리오의 원토큰 문제 해결방안

Stable Stake Coin (SSC)



결제에 사용할 수 있는 완벽한 결제용 토큰

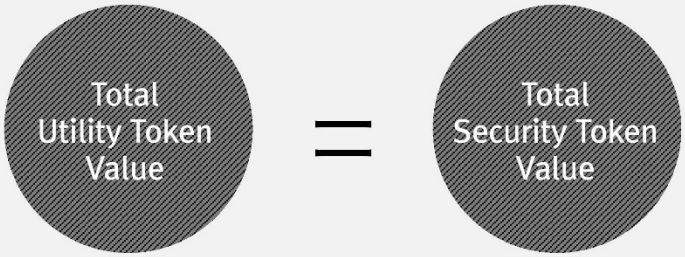
- 델리오 생태계 내에서 상품 결제용 및 보상 토큰으로 사용
- 초기 발행량은 0이며 DELO 사용 기업이 늘어나면서 발행량도 증가함
- 가격이 완전히 안정되어 있는 상거래용 토큰이 이며 1DELO = 0.012USD
- DELO : DELIO = 1:1 에서 시작하며 DELO 는 토큰 발행량이 증가하고 DELIO는 토큰 개당 가격이 올라가는 구조
- DELO와 DELIO는 지정된 Wallet 및 거래소에서 환전 비율에 따라 상호 환전
- DAAS 사용 기업이 자체 토큰으로 발행 및 생태계 내에서만 사용되며 거래소 미상장

투자자, 환전, 자산 확보용 토큰

- DELIO 는 토큰 가격이 상승할 수 있는 가격 변동성 토큰
- 선발행이며 전체 발행량은 50억개로 한정
- DELO토큰 발행량 증가에 따라 DELIO 토큰 개당 가격 상승 매커니즘
- DELIO 가격은 절대 1DELO 가격(0.012USD) 밑으로 떨어지지 않음
- DELIO 토큰으로 상품을 구매하지 못함
- 소유한 DELIO 토큰의 양(지분) 만큼 매출수익 채굴권 부여
- 외부 암호화폐 거래소에 상장
- 향후 증권형 토큰으로 변환 추진

Business with Stablecoin

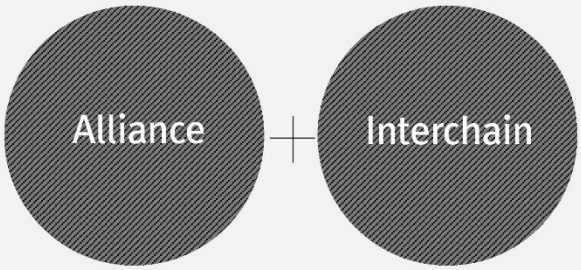
델리오의 원토큰 문제 해결방안



$$\frac{DELIO}{DELO} = n \quad (n >= 1)$$

Business with Stablecoin

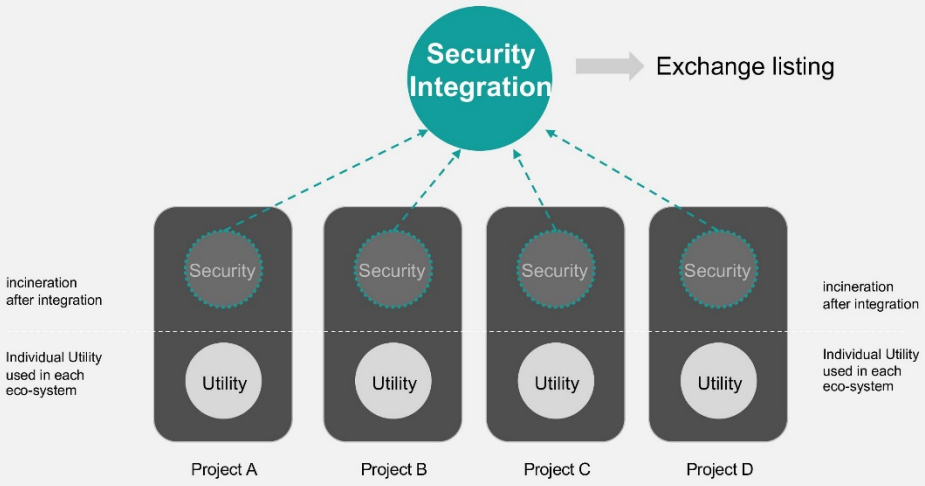
어떻게 토큰 생태계를 통합할 것인가?



- 메인넷의 기술지원이 충분하지 못함
- 각 비즈니스 특성에 맞는 기능을 제공하지 못함
- 토큰의 가치의 통합적 관리가 불가능함
- 비즈니스 지원이 약함
- 홀더 및 커뮤니티 통합이 어려움

Business with Stablecoin

어떻게 토큰 생태계를 통합할 것인가?



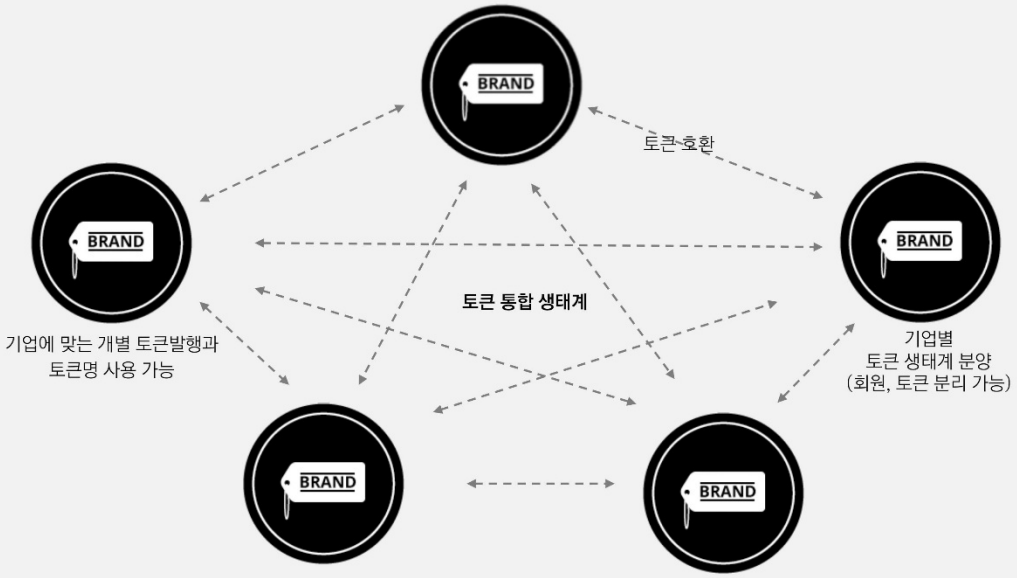
Business with Stablecoin

어떻게 토큰 순환경제 생태계를 구현할 것인가?

["소유와 수익"의
"분산과 공유"의 생태계]

Business with Stablecoin

연합생태계 구성의 중요성



Business with Stablecoin

델리오의 연합생태계 구성 방안

1

SSC (Stable Stake Coin)

최초의 탈중앙화된 상거래 결제 전용 토큰

기존 상거래 결제 토큰들의 문제점을 획기적으로 개선해 사용자를 위한 〞가격 안정성" 과 투자자를 위한 "가치상승" 모두 가능한 차별화된 코인으로 "투자가치도 뛰어납니다" 본격적으로 실물경제에서 상품구매를 위한 상거래 결제용으로 사용할 수 있는 차별화된 "탈중앙화된 스테이블코인 및 탈중앙화된 PG" 입니다.

2

DAAS (Delio As A Service)

ASP방식의 자사 토큰 발행 및 운영 솔루션

기업은 Dapp 이나 Main-net 개발 없이도 ASP 방식으로 쉽고 빠르게 자사의 토큰을 발행하고 독립 토큰이코노미 생태계를 무상으로 구축할 수 있으며 BAAS 방식보다 서비스 구축이 빠르고 효율적이며 확장성이 좋습니다. 또한, 독립된 자사 생태계와 더불어 델리오 연합생태계를 동시에 구축함으로써 고객, 마케팅, 금융 수수료 절감, 매출향상에 도움이 됩니다. 델리오 API를 통해서 기존 앱(App) 및 웹서비스(쇼핑몰 등)를 쉽게 Dapp화 할 수 있습니다

3

Decentralized P2P PG (탈중앙화된 P2P PG)

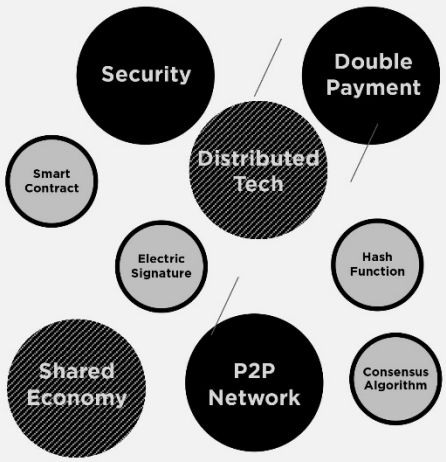
퍼블릭체인 기반의 탈중앙화된 P2P PG

델리오만의 상거래 전용 토큰인 SSC와 DAAS의 파워풀한 기능을 기반으로 제공되는 PG서비스 입니다. 기존 카드사와 결제대행 PG서비스를 배제하고 기업이 고객에게 직접적으로 결제서비스를 제공할 수 있으며, 탈중앙화된 PG의 모든 수익은 델리오 토큰 홀더에게 공유됩니다

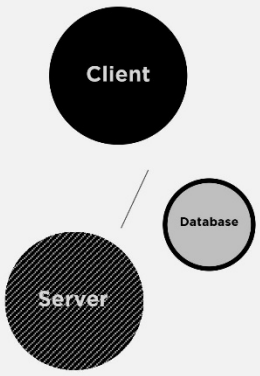
Business with Stablecoin

프라이빗체인의 한계 극복

블록체인 시스템

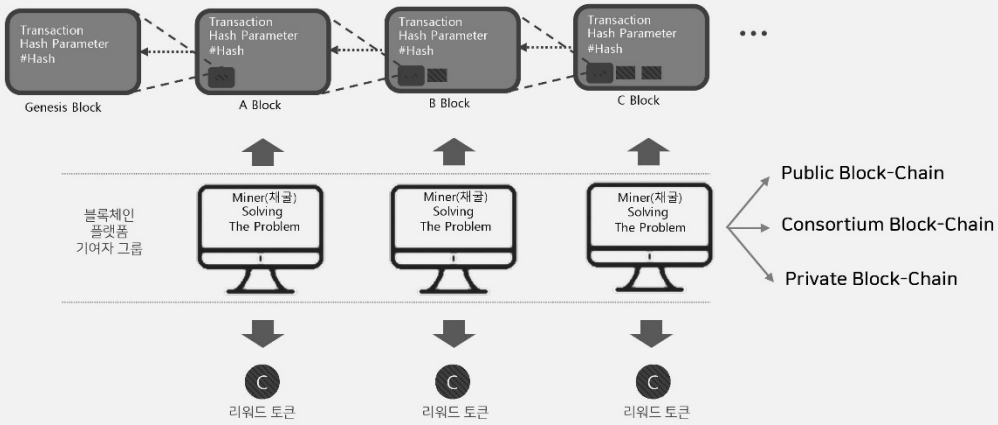


기존 시스템



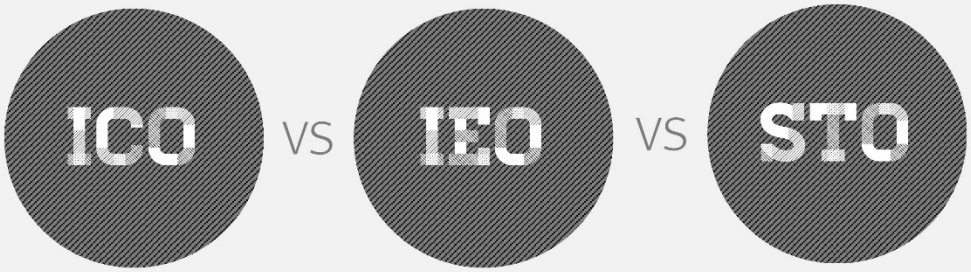
Business with Stablecoin

프라이빗체인의 한계 극복



Business with Stablecoin

성공적인 투자 및 상장 전략



Business with Stablecoin

성공적인 투자 및 상장 전략

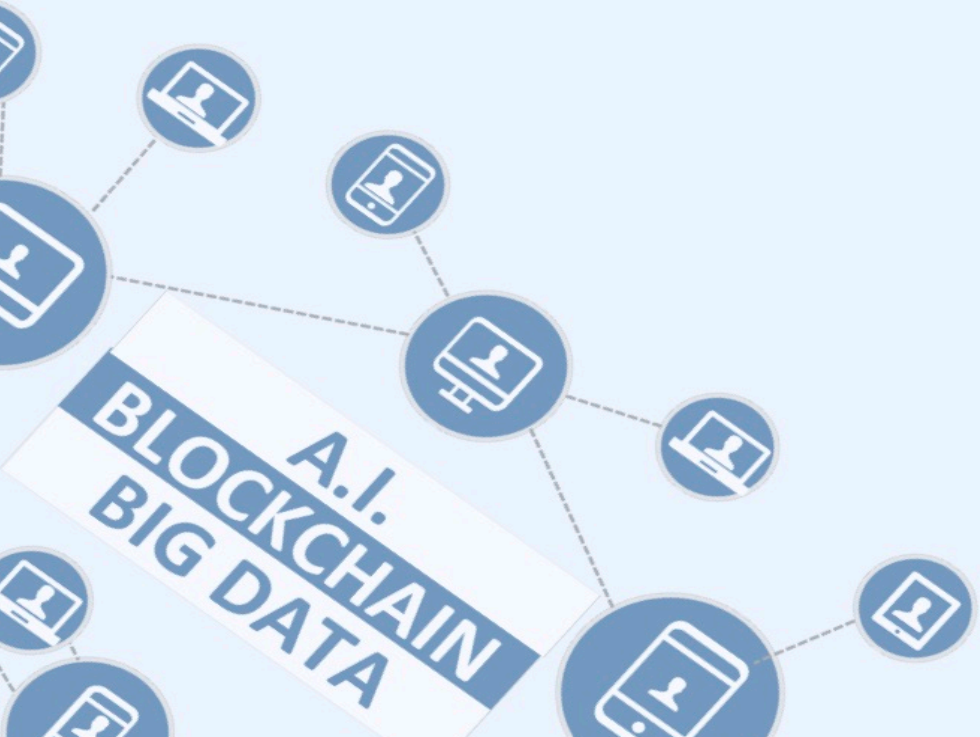
#	이름	조정된 거래량 (24시간)*	거래량(24시간)	거래량(7일)	거래량(30일)	시장 없음	변경(24시간)	거래량 그래프 (7일
1	OKEx	₩1,190,857,712,668	₩1,190,857,712,668	₩7,466,373,922,950	₩41,492,663,196,311	379	-2.93%	
2	Binance	₩1,176,975,543,438	₩1,176,975,543,438	₩6,147,654,583,836	₩38,975,016,986,476	466	7.14%	
3	DigiFinex	₩1,030,706,548,224	₩1,030,706,548,224	₩6,627,649,554,207	₩38,925,614,217,320	173	-5.85%	
4	Coineal	₩968,814,193,496	₩968,814,193,496	₩5,071,488,938,403	₩30,408,224,265,445	50	-2.08%	
5	CoinBene	₩945,163,259,894	₩945,163,259,894	₩5,206,581,396,940	₩27,903,567,447,410	192	-1.52%	
6	Huobi Global	₩933,336,903,915	₩933,336,903,915	₩4,923,293,410,118	₩28,821,266,611,114	430	6.34%	
7	BitForex	₩921,789,844,673	₩921,789,844,673	₩5,120,840,565,948	₩29,610,779,578,835	182	3.11%	
8	HitBTC	₩920,244,800,109	₩920,244,800,109	₩6,069,257,740,884	₩31,013,433,244,162	790	-6.96%	
9	Bibox	₩915,330,994,124	₩915,330,994,124	₩4,897,433,058,574	₩25,952,119,305,256	183	3.78%	
10	BW.com	₩914,418,736,848	₩914,418,736,848	₩4,996,649,476,955	₩28,719,008,859,831	46	1.13%	
11	Bit-Z	₩907,933,624,751	₩907,933,624,751	₩4,869,300,459,886	₩30,524,409,100,553	173	11.40%	
12	IDAX	₩895,337,347,045	₩895,337,347,045	₩4,818,665,856,108	₩25,552,207,976,179	107	1.96%	

Thank you

This material is proprietary to Blockchain Lecture. It contains trade secrets and confidential information which is the property of Blockchain Lecture. This material shall not be used, reproduced, copied, disclosed, transmitted, in whole or in part, without the express consent of Blockchain Lecture.

델리오 정상호 대표
02.2088.2779
aarum@delio.io

-마치며-



| 마치는 글

이 흥 노

광주과학기술원 블록체인경제센터장

2019 년 7 월 22 일

안녕하십니까,

블록체인경제 특론을 마치게 되어 시원하기도 하고 섭섭하기도 합니다. 총 14 차례의 강의가 있었습니다. 제가 블록체인경제를 강의하였고, 열 세분의 블록체인과 암호화폐 분야의 최고 전문가들을 오셔서 블록체인 기술, 그로부터 새롭게 생겨나는 자유, 평등, 경제, 규제, 미래사회의 변화에 대하여 강의를 진행하였습니다. 이를 통하여 확보한 강의 자료와 강의 동영상은 매우 귀중한 자료입니다. 이런 소중한 자료를 공개하여 공유할 수 있도록 허락해 주신 강사님들께 감사드립니다. GIST 의 학생들에게도 감사의 말씀을 드립니다. 서로 다른 주제로 매주 3 시간씩 진행되는 강의에 집중하고, 숙제도 해야하고, 중간고사, 기말고사까지 치러야 했으니 정말 힘든 일정이었습니다. 꾸준히 참석해 주시고, 활발하게 질문도 해 주셨던 외부 청강생 여러분께도 감사의 말씀을 드립니다. 다음에 더 좋은 강의를 기획하여 다시 뵙기를 희망합니다.

참여해 주신 모두에게 다시 한 번 감사드리며 이만 마칩니다.

Heung-No Lee, Ph.D.
==========
Professor, School of EECS, GIST
Director of Blockchain-Internet Economy Center
Director of Sensor Intelligence Center
123 Chemdan gwagiro, Buk-gu
Gwangju, Korea 500-712
Phone: +(82) 62-715-2237
Cell Phone: +(82) 10-4946-4710
Web-site: http://infonet.gist.ac.kr/

자료집 끝

A.I.
BLOCKCHAIN
BIG DATA